



**Security Products**

# **Secure Services Gateway (SSG) 5 Hardware Installation and Configuration Guide**

*ScreenOS 5.4.0*

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

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

Part Number: 530-015647-01, Revision A

## Copyright Notice

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

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

## FCC Statement

The following information is for FCC compliance of Class 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

	<b>About This Guide</b>	<b>5</b>
	Organization .....	5
	WebUI Conventions .....	6
	CLI Conventions .....	6
	Obtaining Documentation and Technical Support .....	7
<b>Chapter 1</b>	<b>Hardware Overview</b>	<b>9</b>
	Port and Power Connectors .....	10
	Front Panel .....	11
	System Status LEDs .....	11
	Port Descriptions .....	13
	Ethernet Ports .....	13
	Console Port .....	13
	AUX Port .....	14
	Back Panel .....	14
	Power Adapter .....	14
	Radio Transceiver .....	14
	Grounding Lug .....	15
	Antennae Types .....	15
	Universal Serial Bus Host Module .....	15
<b>Chapter 2</b>	<b>Installing and Connecting the Device</b>	<b>17</b>
	Before You Begin .....	17
	Equipment Installation .....	18
	Connecting Interface Cables to a Device .....	19
	Connecting the Power .....	19
	Connecting the Device to a Network .....	19
	Connecting a Device to an Untrusted Network .....	20
	Connecting Ethernet Ports .....	21
	Connecting Serial (AUX/Console) Ports .....	21
	Connecting the WAN Ports .....	21
	Connecting a Device to an Internal Network or Workstation .....	22
	Connecting Ethernet Ports .....	22
	Connecting the Wireless Antennae .....	22
<b>Chapter 3</b>	<b>Configuring the Device</b>	<b>23</b>
	Accessing the Device .....	24
	Using a Console Connection .....	24
	Using the WebUI .....	25
	Using Telnet .....	26
	Default Device Settings .....	27
	Basic Device Configuration .....	29

	Changing the Root Admin Name and Password .....	29
	Setting the Date and Time .....	30
	Bridge Group Interfaces .....	30
	Administrative Access .....	31
	Management Services.....	31
	Host and Domain Name .....	31
	Default Route.....	32
	Management Interface Address .....	32
	Backup Untrust Interface Configuration .....	32
	Wireless Configuration .....	33
	Wireless Network Configuration .....	34
	Wireless Configuration Example .....	35
	Authentication and Encryption.....	37
	WAN Configuration .....	38
	ISDN Interface .....	38
	V.92 Modem Interface .....	39
	Basic Firewall Protections .....	40
	Verifying External Connectivity.....	40
	Resetting the Device to Factory Defaults.....	41
	The Reset Pinhole.....	41
<b>Chapter 4</b>	<b>Servicing the Device</b> .....	<b>43</b>
	Required Tools and Parts .....	43
	Memory Upgrade .....	43
<b>Appendix A</b>	<b>Specifications</b> .....	<b>47</b>
	SSG 5 Physical Specifications .....	47
	Electrical Specifications.....	47
	Environmental Tolerance .....	47
	Certifications.....	48
	Safety .....	48
	EMC (Emissions).....	48
	EMC Immunity .....	48
	European Telecommunications Standards Institute (ETSI) .....	48
	Connectors.....	49
<b>Appendix B</b>	<b>Initial Configuration Wizard</b> .....	<b>51</b>
	<b>Index.....</b>	<b>63</b>

# About This Guide

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

Juniper Networks offers six models of the Secure Services Gateway (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

All of the SSG 5 devices support a universal storage bus (USB) host module. The devices also provide protocol conversions between local area networks (LANs) and wide area networks (WANs), and three of the models support wireless local area networks (WLANs).

## Organization

---

This guide contains the following sections:

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

## WebUI Conventions

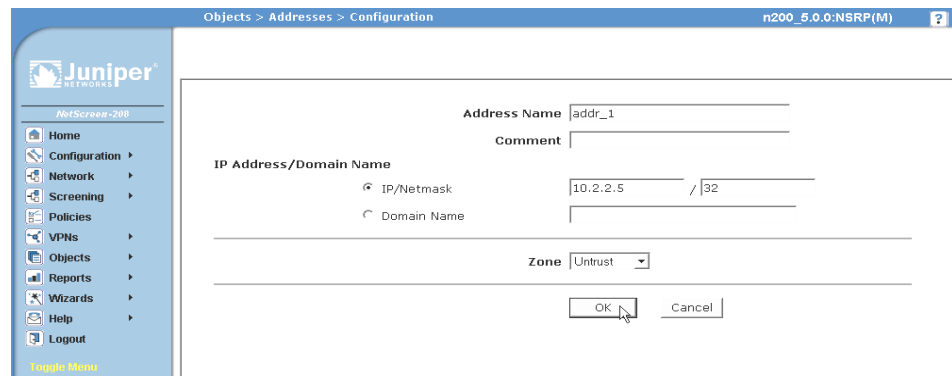
To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. A chevron ( > ) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The set of instructions for each task is divided into navigational path and configuration settings.

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

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

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

**Figure 1: Navigational Path and Configuration Settings**



## CLI Conventions

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

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe ( | ). For example:

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

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

- Variables are in *italic* type:

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

In text:

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

---

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

---

## Obtaining Documentation and Technical Support

---

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

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

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

[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:

- “Port and Power Connectors” on page 10
- “Front Panel” on page 11
- “Back Panel” on page 14

## Port and Power Connectors

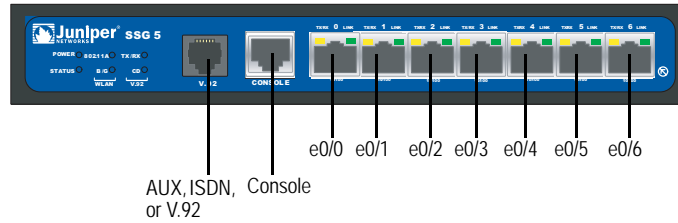


Table 1 shows the ports and power connectors on an SSG 5 device.

**Table 1: SSG 5 Port and Power Connectors**

Port	Description	Connector	Speed/Protocol
Ports 0/0-0/6	Enables direct connections to workstations or a LAN connection through a switch or hub. This connection also allows you to manage the device through a Telnet session or the WebUI.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB	Enables a 1.1 USB connection with the system.	N/A	12M (full speed) or 1.5M (low speed)
Console	Enables a serial connection with the system. Used for terminal-emulation connectivity to launch Command Line Interface (CLI) sessions.	RJ-45	9600 bps/ RS-232C serial
AUX	Enables a backup RS-232 async serial Internet connection through an external modem.	RJ-45	9600 bps — 115 Kbps/ RS-232C serial
V.92 Modem	Enables a primary or backup Internet or untrusted network connection to an Internet Service Provider (ISP).	RJ-11	9600 bps — 115 Kbps/ RS-232 Serial autosensing duplex and polarity
ISDN	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
Antenna A & B (SSG 5-WLAN)	Enables a direct connection to workstations in the vicinity of a wireless radio connection.	RPSMA	802.11 a (54 Mbps on 5GHz radio band) 802.11 b (11 Mbps on 2.4GHz radio band) 802.11 g (54 Mbps on 2.4GHz radio band) 802.11 superG (108 Mbps on 2.4GHz and 5 GHz radio bands)

## Front Panel

This section describes the following elements on the front panel of an SSG 5 device:

- System Status LEDs
- Port Descriptions

### System Status LEDs

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

**Figure 2: Status LEDs**



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

**Table 2: Status LED Descriptions**

Type	Name	Color	State	Description
	POWER	Green	On steadily	Indicates that the system is receiving power
			Off	Indicates that the system is not receiving power
		Red	On steadily	Indicates that the device is not operating normally
			Off	Indicates that the device is operating normally
	STATUS	Green	On steadily	Indicates that the system is booting up or performing diagnostics
			Blinking	Indicates that the device is operating normally
		Red	Blinking	Indicates that there was an error detected
ISDN devices	CH B1	Green	On steadily	Indicates that B-Channel 1 is active
			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

Type	Name	Color	State	Description
V.92 devices	HOOK	Green	On steadily	Indicates that the link is active
			Off	Indicates that the serial interface is not in service
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through
WLAN devices	802.11A	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 baud rate is proportional to the link activity
			Off	Indicates that there is no wireless connection established
	B/G	Green	On steadily	Indicates that a wireless connection is established but there is no link activity
			Blinking	Indicates that a wireless connection is established. The baud rate is proportional to the link activity
			Off	Indicates that there is no wireless connection established

## Port Descriptions

This section explains the purpose and function of the following:

- Ethernet Ports
- Console Port
- AUX Port

### Ethernet Ports

Seven 10/100 Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic. The ports are labeled **0/0** through **0/6**. See “Default Device Settings” on page 27 for the default zone bindings for each Ethernet port.

When configuring one of these ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are: **ethernet0/0** through **ethernet0/6**.

Figure 3 displays the location of the LEDs on each Ethernet port.

**Figure 3: Activity Link LEDs**

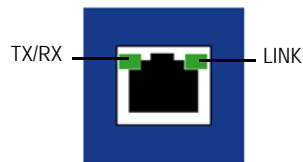


Table 3 describes the Ethernet port LEDs.

**Table 3: Ethernet Port LEDs**

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

### Console Port

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

See “Connectors” on page 49 for the RJ-45 connector pinouts.

## AUX Port

The auxiliary (AUX) port is an RJ-45 serial port wired as Data Terminal Equipment (DTE) that can be connected to a modem to allow remote administration. We do not recommend using this port for regular remote administration. The AUX port is typically assigned to be the backup serial interface. The baud rate is adjustable from 9600 bps to 115200 bps and requires hardware flow control.

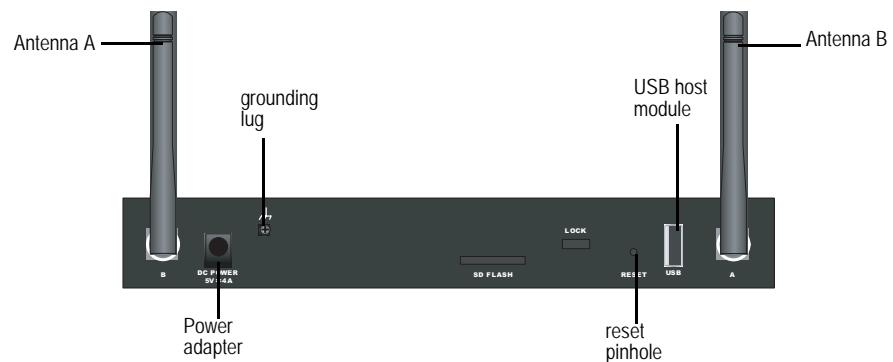
See “Connectors” on page 49 for the RJ-45 connector pinouts.

## Back Panel

This section describes the back panel of an SSG 5 device:

- Power Adapter
- Radio Transceiver
- Grounding Lug
- Antennae Types
- Universal Serial Bus Host Module

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



### Power Adapter

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

### Radio Transceiver

The SSG 5-WLAN devices contain two wireless connectivity radio transceivers, which support 802.11a/b/g standards. The first transceiver (WLAN 0) uses the 2.4 GHz radio band, which supports the 802.11b standard at 11 Mbps and the 802.11g at 54 Mbps. The second radio transceiver (WLAN 1) uses the 5 GHz radio band, which supports the 802.11a standard at 54 Mbps. The two radio bands can work simultaneously. For information on configuring the wireless radio band, see “Wireless Configuration” on page 33.

## Grounding Lug

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

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

## Antennae Types

The SSG 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 well suited for such places as hallways and outer walls (with the antenna facing inward).

## Universal Serial Bus Host Module

The slot labeled USB on the back panel of an SSG 5 device implements a host-only universal serial bus (USB) 1.1 host module for a USB device adapter or USB flash key, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB storage device is installed and configured, it automatically acts as a secondary storage device.

The USB host module allows file transfers, such as device configurations, user certifications, and update version images between an external USB flash key and the internal flash storage located in the security device. The USB host module supports USB 1.1 specification at either low-speed (1.5M) or full-speed (12M) file transfer.

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

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

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

If you want to view the saved file information on the USB flash key or internal flash storage, use the **get file** CLI 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 this page
- “Equipment Installation” on page 18
- “Connecting Interface Cables to a Device” on page 19
- “Connecting the Power” on page 19

---

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

---

## Before You Begin

---

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



**WARNING:** To prevent abuse and intrusion by unauthorized personnel, install an 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.

## Equipment Installation

---

You can front-mount, wall-mount, or desk-mount an SSG 5 device. The mounting kits may be purchased separately.

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

---

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

---

To rack-mount an SSG 5 device:

1. Unscrew the mounting brackets with the phillips screwdriver.

---

**NOTE:** SSG 5-WLAN users with the optional antennae need to remove the existing antennae, then connect the new antenna through the side hole.

---

2. Align the bottom of the device with the base holes.
3. Pull the device forward to lock it in the base holes.
4. Screw the mounting brackets to the device and the rack.
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 4, then continue.
7. Place the tray in the rack.
8. Plug in the power supply to the power outlet.

To wall-mount an SSG 5 device, do the following:

1. Align the wall mount ears to the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Ensure that the wall to be used is smooth, flat, dry and sturdy.
4. Mount the device on the wall with the provided screws.
5. Plug the power supply into the power outlet.

To desk-mount an SSG 5 device:

1. Attach the desktop stand to the side of the device. We recommend the side closest to the power adapter.
2. Place the mounted device on the desktop.
3. Plug the power supply into the power outlet.

---

## Connecting Interface Cables to a Device

---

To connect interface cables to the device:

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

---

## Connecting the Power

---

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

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



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

---

---

## Connecting the Device to a Network

---

The SSG 5 devices provide firewall and general security for networks when it is placed between internal networks and the untrusted network. This section describes the following:

- Connecting a Device to an Untrusted Network
- Connecting a Device to an Internal Network or Workstation

## Connecting a Device to an Untrusted Network

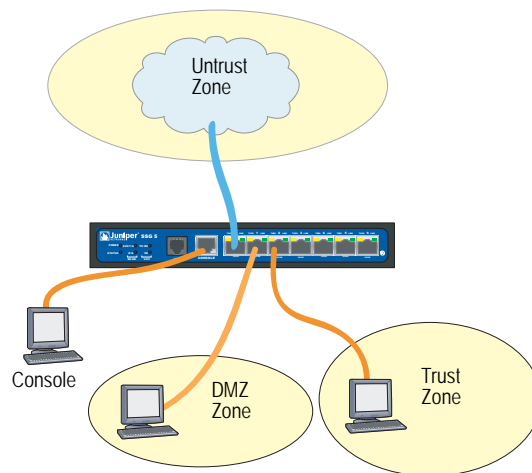
You can connect your SSG 5 device to the untrusted network in one of the following ways:

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

Figure 5 shows the SSG 5 with basic network cabling connections with the 10/100 Ethernet ports cabled as follows:

- The port labeled 0/0 (ethernet0/0 interface) is connected to the untrust network.
- The port labeled 0/1 (ethernet0/1 interface) is connected to a workstation in the DMZ security zone.
- The port labeled 0/2 (bgroup0 interfaces) is connected to a workstation that is in the Trust security zone.
- The console port is connected to a serial terminal for management access.

**Figure 5: Basic Networking Example**



## Connecting Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/0 on an SSG 5 device to the external router. The device autosenses the correct speed, duplex, and MDI/MDIX settings.

## Connecting Serial (AUX/Console) Ports

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



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

---

## Connecting the WAN Ports

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

## Connecting a Device to an Internal Network or Workstation

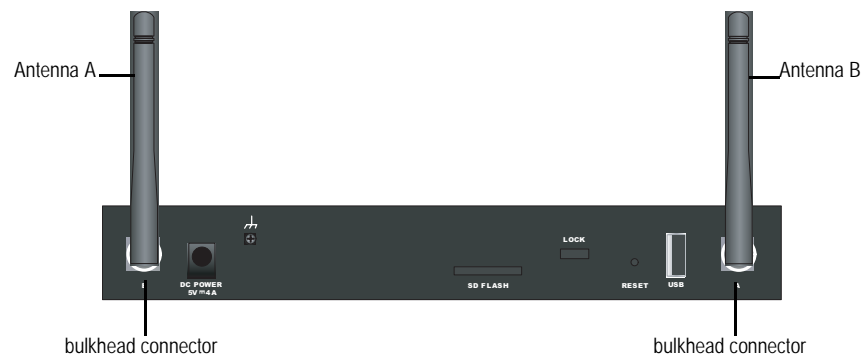
You can connect your local area network (LAN) or workstation with the Ethernet and/or wireless interfaces.

### Connecting Ethernet Ports

An SSG 5 device contains seven Ethernet ports. You can use one or more of these ports to connect to LANs through switches or hubs. You can also connect one or all of the ports directly to workstations, eliminating the need for a hub or switch. You can use either crossover or straight through cables to connect the Ethernet ports to other devices. See “Default Device Settings” on page 27 for the default interface-to-zone bindings.

### Connecting the Wireless Antennae

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



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

## Chapter 3

# Configuring the Device

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

This chapter contains the following sections:

- “Accessing the Device” on page 24
- “Default Device Settings” on page 27
- “Basic Device Configuration” on page 29
- “Wireless Configuration” on page 33
- “WAN Configuration” on page 38
- “Basic Firewall Protections” on page 40
- “Verifying External Connectivity” on page 40
- “Resetting the Device to Factory Defaults” on page 41

---

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

---

## Accessing the Device

---

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

- **Console:** The Console port on the device allows you to access the device through a serial cable connected to your workstation or terminal. To configure the device, you enter ScreenOS Command Line Interface (CLI) commands on your terminal or in a terminal-emulation program on your workstation.
- **WebUI:** The ScreenOS WebUI is a graphical interface available through a Web browser. To initially use the WebUI, the workstation on which you run the Web browser must be on the same subnetwork as the device. You can also access the WebUI through a secure server using secure sockets layer (SSL) using secure HTTP (S-HTTP).
- **Telnet/SSH:** Telnet and Secure Shell (SSH) are applications that allows you to access devices through an IP network. To configure the device, you enter ScreenOS CLI commands in a Telnet session from your workstation. For more information, see the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- **NetScreen-Security Manager:** NetScreen-Security Manager is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks firewall/IPSec VPN devices. For instructions on how to manage your device with NetScreen-Security Manager, refer to the *NetScreen-Security Manager Administrator's Guide*.

## Using a Console Connection

---

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

---

To establish a console connection, do the following:

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.) Figure 6 shows the type of DB-9 connector that is needed.

**Figure 6: DB-9 Adapter**



2. Plug the male end of the RJ-45 CAT5 serial cable into the Console port on the SSG 5. (Be sure that the other end of the CAT5 cable is inserted properly and secured in the DB-9 adapter.)



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

For information on how to configure the device with the CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

## Using the WebUI

To use the WebUI, 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, do the following:

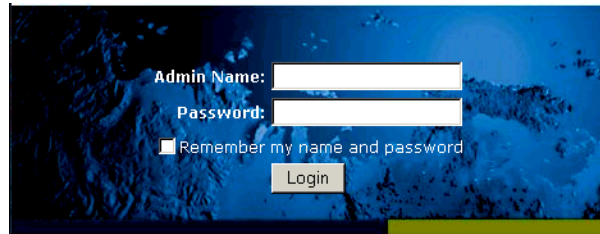
1. Connect your workstation to the 0/2 — 0/6 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for DHCP or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the bgroup0 interface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

---

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

---

The WebUI application displays the login prompt as shown in Figure 7.

**Figure 7: WebUI Login Prompt**

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

## Using Telnet

To establish a Telnet connection, do the following:

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 statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Start a Telnet client application to the IP address for the bgroup0 interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

The Telnet application displays the login prompt.

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

## Default Device Settings

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

Table 4 describes the default zone bindings for ports on the devices.

**Table 4: 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

A bridge group or bgroup, is designed to allow network users to switch between wired and wireless traffic without having to reconfigure or reboot the device. 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.

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

To unset ethernet0/3 from bgroup0 and assign it to the Trust zone with a static IP address of 192.168.3.1/24, use the WebUI or CLI:

**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
```

**Table 5: 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>		
Layer2 interface	vlan1 specifies the logical interfaces used for management and VPN traffic termination while the device is in Transparent mode.	N/A
Tunnel interfaces	tunnel.n specifies a logical tunnel interface. This interface is for VPN traffic.	N/A

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

---

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

---

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

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

## Basic Device Configuration

---

This section describes the following optional configuration:

- Changing the Root Admin Name and Password
- Setting the Date and Time
- Bridge Group Interfaces
- Administrative Access
- Management Services
- Host and Domain Name
- Default Route
- Management Interface Address
- Backup Untrust Interface Configuration

### Changing the Root Admin Name and Password

The root admin user has complete privileges to configure an SSG 5 device. We recommend that you change the default root admin name (**netscreen**) and password (**netscreen**) immediately.

#### WebUI

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

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

---

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

---

#### CLI

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

## Setting the Date and Time

The time set on an SSG 5 device affects events such as the setup of VPN tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device system clock with the workstation clock.

To configure the date and time on a device, use the WebUI or CLI:

### WebUI

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

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

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

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

## Bridge Group Interfaces

By default, the SSG 5 device has Ethernet interfaces ethernet0/2—ethernet0/4 grouped together in the Trust security zone. Grouping interfaces sets interfaces in one subnet. You can unset an interface from a group and assign it to a different security zone. Interfaces must be in the Null security zone before they can be assigned to a group. To place a grouped interface in the Null security zone, use the `unset interface interface port interface` CLI command.

The SSG 5-WLAN devices allow Ethernet and wireless interfaces to be grouped under one subnet.

---

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

---

To configure a group with Ethernet and wireless interfaces, use the WebUI or CLI:

### 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
```

## **Administrative Access**

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

### **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
```

## **Management Services**

ScreenOS provides services for configuring and managing the device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis. To configure the management services on the device, use the WebUI or CLI:

### **WebUI**

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

### **CLI**

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

## **Host and Domain Name**

The domain name defines the network or subnetwork that the device belongs to, while the hostname refers to a specific device. The hostname and domain name together uniquely identify the device in the network. To configure the host and domain name on a device, use the WebUI or CLI:

### **WebUI**

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

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

**CLI**

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

**Default Route**

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

**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
```

**Management Interface Address**

The Trust interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the 0/2—0/4 port on the device to a workstation, you can configure the device from a workstation in the 192.168.1.1/24 subnet using a management service such as Telnet.

You can change the default IP address on the trust interface. For example, you might want to change the interface to match IP addresses that already exist on your LAN.

**Backup Untrust Interface Configuration**

The SSG 5 device allows you to configure a backup interface for untrust failover. To set a backup interface for untrust failover, do the following:

1. Set the backup interface in the Null security zone with the **unset interface interface [ port interface ]** CLI command.
2. Bind the backup interface to the same security zone as the primary interface with the **set interface interface zone zone\_name** CLI command.

---

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

---



To set the ethernet0/4 interface as the backup interface to the ethernet0/0 interface, use the WebUI or CLI:

### **WebUI**

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

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

### **CLI**

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

## **Wireless Configuration**

---

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

---

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

---

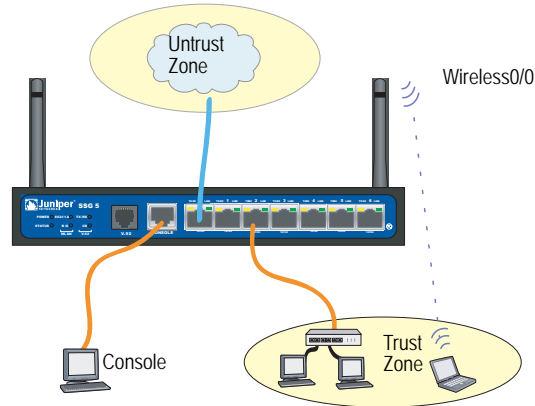
---

**NOTE:** If your regional code is ETSI, you must set the correct country code that meets your local radio spectrum regulation.

---

Figure 8 shows the default configuration for the SSG 5-WLAN device.

**Figure 8: Default SSG 5-WLAN Configuration**



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

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

For more information about WLANs, refer to *WLAN* in the *Concepts & Examples ScreenOS Reference Guide*.

## Wireless Network Configuration

Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs allows you to have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured.

The SSG 5-WLAN device allows you to create up to 16 SSIDs, but only 4 of them can be used simultaneously. You can configure the device to use the 4 SSIDs on either one of the transceivers or split the use on both. For example, 3 SSIDs assigned to WLAN 0 and 1 SSID assigned to WLAN 1. Use the **set interface wireless\_interface wlan { 0 | 1 | both }** CLI command to set the radio transceivers on the SSG 5-WLAN device.

To set the SSID name **netscreen open**, allow the SSID to be open to all users, bind the SSID to the wireless0/0 interface, and use both radio transceivers, use the WebUI or CLI:

### **WebUI**

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

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

### **CLI**

```
set ssid name "netscreen open"  
set ssid "netscreen open" authentication open encryption none  
set ssid "netscreen open" interface wireless0/0  
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.

## **Wireless Configuration Example**

To set up a wireless interface for basic wireless configuration, use the WebUI or CLI:

### **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
```

To set an ethernet and wireless interface to the same bridge group interface, use the WebUI or CLI:

**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 **exec wlan reactivate** CLI command or click **Activate Changes** on the Wireless > General Settings WebUI page.

---

## Authentication and Encryption

The SSG 5-WLAN supports the following authentication and encryption methods:

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

Once you have set an SSID to the wireless0/0 interface, you can access the device using the default wireless0/0 interface IP address in the steps provided “Accessing the Device” on page 24. Refer to the *Concepts & Examples ScreenOS Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

## WAN Configuration

---

This section explains how to configure the following WAN interfaces:

- ISDN Interface
- V.92 Modem Interface

### 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 multi-link 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 encap ppp
set interface bri0/0 ppp profile isdnprofile
save
```

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

To configure the ISDN interface as the backup interface, see “Backup Untrust Interface Configuration” on page 32.

## V.92 Modem Interface

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

---

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

---

To configure the V.92 interface, 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 devices are configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide*.

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 an remote network from trying to identify services to target for further attacks.
- The device applies firewall policies, which can contain content filtering and intrusion detection and prevention (IDP) components, to the traffic that passes the SCREEN filters from one zone to another. By default, no traffic is permitted to pass through the device from one zone to another. To permit traffic to cross the device from one zone to another, you must create a policy that overrides the default behavior.

To set ScreenOS SCREEN options for a zone:

### WebUI

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

### CLI

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

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

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



## Resetting the Device to Factory Defaults

---

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



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

---

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

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

### The Reset Pinhole

You can reset the device and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the device status LEDs on the front panel or start a Console session as described in Using a Console Connection on page 24.

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

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

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

2. Wait for one to two seconds.

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

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

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

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

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

If you do not follow the complete sequence, the reset process cancels without any configuration change and the console message states that the erasure of the configuration is aborted. The STATUS LED returns to blinking green. If the device did not reset, an SNMP alert is sent to confirm the failure.

## Chapter 4

# Servicing the Device

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

- “Required Tools and Parts” on this page
- “Memory Upgrade” on this page

---

**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 an SSG 5 device, you need the following tools and parts:

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

### Memory Upgrade

---

You can upgrade an SSG 5 device from a single 128 MB SDIMM DRAM memory module to a 256 MB module.

To upgrade the memory on an SSG 5 device, do the following:

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 device so that the top of the device is laying 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.

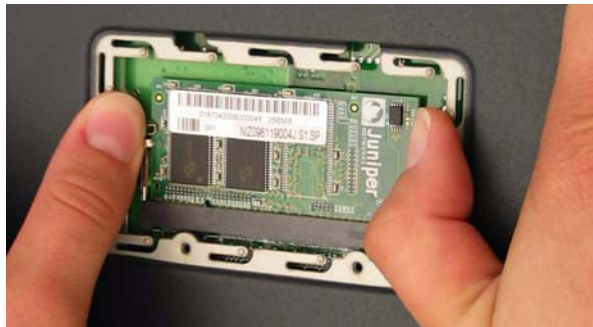
5. Remove the memory card cover.

**Figure 9: Bottom of Device**



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

**Figure 10: Unlocking the Memory Module**



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

**Figure 11: Removing Module Slots**



8. Insert the 256 MB SDIMM DRAM memory modules 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 12: 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.

### SSG 5 Physical Specifications

---

**Table 6: SSG 5 Physical Specifications**

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

### Electrical Specifications

---

**Table 7: SSG 5 Electrical Specifications**

Item	Specification
DC input voltage	12 V
DC system current rating	3-4 Amps

### Environmental Tolerance

---

**Table 8: 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%, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Non-operating storage temperature in shipping carton: -40°F (-40°C) to 158°F (70°C)

## Certifications

---

### **Safety**

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 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 Power Line Harmonics
- EN-61000-4-2 ESD
- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

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

ETSI EN-3000386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements; (equipment category-Other than telecommunication centers)



## Connectors

---

Table 9 lists the RJ-45 connector pinouts for the Console and Modem ports:

**Table 9: Console and Modem Port Connector Pinouts**

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



## Appendix 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 Ethernet Interface Window” on page 53
5. “ISDN Interface Windows” on page 54
6. “V.92 Modem Interface Window” on page 56
7. “Untrust Zone (Ethernet0/0 Interface) Window” on page 57
8. “DMZ Zone (Ethernet0/1 Interface) Window” on page 58
9. “Trust Zone (Ethernet0/2 Interface) Window” on page 58
10. “Wireless Interface (wireless0/0) in Trust Zone Window” on page 59
11. “Interface Summary Window” on page 60
12. “Physical Ethernet DHCP Interface Window” on page 60
13. “Wireless DHCP Interface Window” on page 61
14. “Confirmation Window” on page 61

## 1. Rapid Deployment Window

**Figure 13: Rapid Deployment Window**

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

If you want to bypass the 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 configuration wizard, select the first option, then click **Next**. The ICW welcome screen appears. Click **Next**. The Administrator Login window appears.

## 2. Administrator Login Window

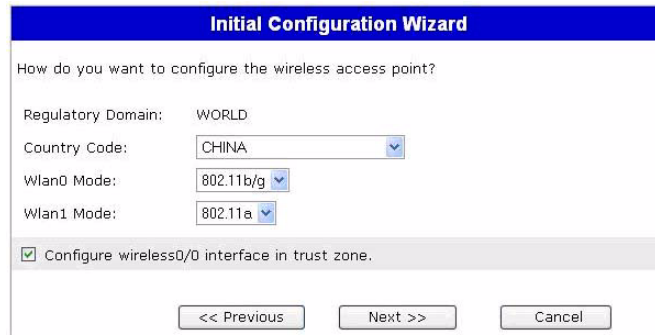
Enter a new administrator login name and password, then Click **Next**.

**Figure 14: Admin Login Window**

### 3. WLAN Access Point Window

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

**Figure 15: Country Code Window**



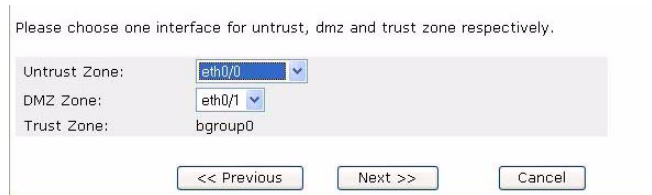
The image shows a screenshot of the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. The main content area has a light gray background and contains the following text and controls:

- Question: 'How do you want to configure the wireless access point?'
- Regulatory Domain: 'WORLD' (text field)
- Country Code: 'CHINA' (dropdown menu)
- Wlan0 Mode: '802.11b/g' (dropdown menu)
- Wlan1 Mode: '802.11a' (dropdown menu)
- Checkbox: 'Configure wireless0/0 interface in trust zone.' (checked)
- Buttons: '<< Previous', 'Next >>', and 'Cancel'.

### 4. Physical Ethernet Interface Window

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

**Figure 16: Ethernet Interface Configuration Window**



The image shows a screenshot of the 'Ethernet Interface Configuration Window'. The title bar is light gray with the text 'Please choose one interface for untrust, dmz and trust zone respectively.'. The main content area has a light gray background and contains the following text and controls:

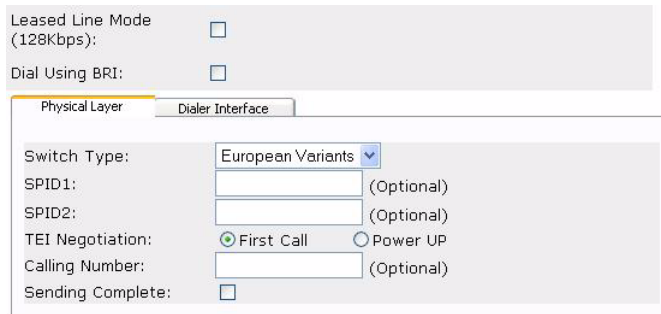
- Text: 'Please choose one interface for untrust, dmz and trust zone respectively.'
- Untrust Zone: 'eth0/0' (dropdown menu)
- DMZ Zone: 'eth0/1' (dropdown menu)
- Trust Zone: 'bgroup0' (text field)
- Buttons: '<< Previous', 'Next >>', and 'Cancel'.

After binding an interface to a zone, you can configure the interface. The configuration windows displayed after this point are dependent 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 17: ISDN Physical Layer Tab Window**



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

Field	Description
Switch Type	Sets the service provider switch type: <ul style="list-style-type: none"> <li>■ att5e - At&amp;T 5ESS</li> <li>■ ntdms100 - Nortel DMS 100</li> <li>■ ins-net - NTT INS-Net</li> <li>■ etsi - European variants</li> <li>■ ni1 - National ISDN-1</li> </ul>
SPID1	Service Provider ID, usually a seven-digit telephone number with some optional numbers. Only the DMS-100 and 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 complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

If you have the ISDN mini PIM installed on your device, you will see the Leased Line Mode and Dial Using BRI checkboxes. Selecting Leased Line Mode or Dial Using BRI displays a window similar to the following:

**Figure 18: Leased-Line and Dial Using BRI Tabs Window**

**Table 11: Field Descriptions for Leased-Line and Dial Using BRI Options**

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 19: V.92 Modem Interface Window**

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

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

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



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

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

**Figure 20: ethernet0/0 Interface Window**

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

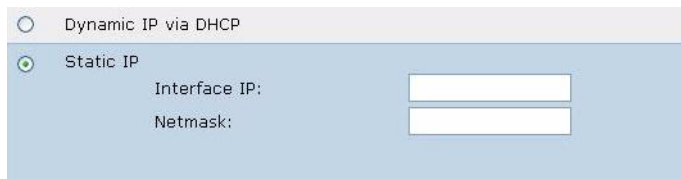
**Table 13: Field Descriptions for Ethernet0/0 Interface**

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

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

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

**Figure 21: Ethernet0/1 Interface Window**



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

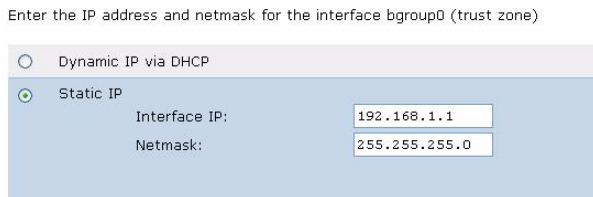
Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the DMZ zone interface from an ISP.
Static IP	Assigns a unique and fixed IP address to the DMZ zone interface. Enter the DMZ zone interface IP and netmask.

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

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

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

**Figure 22: Trust Zone (Ethernet0/2 Interface) Window**



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

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

## 10. Wireless Interface (wireless0/0) in 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 23: Wireless0/0 Interface Window**

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

Field	Description
Wlan Mode	Sets the WLAN radio mode: <ul style="list-style-type: none"> <li>■ 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 wireless connectivity. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64 text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Standard (AES) encryption type for this option, or select <b>Auto</b> to allow either option. <ul style="list-style-type: none"> <li>■ WPA2 Pre-Shared Key</li> <li>■ WPA2 Auto Pre-Shared Key</li> </ul> </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. Check your interface configuration, then click **Next** when ready to proceed. The Physical Ethernet DHCP Interface window appears.

## 11. Interface Summary Window

Before proceeding further, review the following interface settings.

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

```

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

Click Next to enter other configuration

<< Previous    Next >>    Cancel

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

## 12. Physical Ethernet DHCP Interface Window

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

Yes

IP Address Range Start   

End   

DNS Server 1    (optional)   

DNS Server 2    (optional)   

No

<< Previous    Next >>    Cancel

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

### 13. Wireless DHCP Interface Window

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

Yes  
 IP Address Range Start   
 End   
 DNS Server 1 (optional)   
 DNS Server 2 (optional)

No

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

### 14. Confirmation Window

Before proceeding further, review the following all device settings.

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

```

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

Click Next to save CLI into device.



# Index

## B

backup interface to Untrust zone ..... 32

## C

cables

    basic network connections ..... 20

chassis grounding ..... 15

configuration

    admin name and password ..... 29

    administrative access ..... 31

    backup untrust interface ..... 32

    bridge groups (bgroup) ..... 30

    date and time ..... 30

    default route ..... 32

    host and domain name ..... 31

    management address ..... 32

    management services ..... 31

    USB ..... 15

    wireless and ethernet combined ..... 36

    wireless authentication and encryption ..... 37

    wireless example ..... 35

connection

    basic network ..... 20

## D

default ip addresses ..... 28

## G

grounding ..... 15

## I

installation

    chassis grounding ..... 15

## M

management services ..... 31

managing

    through a console ..... 24

    through a Telnet connection ..... 26

    through the WebUI ..... 25

memory upgrade procedure ..... 43

mounting installation

    wall-mount ..... 18

## R

reset pinhole, using ..... 41

## U

Untrust zone, configuring backup interface ..... 32

## W

Wireless

    antennae ..... 22

    using the default interface ..... 22

