JUNIPer
NETWORKS

Engineering
Simplicity

SRX100 Services Gateway Hardware Guide
for B and H Model Numbers

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

4 Maintaining and Troubleshooting Components

5 Replacing Components

About the Documentation

IN THIS SECTION

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX100 Services Gateway (B and H model numbers). After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example.* In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   system {
      scripts {
         commit {
            file ex-script.xsl;
         }
      }
   }
   interfaces {
      fxp0 {
         disable;
         unit 0 {
            family inet {
               address 10.0.0.1/24;
            }
         }
      }
   }
   ```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

   ```
   [edit]
   user@host# load merge /var/tmp/ex-script.conf
   load complete
   ```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

   For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

   ```
   commit {
       file ex-script-snippet.xsl; }
   ```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

   ```
   [edit]
   user@host# edit system scripts
   [edit system scripts]
   ```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

   ```
   [edit system scripts]
   user@host# load merge relative /var/tmp/ex-script-snippet.conf
   load complete
   ```

For more information about the **load** command, see CLI Explorer.

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	user@host> **show chassis alarms** No alarms currently active
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** (***string1*** | ***string2*** | ***string3***)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [** ***community-ids*** **]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		    route default {
		      nexthop *address*;
		      retain;
		    }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

GUI Conventions

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

• Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:
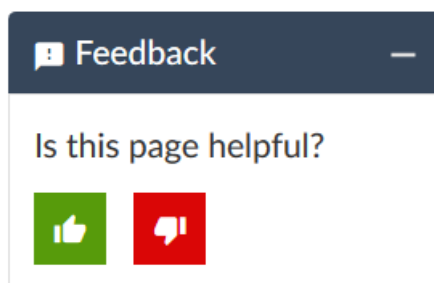
  • Click the thumbs-up icon if the information on the page was helpful to you.

  • Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

• E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales 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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.

- Product warranties—For product warranty information, visit https://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: https://www.juniper.net/customers/support/

- Search for known bugs: https://prsearch.juniper.net/

- Find product documentation: https://www.juniper.net/documentation/

- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/

- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/

- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/

- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.

- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1
PART

Overview

CHAPTER 1

System Overview

IN THIS CHAPTER

SRX100 Services Gateway Description

IN THIS SECTION

This topic includes the following sections:

About the SRX100 Services Gateway

The Juniper Networks SRX100 Services Gateway offers features that provide complete functionality and flexibility for delivering secure Internet and intranet access. The services gateway offers stable, reliable, and efficient IP routing in addition to switching support and LAN connectivity. The device provides IP Security (IPsec), virtual private network (VPN), and firewall services for small and medium-sized companies and enterprise branch and remote offices. The SRX100 Services Gateway can be connected directly to traditional private networks such as leased lines, Frame Relay, or Multi Protocol Label Switching (MPLS) or to the public Internet.

The SRX100 Services Gateway runs the Junos operating system (Junos OS).

SRX100 Services Gateway Models

The following are the two models of the SRX100 Services Gateway available with 1 GB memory. For information on the models with 2 GB memory, see SRX100 Services Gateway Hardware Guide for H2 Model Numbers.

Table 3: SRX100 Services Gateway Models

Product Name	Device Type	Model Number
SRX100 Services Gateway	Low Memory	SRX100B
SRX100 Services Gateway	High Memory	SRX100H

NOTE: You can upgrade from an SRX100 Services Gateway Low Memory version to a High Memory version through a license key. You need not order a separate High Memory device.

NOTE: SRX100H model provides additional security features such as Unified Threat Management (UTM), which consists of IPS antispam, antivirus, and Web filtering.

NOTE: The SRX100 Services Gateway High Memory model ships with a license key.

All SRX100 Services Gateways run the Junos OS.

Accessing the SRX100 Services Gateway

Two user interfaces are available for monitoring, configuring, troubleshooting, and managing the SRX100 Services Gateway:

- J-Web interface: Web-based graphical interface that allows you to operate a services gateway without commands. The J-Web interface provides access to all Junos OS functionality and features.
- Junos OS command-line interface (CLI): Juniper Networks command shell that runs on top of a UNIX-based operating system kernel. The CLI is a straightforward command interface. On a single line, you type commands that are executed when you press the Enter key. The CLI provides command Help and command completion.

SRX100 Services Gateway Features and Functions

The SRX100 Services Gateway is a security optimized, fixed processing system that provides the following features for the Low Memory and High Memory models listed in Table 4 on page 4. For information on the models with 2 GB memory, see SRX100 Services Gateway Hardware Guide for H2 Model Numbers.

Table 4: SRX100 Services Gateway Hardware Features

Features	SRX100 Services Gateway Low Memory	SRX100 Services Gateway High Memory
DDR Memory	512 MB (software upgradable to High Memory through a license key)	1 GB
Power supply adapter	30 watts	30 watts
AC input voltage	100 to 240 VAC	100 to 240 VAC
Fast Ethernet ports	8	8
Console port	1	1
USB port	1	1
LEDs	4	4
NAND flash	1 GB	1 GB

For more details on Junos OS features and licenses for the SRX100 Services Gateway, see the *Junos OS Administration Guide for Security Devices*.

For more information on upgrading an SRX100 Services Gateway Low Memory to High Memory, see "Upgrading the SRX100 Services Gateway Low Memory Version to a High Memory Version" on page 92.

RELATED DOCUMENTATION

CHAPTER 2

Hardware Component Overview

IN THIS CHAPTER

SRX100 Services Gateway LEDs

IN THIS SECTION

This topic includes the following sections:

SRX100 Services Gateway Front Panel LEDs

illustrates the front panel LEDs of the SRX100 Services Gateway.

> **NOTE:** The numbers in correspond to the numbers in .

Figure 1: SRX100 Services Gateway Front Panel LEDs
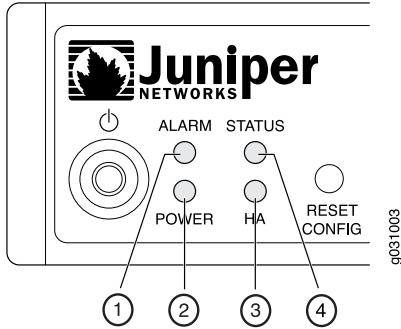
lists the LED indicators on the SRX100 Services Gateway front panel.

Table 5: SRX100 Services Gateway Front Panel LEDs

Number	Component	Description	Usage
1	Alarm LED	The Alarm LED has the following indicator colors: • Solid red indicates a major alarm. • Solid amber indicates a minor alarm. • Off indicates that there are currently no alarms.	The Alarm LED can be used to gather information on major or minor alarms or to determine if the device is functioning normally.
2	Power LED	The Power LED has the following indicator colors: • Solid green indicates that the device is functioning normally. • Solid amber indicates that the power button has been pressed and quickly released. The device is gracefully shutting down. • Off indicates that the device is not receiving power.	The Power LED can be used to determine if the device is receiving power.

Table 5: SRX100 Services Gateway Front Panel LEDs *(continued)*

Number	Component	Description	Usage
3	HA LED	The HA LED has the following indicator colors: • Solid green indicates that all chassis clustering links are available. • Solid red indicates that the chassis clustering links are not working as expected. • Solid amber indicates that some chassis clustering links are not working as expected. • Off indicates that chassis clustering is not enabled.	The HA LED can be used to determine if chassis clustering is enabled on the device.
4	Status LED	The Status LED has the following indicator colors: • Solid green indicates that the device is functioning normally. • Solid amber indicates that the device is starting up. • Solid red indicates that an error is detected in the device.	The Status LED can be used to determine whether the device is starting up, is functioning normally, or has failed.

SRX100 Services Gateway Ethernet Port LEDs

On the SRX100 Services Gateway, each Fast Ethernet port has one functional LED on the left side that indicates Link and Activity. In , this LED is marked as 1.

Figure 2: SRX100 Services Gateway Ethernet Port LEDs
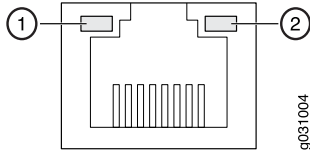
The Table 6 on page 9 applies only to the TX/RX/LINK LED marked 1. Table 6 on page 9 describes the states of this LED.

Table 6: SRX100 Services Gateway Built-In Ethernet Port LEDs

Function	Color	State	Description
TX/RX/LINK	Green	Blinking	Link is active. Data communication is taking place.
		Steady	Link is active. No data communication is taking place.
	Unlit	Off	Link is inactive.

> **NOTE:** The LED marked as 2 in Figure 2 on page 9 is not functional in this release.

RELATED DOCUMENTATION

SRX100 Services Gateway Power Supply

The power supply for the SRX100 Services Gateway is external. You must use the power supply adapter provided by Juniper Networks to provide power to the services gateway.

RELATED DOCUMENTATION

SRX100 Services Gateway Boot Devices and Dual-Root Partitioning Scheme

IN THIS SECTION

This topic includes the following sections:

Boot Devices

The SRX100 Services Gateway can boot from the following storage media (in the order of priority):

- Internal NAND Flash (default; always present)

- USB storage key (alternate)

Dual-Root Partitioning Scheme

Dual-root partitions allow the SRX100 Services Gateways to remain functional if there is file system corruption and facilitate easy recovery of the corrupted file system.

The dual-root partitioning scheme keeps the primary and backup Junos OS images in two independently bootable root partitions. If the primary root partition becomes corrupted, the system will be able to boot from the backup Junos OS image located in the other root partition and remain fully functional.

When the SRX100 Services Gateway powers up, it tries to boot the Junos OS from the default storage media. If the device fails to boot from the default storage media, it tries to boot from the alternate storage media. With the dual-root partitioning scheme, the SRX100 Services Gateway first tries to boot the Junos OS from the primary root partition and then from the backup root partition on the default storage media. If both primary and backup root partitions of a media fail to boot, then the device tries to boot from the next available type of storage media. The SRX100 Services Gateway remains fully functional even if it boots the Junos OS from the backup root partition of storage media.

NOTE: SRX Series devices that ship from the factory with Junos OS Release 10.0 are formatted with the dual-root partitioning scheme.

The SRX100 Services Gateways that are running Junos OS Release 9.6 or earlier use the single-root partitioning scheme. While upgrading these devices to Junos OS Release 10.0, you can choose to format the storage media with dual-root partitions (strongly recommended) or retain the existing single-root partitioning.

For instructions on upgrading to Junos OS Release 10.0, see the following topics:

- Initial Configuration for Security Devices

- Monitoring and Troubleshooting for Security Devices

RELATED DOCUMENTATION

Installation Overview for the SRX100 Services Gateway | 36

SRX100 Services Gateway Software Configuration Overview | 65

CHAPTER 3

Chassis Description

SRX100 Services Gateway Front Panel and Back Panel Views

This topic contains views of the front and back panels of the SRX100 Services Gateway. This topic includes the following sections:

SRX100 Services Gateway Front Panel

shows the front panel of the SRX100 Services Gateway.

Figure 3: SRX100 Services Gateway Front Panel
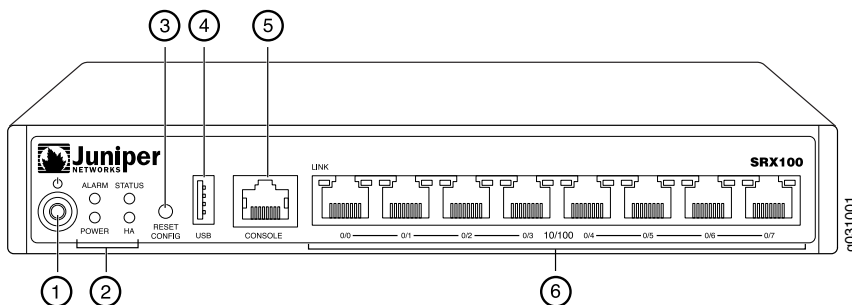
lists the front panel components of the services gateway.

Table 7: SRX100 Services Gateway Front Panel Components

Number	Component
1	Power button
2	LEDs: Alarm, Status, Power, HA
3	Reset Config button
4	Universal serial bus (USB) port
5	Console port
6	Fast Ethernet ports

For more information on the front panel components, see the following topics:

- SRX100 Services Gateway Built-In Interfaces on page 14
- SRX100 Services Gateway LEDs on page 6
- SRX100 Services Gateway Boot Devices and Dual-Root Partitioning Scheme on page 10

SRX100 Services Gateway Back Panel

illustrates the back panel of the SRX100 Services Gateway.

Figure 4: SRX100 Services Gateway Back Panel
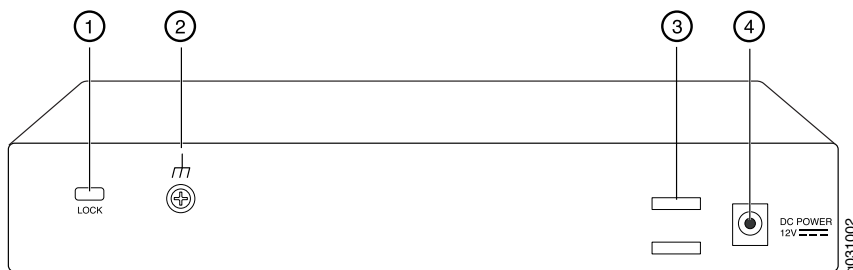
lists the components available on the back panel of the SRX100 Services Gateway.

Table 8: SRX100 Services Gateway Back Panel

Number	Component
1	Lock
2	Grounding point
3	Cable tie holder
4	Power supply point

NOTE: The cable tie holder provides support for holding the power cord on the power supply point.

The lock provides the option to lock and secure the device to the installation site.

RELATED DOCUMENTATION

SRX100 Services Gateway Built-In Interfaces

Table 9 on page 15 summarizes the interface ports supported on the SRX100 Services Gateway.

Table 9: SRX100 Services Gateway Built-In Hardware Interfaces

Interface Type	Specifications	Description
Fast Ethernet	The Fast Ethernet ports: • Consist of eight fixed ports • Are labeled as port 0/0 to port 0/7 on the front panel • Provide link speeds of 10/100 Mbps • Operate in full-duplex and half-duplex modes • Support flow control • Support autonegotiation • Support autosensing	The Fast Ethernet ports can be used: • To provide LAN connectivity to hubs, switches, local servers, and workstations. • To forward incoming data packets to the device. • To receive outgoing data packets from the device.

Universal Serial Bus (USB)	The USB port:
	
	• Consists of one port
	• Supports the following modes:
	  • Full speed
	  • High speed
	• Complies with USB revision 2.0
		The USB port can be used:
		
		• To support a USB storage device that functions as a secondary boot device in case of internal flash failure on startup, if the USB storage device is installed and configured
		
		NOTE: You must install and configure the USB storage device on the USB port to use it as secondary boot device. Additionally, the USB device must have Junos installed.
		
		• To provide the USB interfaces that are used to communicate with many types of Juniper-supported USB storage devices

Console	The console port: • Consists of one port • Uses an RJ-45 serial cable connector • Supports the RS-232 (EIA-232) standard	The console port can be used: • To provide the console interface. • To function as a management port to log into a device directly. • To configure the device using the CLI.

> **NOTE:** The Reset Config button is used to remove the current configuration and reset the device to the default configuration.
>
> The button is recessed in the front panel to prevent it from being pressed accidentally.

> ⚠️ **CAUTION:** Pressing and holding the Reset Config button for 15 seconds or more deletes all configurations on the device and loads and commits the factory configuration.

RELATED DOCUMENTATION

2
PART

Site Planning and Specifications

CHAPTER 4

Planning and Preparing the Site

IN THIS CHAPTER

Site Preparation Checklist for the SRX100 Services Gateway

The checklist in Table 10 on page 18 summarizes the tasks you need to perform when preparing a site for installing the SRX100 Services Gateway.

Table 10: Site Preparation Checklist for Services Gateway Installation

Item or Task	Additional Information	Performed By	Date	Notes
Environment				
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX100 Services Gateway Specifications" on page 21			
Power				

Table 10: Site Preparation Checklist for Services Gateway Installation *(continued)*

Item or Task	Additional Information	Performed By	Date	Notes
• Measure the distance between the external power sources and the device installation site. • Locate sites for connection of system grounding. • Calculate the power consumption and requirements.	"SRX100 Services Gateway Site Electrical Wiring Guidelines" on page 27 "SRX100 Services Gateway Power Specifications and Requirements" on page 29			
Rack Requirements				
Verify that your rack meets the minimum requirements.	"SRX100 Services Gateway Rack Requirements" on page 24			
Rack Installation				
• Plan the rack location, including required space clearances. • Secure the rack to the floor and building structure.	"Preparing the SRX100 Services Gateway for Rack-Mount Installation" on page 43			
Cabinet Requirements				
• Verify that your cabinet meets the minimum requirements. • Plan the cabinet location, including required space clearances.	"SRX100 Services Gateway Cabinet Requirements" on page 23			
Wall Installation				

Table 10: Site Preparation Checklist for Services Gateway Installation *(continued)*

Item or Task	Additional Information	Performed By	Date	Notes
• Verify that the area selected meets the minimum requirements. • Verify that you have the required hardware to proceed with the installation.	"Preparing the SRX100 Services Gateway for Wall-Mount Installation" on page 45			
Desktop Installation				
• Verify that the area selected meets the minimum requirements. • Plan the installation location, including required space clearances and airflow requirements.	"Preparing the SRX100 Services Gateway for Desk-Mount Installation" on page 44			
Cables				
• Acquire cables and connectors. • Review the maximum distance allowed for each cable. Choose the length of cable based on the distance between the hardware components being connected. • Plan the cable routing and management.	"Interface Cable and Wire Specifications for the SRX100 Services Gateway" on page 31			

RELATED DOCUMENTATION

General Site Guidelines for Installing the SRX100 Services Gateway

Keep the following precautions in mind to help you plan an acceptable operating environment for your SRX100 Services Gateway and avoid environmentally caused equipment failures:

- For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted. Allow sufficient clearance between the front and back of the chassis and adjacent equipment. Ensure that there is adequate circulation in the installation location.

- Follow the ESD procedures to avoid damaging equipment. Static discharge can cause components to fail completely or intermittently over time.

  NOTE: The SRX100 Services Gateway does not include a fan and does not generate any acoustic noise.

RELATED DOCUMENTATION

SRX100 Services Gateway Specifications

The SRX100 Services Gateway chassis is a rigid sheet metal structure that houses all the other hardware components (see Figure 5 on page 22).

Table 11 on page 22 provides information on the physical specifications of the device.

Table 11: SRX100 Services Gateway Specifications

Specification	Value
Chassis height	1.38 in. (35 mm)
Chassis width	8.5 in. (216 mm)
Chassis depth	5.79 in. (147 mm)
Chassis weight	1.86 lb (844 g)
Average power consumption	• SRX100 Services Gateway Low Memory model: 10 watts • SRX100 Services Gateway High Memory model: 10 watts
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (+40°C) Nonoperating storage temperature in shipping container: –40°F (–40°C) to 158°F (70°C) **NOTE:** The SRX100 Services Gateway operating temperature is 35°C when installed in a rack.
Maximum thermal output	The maximum thermal values for the two models of services gateways are as follows: • Low Memory — AC power: 80 BTU/hour (21.5 W) • High Memory — AC power: 80 BTU/hour (21.5 W) **NOTE:** These specifications are estimates and subject to change.

Figure 5: SRX100 Services Gateway
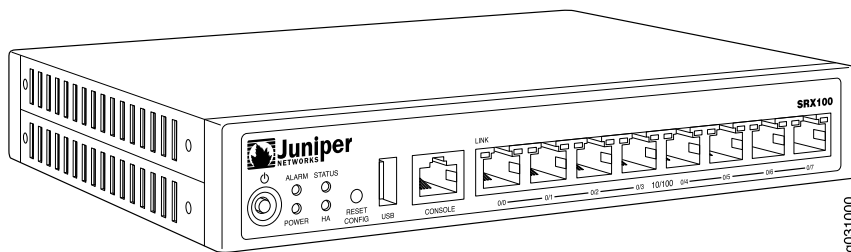
> **CAUTION:** Before removing or installing components of a functioning services gateway, attach an electrostatic discharge (ESD) strap to an ESD point and place the other end of the strap around your bare wrist. Failure to use an ESD strap could result in damage to the services gateway.

SRX100 Services Gateway Cabinet Requirements

The SRX100 Services Gateway can be installed in a standard 31.5 in. (800 mm) or larger enclosed cabinet. Table 12 on page 23 provides the details on cabinet size, clearance, and airflow requirements.

Table 12: SRX100 Services Gateway Cabinet Requirements

Cabinet Requirements	Specifications
Cabinet size	19 in. (48.3 cm) as defined in *Cabinets, Racks, Panels, and Associated Equipment* (document number EIA-310–D) published by the Electronics Industry Association (http://www.eia.org). You can mount the gateway horizontally in the cabinet.
Clearance requirements	• The cabinet is at least 1 U (1.75 in. or 4.5 cm) high. • The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.3 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting brackets. • The minimum total clearance inside the cabinet is 30.7 in. (78 cm) between the inside of the front door and the inside of the rear door. **NOTE:** The holes for the mounting brackets chassis are spaced 1.25 in. (3.2 cm) apart, measured from the center of the hole.

Table 12: SRX100 Services Gateway Cabinet Requirements *(continued)*

Cabinet Requirements	Specifications
Cabinet airflow requirements	• Ensure sufficient ventilation through the cabinet is sufficient to prevent overheating. • Ensure adequate cool air supply to dissipate the thermal output of the device. • Install the device as close as possible to the front of the cabinet so that the cable management system clears the inside of the front door. Installing the chassis close to the front of the cabinet maximizes the clearance in the rear of the cabinet for critical airflow. • Route and dress all cables to minimize the blockage of airflow to and from the chassis. NOTE: A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

RELATED DOCUMENTATION

SRX100 Services Gateway Rack Requirements

The services gateway can be installed in a rack. Many types of racks are acceptable, including front-mount racks and four-post (telco) racks.

> NOTE: The services gateway cannot be center mounted in a rack.

Table 13 on page 24 provides the details of requirements for rack size, clearance, airflow, spacing of mounting brackets and flange holes, and connecting to the building structure.

Table 13: Rack Requirements for the Services Gateway

Rack Requirement	Specifications
Size	A 19 in. (48.3 cm) rack as defined in *Cabinets, Racks, Panels, and Associated Equipment* (document number EIA-310-D) published by the Electronics Industry Association (http://www.eia.org).

Table 13: Rack Requirements for the Services Gateway *(continued)*

Rack Requirement	Specifications
Clearance	• The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.3 cm). • The front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting ears. • Maximum permissible ambient temperature when two devices are placed side by side in a 19 in. rack is 40° C.
Spacing of Mounting Bracket and Flange Holes	• The holes within each rack set are spaced at 1 U [1.75 in. (4.5 cm)]. The device can be mounted in any rack that provides holes or hole patterns spaced at 1-U [1.75 in. (4.5 cm)] increments. • The mounting brackets and front-mount flanges used to attach the chassis to a rack are designed to fasten to holes spaced at rack distances of 1 U (1.75 in.). • The mounting holes in the mounting brackets provided with the device are spaced 1.25 in. (3.2 cm) apart (top and bottom mounting hole).
Connecting to the Building Structure	Always secure the rack in which you are installing the services gateway to the structure of the building. If your geographical area is subject to earthquakes, bolt the rack to the floor. For maximum stability, also secure the rack to ceiling brackets.

RELATED DOCUMENTATION

Clearance Requirements for Airflow and Hardware Maintenance of the SRX100 Services Gateway

When planning the installation site for the SRX100 Services Gateway, you need to allow sufficient clearance around the device.

When planning the installation site for the services gateway, consider the following:

• For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted.

- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the device. Allow at least 24 in. (61 cm) both in front of and behind the device.

- If you are mounting the device in a rack with other equipment, or if you are placing it on the desktop near other equipment, ensure that the exhaust from other equipment does not blow into the intake vents of the chassis.

Table 14 on page 26 provides information on the clearance requirements for maintaining the optimum airflow and the distances for facilitating easy maintenance of the device.

Table 14: Clearance Requirements for the SRX100 Services Gateway

Location	Recommended Clearance	Requirement for Clearance
Front of the chassis	2.5 in. (6.35 cm)	Space for service personnel to remove and install hardware components
Rear of the chassis	2.5 in. (6.35 cm)	Space for service personnel to remove and install hardware components
Between front-mounting flange and rack or cabinet edge	2.5 in. (6.35 cm)	Space for cable management and organization
Between side of the chassis and any non-heat-producing surface such as a wall or cabinet side	2.5 in. (6.35 cm)	Space for the cooling system to function properly and to maintain unrestricted airflow around the chassis
Between side of the chassis and devices that have fans or blowers	0.4 in. (1 cm)	Space for the cooling system to function properly and to maintain unrestricted airflow around the chassis

NOTE: The air vents are provided on the sides of the chassis for the SRX100 Services Gateway.

RELATED DOCUMENTATION

General Site Guidelines for Installing the SRX100 Services Gateway | **21**

SRX100 Services Gateway Cabinet Requirements | **23**

SRX100 Services Gateway Rack Requirements | **24**

CHAPTER 5

Power Requirements and Specifications

IN THIS CHAPTER

SRX100 Services Gateway Site Electrical Wiring Guidelines

Table 15 on page 28 describes the factors you must consider while planning the electrical wiring for the services gateway at your site.

> ⚠ **CAUTION:** It is particularly important to provide a properly grounded and shielded environment and to use electrical surge-suppression devices.

> ⚠ **CAUTION:** For devices with AC power supplies, an external surge protective device (SPD) must be used at the AC power source.

Table 15: Site Electrical Wiring Guidelines for the Services Gateway

Site Wiring Factor	Guideline

Signaling Limitations	To ensure that signaling functions optimally:
	
	• Install wires correctly.
	
	  Improperly installed wires can emit radio interference.
	
	• Do not exceed the recommended distances or pass wires between buildings.
	
	  The potential for damage from lightning strikes increases if wires exceed recommended distances or if wires pass between buildings.
	
	• Shield all conductors.
	
	  The electromagnetic pulse (EMP) caused by lightning can damage unshielded conductors and destroy electronic devices.

Radio Frequency Interference (RFI)	To reduce or eliminate the emission of RFI from your site wiring: • Use twisted-pair cable with a good distribution of grounding conductors. • Use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable, if you must exceed the recommended distances.
Electromagnetic Compatibility (EMC)	Provide a properly grounded and shielded environment and use electrical surge-suppression devices. Strong sources of electromagnetic interference (EMI) can cause the following damage: • Destroy the signal drivers and receivers in the device • Conduct power surges over the lines into the equipment, resulting in an electrical hazard **NOTE:** If your site is susceptible to problems with EMC, particularly from lightning or radio transmitters, you may want to seek expert advice.

⚠️ **CAUTION:** To comply with intrabuilding lightning/surge requirements, the intrabuilding wiring must be shielded. The shielding for the wiring must be grounded at both ends.

RELATED DOCUMENTATION

General Site Guidelines for Installing the SRX100 Services Gateway | **21**

Monitoring the SRX100 Services Gateway Power System | **103**

SRX100 Services Gateway Electrical and Power Requirements

This topic provides information on the factors you must consider while planning the electrical wiring and power availability at your site. These requirements cover the following areas:

- Power specifications and requirements for the device

- Electrical wiring guidelines for the device installation site

- Power, connection, and power cord specifications for the device

- Grounding guidelines and specifications for the device

RELATED DOCUMENTATION

SRX100 Services Gateway Power Specifications and Requirements

The AC power system electrical specifications for the SRX100 Services Gateway are listed in .

Table 16: Power System Electrical Specifications for the SRX100 Services Gateway

Power Requirement	Specification
AC input voltage	100 to 240 VAC
AC input line frequency	50 to 60 Hz
AC system current rating	1 A maximum

> **WARNING:** The AC power cord for the services gateway is intended for use with the device only and not for any other use.

RELATED DOCUMENTATION

CHAPTER 6

Cable Specifications and Pinouts

IN THIS CHAPTER

Interface Cable and Wire Specifications for the SRX100 Services Gateway

Table 17 on page 31 lists the specifications for the cables that connect to ports.

Table 17: Cable and Wire Specifications for Ports

Port	Cable Specification	Cable/Wire Required	Maximum Length	Device Receptacle
Console port	RS-232 (EIA-232) serial cable	One 6-ft (1.83-m) length with DB-9/RJ-45 connectors	6 ft (1.83 m)	RJ-45
Ethernet port	CAT-5e (Category 5) cable or equivalent suitable for 100BASE-T operation	One 15-ft (4.57-m) length with RJ-45/RJ-45 connectors	328 ft (100 m)	RJ-45

RELATED DOCUMENTATION

RJ-45 Connector Pinouts for the SRX100 Services Gateway Ethernet Port

Figure 6 on page 32 shows the RJ-45 cable connector pinouts for Ethernet ports.

Figure 6: Ethernet Cable Connector (RJ-45)
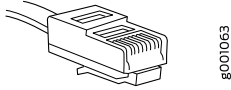
Table 18 on page 32 describes the RJ-45 connector pinouts for the Ethernet port.

Table 18: RJ-45 Connector Pinouts for the Services Gateway Ethernet Port

Pin	Signal
1	TX+
2	TX -
3	RX+
4	Termination network
5	Termination network
6	RX-
7	Termination network
8	Termination network

RELATED DOCUMENTATION

Interface Cable and Wire Specifications for the SRX100 Services Gateway | **31**

RJ-45 Connector Pinouts for the SRX100 Services Gateway Console Port | **32**

RJ-45 Connector Pinouts for the SRX100 Services Gateway Console Port

Figure 7 on page 33 shows the RJ-45 connector pinouts for the console port.

Figure 7: Console Cable Connector

g003781
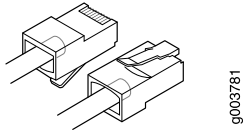
describes the RJ-45 connector pinouts for the console port.

Table 19: RJ-45 Connector Pinouts for the Services Gateway Console Port

Pin	Signal	Description
1	RTS	Request to Send
2	DTR	Data Terminal Ready
3	TXD	Transmit Data
4	Ground	Signal Ground
5	Ground	Signal Ground
6	RXD	Receive Data
7	DSR/DCD	Data Set Ready
8	CTS	Clear to Send

RELATED DOCUMENTATION

Interface Cable and Wire Specifications for the SRX100 Services Gateway | **31**

RJ-45 Connector Pinouts for the SRX100 Services Gateway Ethernet Port | **32**

3
PART

Initial Installation and Configuration

CHAPTER 7

Installation Overview

IN THIS CHAPTER

Installation Overview for the SRX100 Services Gateway

After you have prepared your installation site, you are ready to unpack and install the services gateway. It is important to proceed through the installation process in the order shown in Table 20 on page 36.

Table 20: Installation Process Order for the SRX100 Services Gateway

Steps	Process	For More Information, See
1	Review the safety guidelines.	"SRX100 Services Gateway Safety Requirements, Warnings, and Guidelines" on page 125
2	Verify that you have prepared your site for the installation of the services gateway using the checklist.	"Site Preparation Checklist for the SRX100 Services Gateway" on page 18
3	Follow the instructions for unpacking the services gateway and verify that the parts are received.	"Unpacking the SRX100 Services Gateway" on page 40
4	Prepare the services gateway for installation.	"Preparing the SRX100 Services Gateway for Rack-Mount Installation" on page 43 "Preparing the SRX100 Services Gateway for Desk-Mount Installation" on page 44 "Preparing the SRX100 Services Gateway for Wall-Mount Installation" on page 45
5	Install the services gateway.	"Installing the SRX100 Services Gateway in a Rack" on page 46 "Installing the SRX100 Services Gateway on a Desk" on page 48 "Installing the SRX100 Services Gateway on a Wall" on page 49
6	Connect cables to external devices.	"Connecting and Organizing Interface Cables to the SRX100 Services Gateway" on page 55
7	Connect the grounding cable.	"Grounding the SRX100 Services Gateway" on page 52
8	Power on the services gateway.	"Powering On and Powering Off the SRX100 Services Gateway" on page 61

Required Tools and Parts for Installing and Maintaining the SRX100 Services Gateway

Table 21 on page 37 lists the tools and parts required to install and maintain the SRX100 Services Gateway.

Table 21: Required Tools and Parts for Installing and Maintaining the SRX100 Services Gateway

Task	Tools and Parts	Related Topic
Installing the SRX100 Services Gateway	• Phillips (+) screwdriver, numbers 1 and 3 • Tie wrap	"Installing the SRX100 Services Gateway in a Rack" on page 46 "Installing the SRX100 Services Gateway on a Desk" on page 48 "Installing the SRX100 Services Gateway on a Wall" on page 49
Connecting the SRX100 Services Gateway	Electrostatic discharge (ESD) grounding wrist strap	"Connecting the SRX100 Services Gateway to the Power Supply" on page 60
Grounding the SRX100 Services Gateway	Phillips (+) screwdriver, number 1	"Grounding the SRX100 Services Gateway" on page 52
Packing the SRX100 Services Gateway	• Electrostatic bag or antistatic mat, for each component • Electrostatic discharge (ESD) grounding wrist strap	"Packing the SRX100 Services Gateway and Components for Shipment" on page 113

SRX100 Services Gateway Autoinstallation Overview

The autoinstallation process begins any time a services gateway is powered on and cannot locate a valid configuration file in the internal flash. Typically, a configuration file is unavailable when a services gateway is powered on for the first time or if the configuration file is deleted from the internal flash. The autoinstallation feature enables you to deploy multiple services gateways from a central location in the network.

If you are setting up many devices, autoinstallation can help automate the configuration process by loading configuration files onto new or existing devices automatically over the network. You can use either the J-Web interface or the CLI to configure a device for autoinstallation.

For the autoinstallation process to work, you must store one or more host-specific or default configuration files on a configuration server in the network and have a service available—typically Dynamic Host Configuration Protocol (DHCP)—to assign an IP address to the services gateway.

Autoinstallation takes place automatically when you connect an Ethernet port on a new services gateway to the network and power on the device. To simplify the process, you can explicitly enable autoinstallation on a device and specify a configuration server, an autoinstallation interface, and a protocol for IP address acquisition.

For more information about configuring autoinstallation, see the following topics:

- Installation and Upgrade Guide

- Network Monitoring and Troubleshooting

CHAPTER 8

Unpacking the Services Gateway

IN THIS CHAPTER

-
-

Unpacking the SRX100 Services Gateway

The SRX100 Services Gateway is shipped in a cardboard carton. The carton also contains an accessory box and the *SRX100 Services Gateway Quick Start*.

> **NOTE:** The device is maximally protected inside the shipping carton. Do not unpack it until you are ready to begin installation.

To unpack the SRX100 Services Gateway:

1. Open the box in which the device is shipped.

2. Verify the parts received against the lists in .

3. Store the shipping box and packing material in case you need to return or move the device at a later time.

RELATED DOCUMENTATION

Verifying Parts Received with the SRX100 Services Gateway

The SRX100 Services Gateway shipment package contains a packing list. Check the parts in the shipment against the items on the packing list. The packing list specifies the part numbers and descriptions of each part in your order.

If any part is missing, contact your Juniper Networks customer service representative.

A fully configured SRX100 Services Gateway contains the chassis with installed components, listed in Table 22 on page 41, and an accessory box, which contains the parts listed in Table 23 on page 41.

NOTE: The parts shipped with your device can vary depending on the configuration you ordered.

Table 22: Parts List for a Fully Configured SRX100 Services Gateway

Component	Quantity
Chassis, with 8xFE ports	1
Power supply adapter (30 W)	1
2-prong power cord	1
DB-9 to RJ-45 adapter, straight through, 7 ft	1

Table 23: Accessory Parts List for the SRX100 Services Gateway

Part	Quantity
Juniper Networks Product Warranty	1
End User License Agreement	1
Quick Start	1
Security Products Safety Guide	1
Juniper Compliance Form Letter	1

Table 23: Accessory Parts List for the SRX100 Services Gateway *(continued)*

Part	Quantity
Product Registration	1

> **NOTE:** The mounting kits available for rack, desk, and wall installation of the SRX100 Services Gateway must be ordered separately. Contact your Juniper Networks customer service representative for more information.

RELATED DOCUMENTATION

CHAPTER 9

Installing the Mounting Hardware

IN THIS CHAPTER

Preparing the SRX100 Services Gateway for Rack-Mount Installation

You can mount an SRX100 Services Gateway in four-post (telco) racks, enclosed cabinets, and open-frame racks.

> **NOTE:** The SRX100 Services Gateway cannot be center-mounted in racks.

Before mounting the SRX100 Services Gateway in a rack:

- Verify that the installation site meets the requirements described in the site preparation checklist.

- Verify that the racks or cabinets meet the specific requirements described in "SRX100 Services Gateway Rack Requirements" on page 24.

- Place the rack or cabinet in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure. For more information, see "Clearance Requirements for Airflow and Hardware Maintenance of the SRX100 Services Gateway" on page 25.

- Remove the services gateway chassis from the shipping carton. For unpacking instructions, see "Unpacking the SRX100 Services Gateway" on page 40.

- Verify that you have the following parts available in your rack-mounting kit for the SRX100 Services Gateway:

  - Rack-mount tray

  - Screws

> **NOTE:** The rack-mounting kit is not shipped with the device and must be ordered separately.

Preparing the SRX100 Services Gateway for Desk-Mount Installation

You can mount an SRX100 Services Gateway on a desk or other level surface horizontally or vertically. The four rubber feet attached to the chassis provide stability.

Before mounting an SRX100 Services Gateway on a desk or other level surface:

- Verify that the site meets the requirements described in the site preparation checklist.

- Place the desk in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure.

- Remove the services gateway chassis from the shipping carton. For unpacking instructions, see "Unpacking the SRX100 Services Gateway" on page 40.

- If you are mounting the device vertically on the desk, make sure that the following parts are available in your vertical desk-mounting kit for the SRX100 Services Gateway:

  - Vertical stand

  - Screws

> **NOTE:** The vertical desk-mounting kit is not shipped with the device and must be ordered separately.

Preparing the SRX100 Services Gateway for Wall-Mount Installation

You can mount an SRX100 Services Gateway on a wall. The four rubber feet attached to the chassis provide stability.

Before mounting an SRX100 Services Gateway on a wall:

- Verify that the site meets the requirements described in "Site Preparation Checklist for the SRX100 Services Gateway" on page 18.
- Remove the services gateway chassis from the shipping carton. For unpacking instructions, see "Unpacking the SRX100 Services Gateway" on page 40.
- Verify that you have the following parts available in your wall-mounting kit for the SRX100 Services Gateway:
  - Wall-mounting brackets
  - Screws

    NOTE: The wall-mounting kit is not shipped with the device and must be ordered separately.

CHAPTER 10

Installing the Services Gateway

IN THIS CHAPTER

Installing the SRX100 Services Gateway in a Rack

You can front-mount two SRX100 Services Gateways in a rack. Many types of racks are acceptable, including four-post (telco) racks, enclosed cabinets, and open-frame racks. For more information about the type of rack or cabinet the SRX100 Services Gateway can be installed into, see "SRX100 Services Gateway Rack Requirements" on page 24.

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

To install the device in a rack:

1. Position the two devices in the rack-mount tray as shown in .

Figure 8: Installing the SRX100 Services Gateway in a Rack
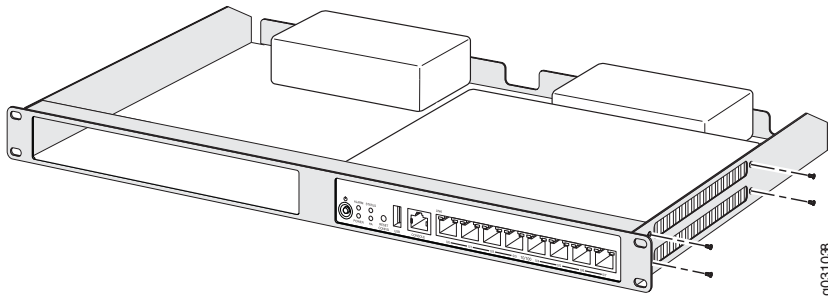
2. Use a number-1 Phillips screwdriver to install the screws that secure the device to the rack-mount tray.

3. Have one person grasp the sides of the rack-mount tray, lift it, and position it in the rack.

4. Align the bottom hole in each side of the rack-mount tray with a hole in each rack rail as shown in , making sure the rack-mount tray is level.

Figure 9: Hanging the SRX100 Services Gateway in a Rack
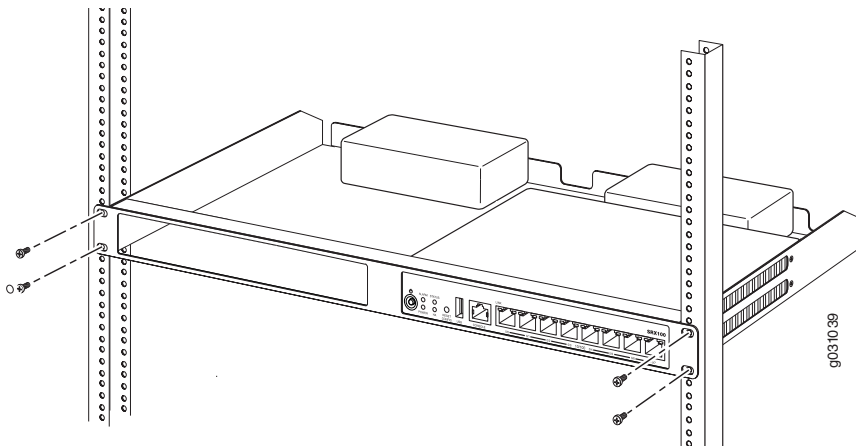
5. Have a second person install a mounting screw into each of the two aligned holes. Use a number-3 Phillips screwdriver to install the mounting screws.

6. Install the second screw in each side of the rack-mount tray.

7. Verify that the mounting screws on one side of the rack-mount tray are aligned with the mounting screws on the opposite side and that the tray is level.

> **NOTE:** The rack-mounting kit is not shipped with the device and must be ordered separately.

Installing the SRX100 Services Gateway on a Desk

You can install the SRX100 Services Gateway on a desk, table, or other level surface. The device is shipped with the rubber feet attached. The rubber feet are necessary to stabilize the device on the desk.

You can install the device in a horizontal or vertical position.

> **NOTE:** The desk-mounting kit is not shipped with the device and must be ordered separately.

Horizontal Desk Mounting

The horizontal position is the standard installation position and does not require the vertical installation kit.

To install the device in a horizontal position:

1. Make sure that the rubber feet are attached to the chassis.

2. Place the device on a desk with the Juniper Networks logo embossed on the top cover facing up.

Vertical Desk Mounting

The vertical position requires the vertical installation kit, which consists of a vertical installation stand.

To install the device in a vertical position:

1. Place the device on a flat and level surface with the Juniper Networks logo on the front panel facing up, as shown in Figure 10 on page 49.

Figure 10: Installing the SRX100 Services Gateway on a Desk
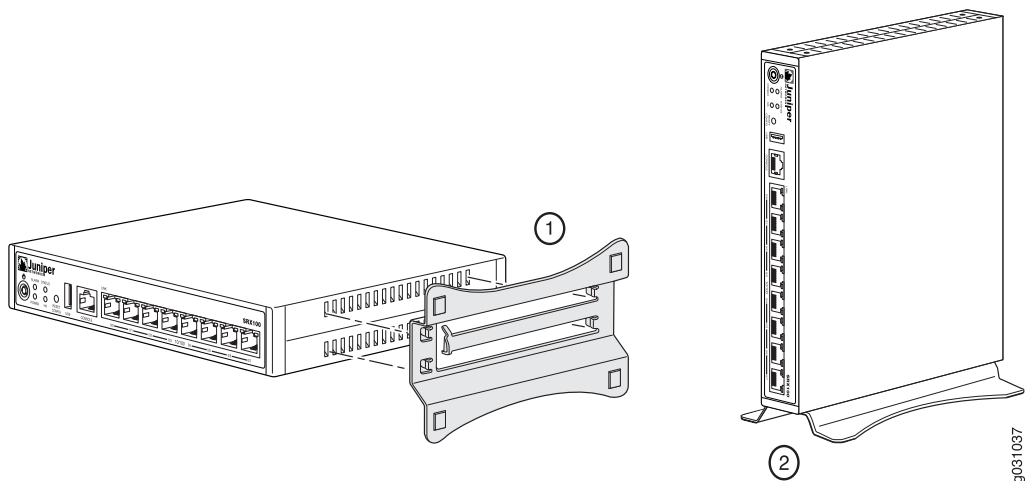
2. Attach the vertical stand to the right side of the chassis as shown in Figure 10 on page 49.

3. Place the chassis vertically on the desk with the stand resting on the desk.

Installing the SRX100 Services Gateway on a Wall

You can install the SRX100 Services Gateway on a wall. The device is shipped with the rubber feet attached. The rubber feet help stabilize the device on the wall and enhance airflow.

> **NOTE:** The wall-mounting kit is not shipped with the device and must be ordered separately.

To install the device on a wall:

1. Place the device on a flat and level surface with the Juniper Networks logo embossed on the top cover facing up.

2. Position a mounting bracket on each side of the chassis as shown in Figure 11 on page 50.

Figure 11: Installing the SRX100 Services Gateway on a Wall
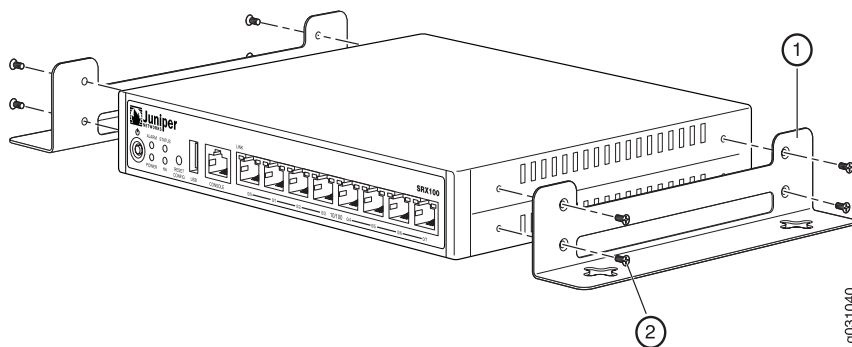
3. Use a number–1 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.

4. If you are using wall anchors to support the chassis, install two pairs of anchors on the wall with mounting brackets attached.

5. Have one person grasp the sides of the device, lift it, and position it on the wall.

6. Have a second person install two pairs of mounting screws through the bracket holes on either side of the device to secure it to the wall.

7. Verify that the mounting screws on one side are aligned with the mounting screws on the opposite side and that the device is level (see Figure 12 on page 51).

Figure 12: Hanging the SRX100 Services Gateway on a Wall
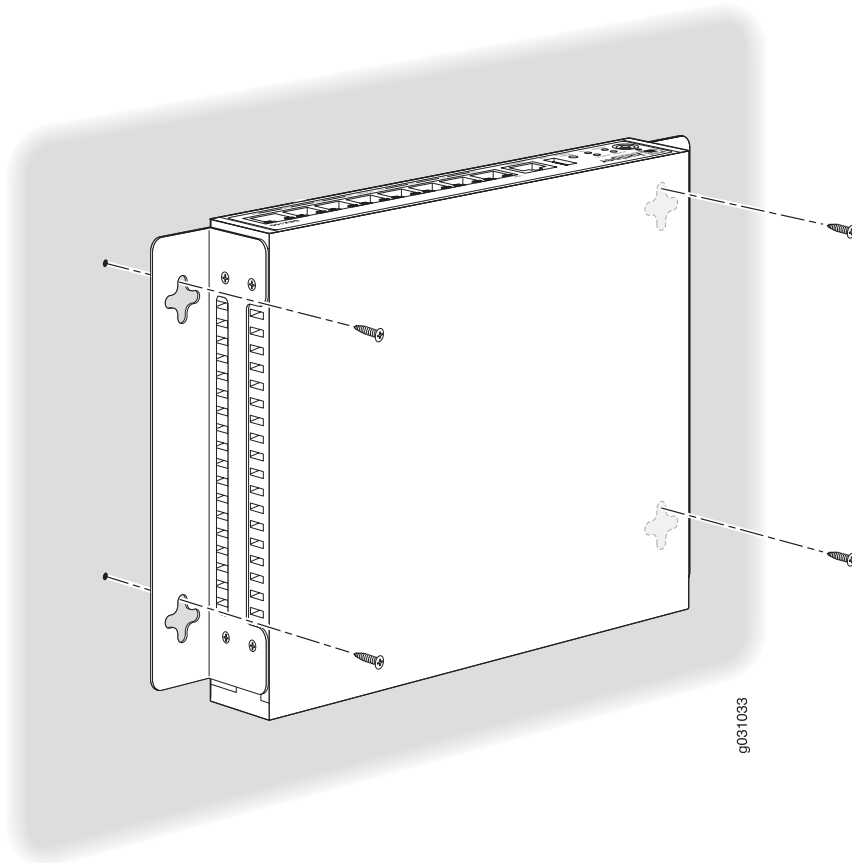
RELATED DOCUMENTATION

CHAPTER 11

Grounding the SRX100 Services Gateway

IN THIS CHAPTER

●

Grounding the SRX100 Services Gateway

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the SRX100 Services Gateway must be adequately grounded before power is connected.

illustrates how a grounding cable connects to the services gateway.

Figure 13: Grounding the SRX100 Services Gateway
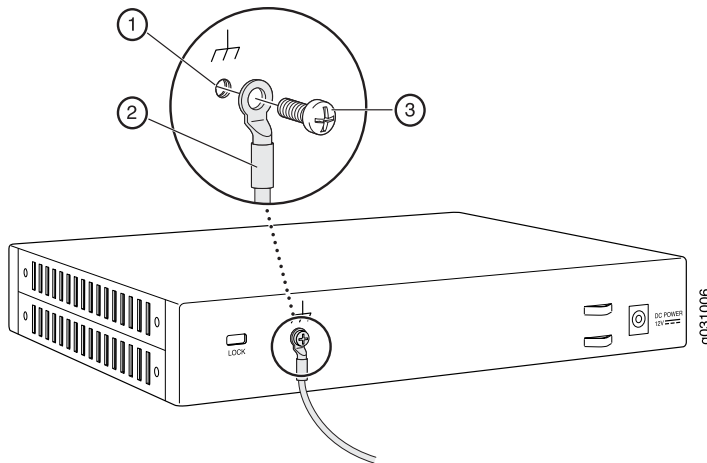
You ground the device by connecting a grounding cable to earth ground and then attaching it to the chassis grounding points using one M3 screw.

> ⚠ **CAUTION:** Before device installation begins, a licensed electrician must attach a cable lug to the grounding and power cables that you use. A cable with an incorrectly attached lug can damage the device (for example, by causing a short circuit).

Table 24 on page 53 lists the grounding components of the SRX100 Services Gateway.

Table 24: SRX100 Services Gateway Grounding Components

Number	Component
1	Grounding point on the chassis
2	Grounding lug
3	Grounding screw (M3 screw)

Table 25 on page 53 lists the specifications of the grounding cable used with the device.

Table 25: Grounding Cable Specifications for the Services Gateway

Grounding Requirement	Specification
Grounding cable	14 AWG single-strand wire cable
Amperage of grounding cable	Up to 4 A
Grounding lug	Ring-type, vinyl-insulated TV14-6R lug or equivalent

To ground the device:

1. Connect the grounding cable to a proper earth ground.

2. Verify that a licensed electrician has attached the cable lug to the grounding cable.

3. Place the grounding cable lug over the grounding point on the middle rear of the chassis.

4. Secure the grounding cable lug to the grounding point with the screw as shown in Figure 13 on page 52.

5. Dress the grounding cable and verify that it does not touch or block access to the services gateway components and that it does not drape where people could trip on it.

NOTE: The device should be permanently connected to ground during operation.

RELATED DOCUMENTATION

Connecting the SRX100 Services Gateway to External Devices

IN THIS CHAPTER

Connecting and Organizing Interface Cables to the SRX100 Services Gateway

You can connect the interfaces installed in the services gateway to various network media. Each type of interface on the services gateway uses a particular medium to transmit data. You must configure each network interface before it can operate on the device.

To connect and organize an interface cable for 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 interface faceplate.

3. 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.

RELATED DOCUMENTATION

Connecting the SRX100 Services Gateway to the Power Supply | **60**

Connecting the Modem at the SRX100 Services Gateway End

> **NOTE:** These instructions use Hayes-compatible modem commands to configure the modem. If your modem is not Hayes-compatible, refer to the documentation for your modem and enter the equivalent modem commands.

To configure the modem on the services gateway end:

1. Connect the modem to a PC or laptop computer.

2. Power on the modem.

3. From the PC or laptop computer, start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal), and select the **COM** port to which the modem is connected (for example, **COM1**).

4. Configure the port settings as shown in .

   Table 26: Port Settings for Configuring the Modem on the Services Gateway End

Port Setting	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

5. In the HyperTerminal window, enter **AT**.

An **OK** response verifies that the modem can communicate successfully with the **COM** port on the PC or laptop.

For more information on the AT commands, see Administration Guide for Security Devices.

6. Configure the modem to answer a call on the first ring by entering **ATS0=1**.

7. Configure the modem to accept modem control DTR signals by entering **AT&D1**.

8. Disable flow control by entering **AT&K0**.

9. Save modem settings by entering **AT&W**.

RELATED DOCUMENTATION

Connecting the Modem to the Console Port on the SRX100 Services Gateway

To connect the dial-up modem to the console port on the services gateway:

1. Turn off power to the services gateway.

2. Turn off power to the modem.

3. Plug one end of the Ethernet cable supplied with your services gateway into the console port on the services gateway.

4. Plug the other end of the CAT-5e cable (Ethernet cable) into the RJ-45 to DB-9 serial port adapter supplied with your services gateway.

5. Connect the serial port adapter to a separately purchased DB-9 female to DB-25 male adapter or other adapter appropriate for your modem.

6. Plug the modem adapter into the DB-25 connector on the modem.

7. Connect the modem to your telephone network.

8. Turn on the power to the modem.

9. Power on the services gateway by pressing the Power button on the front panel. Verify that the **Power** LED on the front panel turns green.

> **NOTE:** Most modems have an RS-232 DB-25 connector. You must separately purchase an adapter to connect your modem to the RJ-45 to DB-9 adapter and the Ethernet cable supplied with the services gateway.

Connecting to the CLI at the User End for the SRX100 Services Gateway

To remotely connect to the CLI through a dial-up modem connected to the console port on the services gateway:

1. Connect a modem at your remote location to a management device such as a PC or laptop computer.

2. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) on the PC or laptop computer.

3. Select the **COM** port to which the modem is connected (for example, **COM1**).

4. Configure the port settings shown in .

   Table 27: Port Settings for Connecting to the CLI at User End

Port Setting	Value
Bits per second	9600
Data bits	8

Table 27: Port Settings for Connecting to the CLI at User End *(continued)*

Port Setting	Value
Parity	None
Stop bits	1
Flow control	None

5. In the HyperTerminal window, enter **AT**.

   An **OK** response verifies that the modem can communicate successfully with the **COM** port on the PC or laptop.

   For more information on the AT commands, see Administration Guide for Security Devices.

6. Dial the modem that is connected to the console port on the services gateway by entering **ATDT** *remote-modem-number*. For example, if the number of the modem connected to the console port on the services gateway is **0013033033030**, enter **ATDT 0013033033030**.

   The services gateway login prompt appears.

7. Log in as the user **root**. No password is required at initial connection, but you must assign a root password before committing any configuration settings.

RELATED DOCUMENTATION

CHAPTER 13

Providing Power to the SRX100 Services Gateway

IN THIS CHAPTER

Connecting the SRX100 Services Gateway to the Power Supply

To connect the device to the power supply:

> ⚠️ **CAUTION:** Before connecting the device to the power supply, attach an ESD strap to an ESD point and place the other end of the strap around your bare wrist.

1. Plug the DC connector end of the power cable into the power connector on the back of the device (see).

2. Plug the AC adapter end of the power cable into an AC power outlet.

Figure 14: Connecting the Services Gateway to the Power Supply
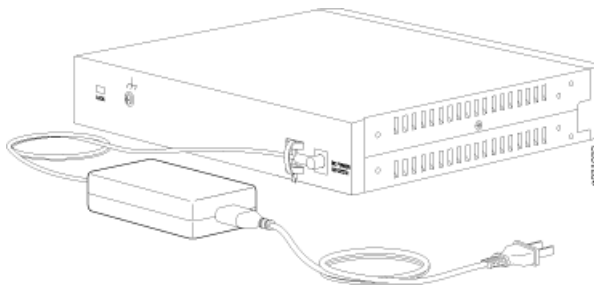
> **NOTE:** The device must be connected to earth ground during normal operation. The protective earthing terminal on the rear of the chassis is provided to connect the device to ground.

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

> **NOTE:** Use the cable tie holder to secure the power cord on to the power supply point.

> **NOTE:** We strongly recommend that you use only the 3-prong power cord supplied with your services gateway. If you are using a 2-prong power cord, then ensure that your device is adequately grounded using the grounding point available on the back panel of the chassis.

RELATED DOCUMENTATION

Powering On and Powering Off the SRX100 Services Gateway

This topic describes the following procedures:

Powering On the SRX100 Services Gateway

To power on the services gateway:

1. Ensure that you have connected the power supply to the device.

2. Insert the plug of the power supply adapter into an AC power source receptacle.

3. Turn on the power to the AC power receptacle.

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

> **NOTE:** After the power supply is turned on, it can take up to 60 seconds for status indicators—such as the Status and Power LEDs—to show that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

> **NOTE:** If the system is completely powered off when you turn on the power supply, the device starts as the power supply completes its startup sequence. If the device finishes starting and you need to power off the system again, first issue the CLI **request system power-off** command.

SEE ALSO

Powering Off the SRX100 Services Gateway

You can power off the services gateway in one of the following ways:

- Graceful shutdown—Press and immediately release the Power button. The device begins gracefully shutting down the operating system and then powers itself off.

  > **WARNING:** Use the graceful shutdown method to power off or reboot the services gateway.

- Forced shutdown—Press the Power button and hold it for ten seconds. The device immediately powers itself off without shutting down the operating system.

> **WARNING:** Use the forced shutdown method as a last resort to recover the services gateway if the services gateway operating system is not responding to the graceful shutdown method.

For more information on power button, see "SRX100 Services Gateway LEDs" on page 6.

> **WARNING:** Do not press the Power button while the device is shutting down.

> **CAUTION:** Forced shutdown can result in data loss and corruption of the file system.

> **NOTE:** To remove power completely from the device, unplug the power cord or switch off the AC power source.
>
> After powering off a power supply, wait at least 10 seconds before turning it back on. After powering on a power supply, wait at least 10 seconds before turning it off.
>
> The power button on the services gateway is a standby power switch, which will not turn off the input power to the services gateway.

> **TIP:** When you are powering off the device, the CLI displays the following message: **Turning the system power off**. You can now safely remove the power cable to completely power off the device.

> **NOTE:** You can use the request system reboot CLI command to schedule a reboot to the services gateway using **request system reboot**.

For more information about halting, powering off, or rebooting the services gateway using the CLI, see the following topics:

- Initial Configuration for Security Devices
- Monitoring and Troubleshooting for Security Devices

SEE ALSO

RELATED DOCUMENTATION

CHAPTER 14

Performing Initial Configuration

SRX100 Services Gateway Software Configuration Overview

This topic includes the following sections:

Preparing the SRX100 Services Gateway for Configuration

The Juniper Networks Junos operating system (Junos OS) is preinstalled on the SRX100 Services Gateway. When the services gateway is powered on, it is ready to be configured.

You can perform the initial software configuration of the services gateway by using either the browser-based setup wizard or the command-line interface (CLI).

Before configuring the device, gather the configuration information required to deploy the device in your network. At minimum, the setup wizard requires the following information:

- Device name to be used on the network

- Password for the root user

- Time information for the services gateway location:

  - Local time zone

  - Name or IP address of a Network Time Protocol (NTP) server, if NTP is used to set the time on the services gateway

  - Local date and time if an NTP server is not used to set the time

Understanding the Factory Default Configuration

Your services gateway comes configured with a default factory configuration. This configuration sets up the following network topology:

- Interface **fe-0/0/0** (port 0/0) is configured for Internet access. A DHCP client running on the interface enables the interface to receive its network settings—IP address, default gateway, and DNS servers—from an Internet service provider (ISP).

- Interfaces **fe-0/0/1** through **fe-0/0/7** (port 0/1 through port 0/7) are configured as switched interfaces in a common VLAN on which the IP address **192.168.1.1/24** is configured.

- A DHCP server is active on interfaces **fe-0/0/1** through **fe-0/0/7**. The DHCP server assigns IP addresses in the **192.168.1.0/24** network to connected devices.

The default configuration also includes the following security configuration:

- Two security zones are created: trust and untrust.

- Interface **fe-0/0/0** is in the untrust zone, while interfaces **fe-0/01** through **fe-0/0/7** are in the trust zone.

- A security policy is created that permits outbound traffic from the trust zone to the untrust zone. Inbound traffic originating in the untrust zone is blocked.

- Source Network Address Translation (NAT) is configured on the trust zone.

Understanding Built-In Ethernet Ports and Initial Configuration

During the initial configuration of the services gateway, how you use the built-in Ethernet ports (ports 0/0 through 0/7) depends on the initial configuration you are performing:

- Configuration using autoinstallation—Use built-in Ethernet port 0/0 to connect to the DHCP server. A DHCP client is configured on this interface, allowing the services gateway to receive its IP address from the DHCP server.

- Configuration using the setup wizard—Use the following built-in Ethernet ports:

  - Port 0/1—Connect your management device to this port. A DHCP server running on this interface automatically assigns your management device an IP address in the same subnetwork as the interface, allowing your management device to communicate with the services gateway through this interface.

  - Port 0/0—Connect your services gateway to the Internet on this port if you plan to download purchased software licenses through the setup wizard. A DHCP client running on this interface allows it to receive its network settings from the ISP.

    > **NOTE:** Downloading of purchased licenses from the setup wizard is available only in Junos OS Release 11.2R3 or later.

- Configuration of a chassis cluster—Perform the initial configuration of the chassis cluster using a console connection. Before you perform the initial configuration, connect the built-in Ethernet ports as follows:

  - Port 0/6—Connect to the out-of-band management network for management of the device. When you enable chassis clustering as part of configuring the chassis cluster, the management interface (**fxp0**) is automatically created on this port.

  - Port 0/7—Connect to the other device in the chassis cluster. When you enable chassis clustering, the control interface between the two devices (**fxp1**) is automatically created on this port.

  You must also make another connection between the two devices for the fabric link. You can use any available Fast Ethernet port for this connection. You must configure the interface you choose as the fabric link. For more information on configuring chassis clusters, see the Security Basics.

Mapping the Chassis Cluster Ports

On the SRX100 Services Gateway, the **fxp1** port is not user configurable when the services gateway is operating in chassis cluster mode.

The **fxp0** port is dedicated as the out-of-band management interface for each of the devices in the chassis cluster setup and the **fxp1** port is dedicated as the chassis-cluster control port.

Table 28 on page 68 shows the mapping of the chassis cluster ports.

Table 28: Mapping the Chassis Cluster Ports on an SRX100 Services Gateway

FE Ports on SRX100 Services Gateway	Management Interface
fe-0/0/6	fxp0 (management port)
fe-0/0/7	fxp1 (control port)

The Junos OS automatically creates the fxp0 and fxp1 interfaces on these ports when the SRX100 Services Gateway is operating in chassis cluster mode.

For more information, see the following guides:

- Interfaces for Security Devices

- Security Basics

Understanding Management Access

Telnet allows you to connect to the services gateway and access the CLI to execute commands from a remote system. The Telnet CLI connections are not encrypted and therefore can be intercepted.

> **NOTE:** Telnet access to the root user is prohibited. You must use more secure methods, such as SSH, to log in as **root**.

SSH provides the following features:

- Allows you to connect to the device and access the CLI to execute commands from a remote system

- Encrypts traffic so that it cannot be intercepted (unlike Telnet)

- Can be configured so that connections are authenticated by a digital certificate

- Uses public–private key technology for both connection and authentication

The SSH client software must be installed on the machine where the client application runs. If the SSH private key is encrypted (for greater security), the SSH client must be able to access the passphrase used to decrypt the key.

For information about obtaining SSH software, see http://www.ssh.com and http://www.openssh.com.

If you are using a Junos XML management protocol server to configure and monitor devices, you can activate cleartext access on the device to allow unencrypted text to be sent directly over a Transmission Line Protocol (TCP) connection without using any additional protocol (such as SSH, SSL, or Telnet). For more information about the Junos XML management protocol application programming interface (API), see the NETCONF XML Management Protocol Guide.

> **NOTE:** Information sent in cleartext is not encrypted and therefore can be intercepted.

If the device is operating in a Common Criteria environment, see the Configuration Guides for Junos OS Public Sector Certifications.

Connecting to the SRX100 Services Gateway Setup Wizard

If you plan to use the setup wizard to perform the initial configuration of the services gateway, you must connect your management device (such as a laptop or desktop computer) to one of the built-in Ethernet ports 0/1 through 0/7 on the services gateway as shown in Figure 15 on page 69. Do not use built-in Ethernet port 0/0.

Figure 15: Connecting to the Ethernet Port on an SRX100 Services Gateway
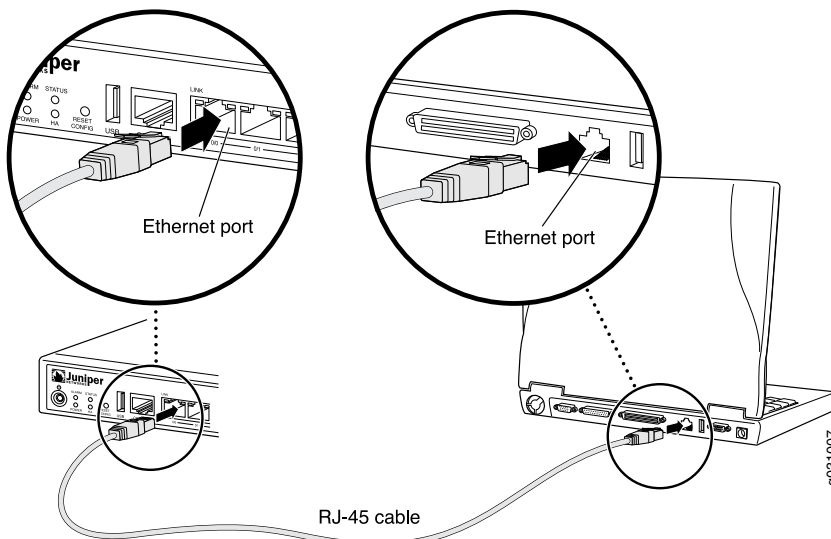
To enable communication between the management device and the services gateway, ports 0/1 through 0/7 are preconfigured with the IP address 192.168.1.1 and use DHCP to assign an IP address in the 192.168.1.0/24 network to any connected device.

To connect a management device to the built-in Ethernet ports:

1. Ensure that the IP address for the Ethernet port on the management device is configured in one of the following ways:

   - The IP address is assigned by DHCP.

   - The IP address is on the **192.168.1.0/24** subnetwork (but is not **192.168.1.1**).

2. Turn off the management device.

3. Plug one end of the CAT-5e (Ethernet cable) into the Ethernet port on the management device.

4. Connect the other end of the Ethernet cable to a built-in Fast Ethernet port (any of ports 0/1 through 0/7) on the services gateway. If the services gateway has not already been powered on, power it on now.

5. Wait until the **Status** LED on the front panel of the services gateway turns solid green.

6. Turn on the power to the management device. The services gateway assigns an IP address to the management device within the **192.168.1.0/24** subnetwork if the management device is configured to use DHCP.

7. To access the setup wizard, open a Web browser on the management device and enter the IP address **192.168.1.1** in the address field.

RELATED DOCUMENTATION

Connecting the SRX100 Services Gateway to the CLI

SRX100 Services Gateway Secure Web Access Overview

You can manage a services gateway remotely through the J-Web interface. To communicate with the services gateway, the J-Web interface uses Hypertext Transfer Protocol (HTTP). HTTP allows easy Web

access but no encryption. The data that is transmitted between the Web browser and the services gateway by means of HTTP is vulnerable to interception and attack. To enable secure Web access, the services gateway supports HTTP over Secure Sockets Layer (HTTPS). You can enable HTTP or HTTPS access on specific interfaces and ports as needed.

The services gateway uses the SSL protocol to provide secure management of services gateways through the J-Web. SSL uses public-private key technology that requires a paired private key and an authentication certificate for providing the SSL service. SSL encrypts communication between your device and the Web browser with a session key negotiated by the SSL server certificate.

An SSL certificate includes identifying information such as a public key and a signature made by a certificate authority (CA). When you access the services gateway through HTTPS, an SSL handshake authenticates the server and the client and begins a secure session. If the information does not match or if the certificate has expired, your access to the services gateway through HTTPS is restricted.

Without SSL encryption, communication between your services gateway and the browser is sent in the open and can be intercepted. We recommend that you enable HTTPS access on your WAN interfaces.

RELATED DOCUMENTATION

Connecting an SRX100 Services Gateway to the CLI Locally

If you plan to use the CLI to configure the SRX100 Services Gateway, you must connect through the console port, as shown in .

Figure 16: Connecting to the Console Port on an SRX100 Services Gateway
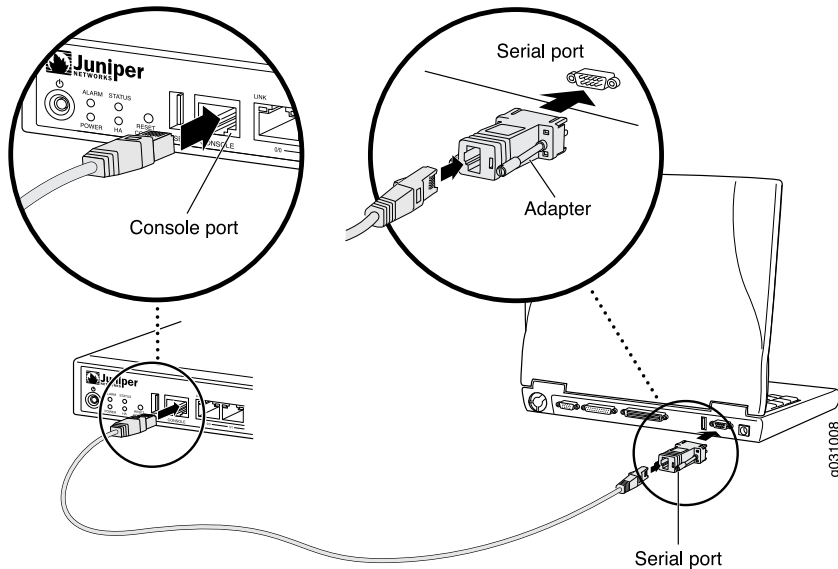
> **NOTE:** shows a connection to a local management device. A remote connection to the services gateway through a modem requires the cable and connector shown (provided in the services gateway accessory box), plus a DB-9 plug to DB-25 plug (or similar) adapter for your modem, which you must purchase separately.

To connect to the CLI using a local management device through the console port on the services gateway:

1. Turn off power to the services gateway.

2. Turn off power to the management device, such as a PC or laptop computer, that you are using to access the CLI.

3. Plug one end of the Ethernet cable supplied with your services gateway into the RJ-45 to DB-9 serial port adapter supplied with your services gateway (see).

4. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device (see).

5. Connect the other end of the Ethernet cable to the console port on the services gateway (see).

6. Turn on the power to the management device.

7. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate **COM** port to use (for example, **COM1**).

8. Configure the port settings shown in .

Table 29: Console Port Settings for the SRX100 Services Gateway

Port Settings	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

9. Power on the services gateway by pressing the Power button on the front panel. Verify that the **Power** LED on the front panel turns green.

   The terminal emulation screen on your management device displays the startup sequence. When the services gateway has finished starting up, a login prompt appears.

10. Log in as the user **root**. No password is required at initial connection, but you must assign a root password before committing any configuration settings.

SRX100 Services Gateway Basic Connectivity Overview

Displaying Basic Connectivity Configurations for the SRX100 Services Gateway

Connecting an SRX100 Services Gateway to the CLI Remotely

You can connect an SRX100 Services Gateway to the CLI from a remote location through two dial-up modems:

- A modem that is connected to the console port on the services gateway

- A second modem connected to a remote management device

The modem connection allows you to remotely perform the same console operations you can perform locally.

Viewing Factory-Default Settings of the SRX100 Services Gateway

To view the factory-default configuration of the services gateway using the CLI:

1. Verify that the services gateway is powered on.

2. Log in as the root user and provide your credentials.

3. In shell mode, navigate to the **/etc/config** folder.

   % cd /etc/config

4. View the list of default config files.

   % ls

   The following sample output displays the list of factory-default configuration files:

```
j-series-defaults.conf                  srx210h-defaults.conf
jsrxsme-series-defaults.conf            srx210h-factory.conf
```

```
jsrxsme-series-factory.conf          srx210h-poe-defaults.conf
junos-defaults.conf                  srx210h-poe-factory.conf
junos-factory.conf                   srx210he-defaults.conf
junos-fips-defaults.conf             srx210he-factory.conf
ptx-series-defaults.conf             srx210he-poe-defaults.conf
srx100-8xfe-factory.conf             srx210he-poe-factory.conf
srx100b-defaults.conf                srx210he2-defaults.conf
srx100b-factory.conf                 srx210he2-factory.conf
srx100h-defaults.conf                srx210he2-poe-defaults.conf
srx100h-factory.conf                 srx210he2-poe-factory.conf
srx100h2-defaults.conf               srx220-8xge-factory.conf
srx100h2-factory.conf                srx220-poe-8xge-factory.conf
srx110-8xfe-vdsl-factory.conf        srx220h-defaults.conf
srx110-8xfe-vdsl-wl-factory.conf     srx220h-factory.conf
srx110-8xfe-wl-factory.conf          srx220h-poe-defaults.conf
srx110b-defaults.conf                srx220h-poe-factory.conf
srx110b-va-defaults.conf             srx220h2-defaults.conf
srx110b-va-factory.conf              srx220h2-factory.conf
srx110b-vb-defaults.conf             srx220h2-poe-defaults.conf
srx110b-vb-factory.conf              srx220h2-poe-factory.conf
srx110b-wl-defaults.conf             srx240-16xge-factory.conf
srx110b-wl-factory.conf              srx240-poe-16xge-factory.conf
srx110h-defaults.conf                srx240b-factory.conf
srx110h-va-defaults.conf             srx240b2-factory.conf
srx110h-va-factory.conf              srx240h-dc-defaults.conf
srx110h-va-wl-defaults.conf          srx240h-dc-factory.conf
srx110h-va-wl-factory.conf           srx240h-defaults.conf
srx110h-vb-defaults.conf             srx240h-factory.conf
srx110h-vb-factory.conf              srx240h-poe-defaults.conf
srx110h-vb-wl-defaults.conf          srx240h-poe-factory.conf
srx110h-vb-wl-factory.conf           srx240h2-dc-defaults.conf
srx110h-wl-defaults.conf             srx240h2-dc-factory.conf
srx110h-wl-factory.conf              srx240h2-defaults.conf
srx110h2-va-defaults.conf            srx240h2-factory.conf
srx110h2-va-factory.conf             srx240h2-poe-defaults.conf
srx110h2-vb-defaults.conf            srx240h2-poe-factory.conf
srx110h2-vb-factory.conf             srx550-6xge-factory.conf
srx210-2xge-6xfe-factory.conf        srx550-defaults.conf
srx210-poe-2xge-6xfe-factory.conf    srx550-factory.conf
srx210b-defaults.conf                srx650-4xge-factory.conf
srx210b-factory.conf                 srx650-defaults.conf
srx210be-defaults.conf               srx650-factory.conf
srx210be-factory.conf
```

5. View the required default config file.

% vi *config file name*

For example, enter the following command to view the default configuration file for the SRX240 Services Gateway.

% vi srx240-poe-16xge-factory.conf

The following sample output displays the factory-default configuration on an SRX240 Services Gateway:

```
##
## $Id: $
##
## Copyright (c) 2009, Juniper Networks, Inc.
## All rights reserved.
##
system {
    autoinstallation {
        delete-upon-commit;
        traceoptions {
            level verbose;
            flag {
                all;
            }
        }
        interfaces {
            ge-0/0/0 {
                bootp;
            }
        }
    }
    services {
        ssh;
        telnet;
        dhcp {
            router {
                192.168.1.1;
            }
            pool 192.168.1.0/24 {
                address-range low 192.168.1.2 high 192.168.1.254;
            }
            propagate-settings ge-0/0/0.0;
        }
        web-management {
            http {
                interface [ vlan.0 ];
            }
```

```
                https {
                    system-generated-certificate;
                    interface [ vlan.0 ];
                }
            }
            xnm-clear-text;
        }
        name-server {
            208.67.222.222;
            208.67.220.220;
        }
        syslog {
            archive size 100k files 3;
        }
}

interfaces {
    ge-0/0/0 {
        unit 0;
    }
    ge-0/0/1 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }

    ge-0/0/2 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/3 {
        unit 0 {
            family ethernet-switching {
```

```
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/4 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/5 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/6 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/7 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }
```

```
            }
        }
        ge-0/0/8 {
            unit 0 {
                family ethernet-switching {
                    vlan {
                        members vlan-trust;
                    }
                }

            }
        }
        ge-0/0/9 {
            unit 0 {
                family ethernet-switching {
                    vlan {
                        members vlan-trust;
                    }
                }

            }
        }
        ge-0/0/10 {
            unit 0 {
                family ethernet-switching {
                    vlan {
                        members vlan-trust;
                    }
                }

            }
        }
        ge-0/0/11 {
            unit 0 {
                family ethernet-switching {
                    vlan {
                        members vlan-trust;
                    }
                }

            }
        }
        ge-0/0/12 {
```

```
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/13 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/14 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    ge-0/0/15 {
        unit 0 {
            family ethernet-switching {
                vlan {
                    members vlan-trust;
                }
            }

        }
    }
    vlan {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
```

```
            }
        }
}

poe {
    interface all;
}

security {
    nat {
        source {
            rule-set trust-to-untrust {
                from zone trust;
                to zone untrust;
                rule source-nat-rule {
                    match {
                        source-address 0.0.0.0/0;
                    }
                    then {
                        source-nat {
                            interface;
                        }
                    }
                }
            }
        }
    }
    screen {
        ids-option untrust-screen {
            icmp {
                ping-death;
            }
            ip {
                source-route-option;
                tear-drop;
            }
            tcp {
                syn-flood {
                    alarm-threshold 1024;
                    attack-threshold 200;
                    source-threshold 1024;
                    destination-threshold 2048;
                    timeout 20;
                }
```

```
                land;
            }
        }
    }
    zones {
        security-zone trust {
            host-inbound-traffic {
                system-services {
                    all;
                }
                protocols {
                    all;
                }
            }
            interfaces {
                vlan.0;
            }
        }
        security-zone untrust {
            interfaces {
                ge-0/0/0.0 {
                    host-inbound-traffic {
                        system-services {
                            dhcp;
                            tftp;
                        }
                    }
                }
            }
            screen untrust-screen;
        }
    }
    policies {
        from-zone trust to-zone untrust {
            policy trust-to-untrust {
                match {
                    source-address any;
                    destination-address any;
                    application any;
                }
                then {
                    permit;
                }
            }
```

```
            }
        }
    }
    vlans {
        vlan-trust {
            vlan-id 3;
            l3-interface vlan.0;
        }
    }
    protocols {
            stp;
    }
```

Performing Initial Software Configuration on the SRX100 Services Gateway Using the CLI

This procedure connects the device to the network but does not enable it to forward traffic. For complete information about enabling the device to forward traffic, including examples, see Security Basics.

To configure the software:

1. Verify that the device is powered on.

2. Log in as the root user. There is no password.

3. Start the CLI.

```
    root# cli
    root@>
```

4. Enter configuration mode.

```
configure
[edit]
root@#
```

5. Set the root authentication password by entering a cleartext password, an encrypted password, or an SSH public key string (DSA or RSA).

```
[edit]
root@# set system root-authentication plain-text-password
New password: password
Retype new password: password
```

6. Configure an administrator account on the device.

```
[edit]
root@# set system login user admin class super-user authentication plain-text-password
```

7. Commit the configuration to activate it on the device.

```
[edit]
root@# commit
```

8. Log in as the administrative user you configured in Step 6.

9. Configure the name of the device. If the name includes spaces, enclose the name in quotation marks (" ").

```
configure
[edit]
admin@# set system host-name host-name
```

10. Configure the traffic interface.

```
[edit]
admin@# set interfaces fe-0/0/1 unit 0 family inet address address/prefix-length
```

11. Configure the default route.

```
[edit]
admin@# set routing-options static route 0.0.0.0/0 next-hop gateway
```

12. Configure basic security zones and bind them to traffic interfaces.

```
[edit]
admin@# set security zones security-zone untrust interfaces fe-0/0/1
```

13. Configure basic security policies.

```
[edit]
admin@# set security policies from-zone trust to-zone untrust policy policy-name match source-address any
    destination-address any application any
root@# set security policies from-zone trust to-zone untrust policy policy-name then permit
```

14. Create a NAT rule for source translation of all Internet bound traffic.

```
[edit]
admin@# set security nat source rule-set interface-nat from zone trust
admin@# set security nat source rule-set interface-nat to zone untrust
admin@# set security nat source rule-set interface-nat rule rule1 match source-address 0.0.0.0/0
    destination-address 0.0.0.0/0
admin@# set security nat source rule-set interface-nat rule rule1 then source-nat interface
```

15. Check the configuration for validity.

```
[edit]
admin@# commit check
configuration check succeeds
```

16. Commit the configuration to activate it on the device.

```
[edit]
admin@# commit
commit complete
```

17. Optionally, display the configuration to verify that it is correct.

```
[edit]
user@host# show
system {
    host-name devicea;
    domain-name lab.device.net;
    domain-search [ lab.device.net device.net ];
    backup-device 192.168.2.44;
    time-zone America/Los_Angeles;
    root-authentication {
        ssh-rsa "ssh-rsa AAAAB3Nza...D9Y2gXF9ac==root@devicea.lab.device.net";
    }
    name-server {
        10.148.2.32;
    }
    services {
    }
    ntp {
        server 10.148.2.21;
    }
}
interfaces {
    fe-0/0/0 {
        unit 0 {
            family inet {
                address 192.168.1.1/24;
            }
        }
    }
    lo0 {
        unit 0 {
            family inet {
                address 172.16.1.24/32;
            }
        }
    }
}
```

18. Commit the configuration to activate it on the device.

```
[edit]
admin@# commit
```

19. Optionally, configure additional properties by adding the necessary configuration statements. Then commit the changes to activate them on the device.

```
[edit]
admin@host# commit
```

20. When you have finished configuring the device, exit configuration mode.

```
[edit]
admin@host# exit
admin@host>
```

RELATED DOCUMENTATION

Connecting the SRX100 Services Gateway to the CLI

Performing Initial Software Configuration on the SRX100 Services Gateway Using the J-Web Interface

IN THIS SECTION

- Establishing Basic Connectivity | **88**
- Configuring Basic System Properties | **89**

This topic includes the following sections:

Establishing Basic Connectivity

To establish basic connectivity:

1. Connect an Ethernet cable from any of ports 0/1 through 0/7 to the Ethernet port on the management device (workstation or laptop).

2. Connect the power cable to the device and a power source. (We recommend using a surge protector.) Note the following indications:

   - Power LED (steadily green): The device is receiving power.

   - Status LED (steadily green): The device is operating normally.

     NOTE: The services gateway functions as a DHCP server and will assign an IP address to the management device.

3. Ensure that the management device acquires an IP address on the 192.168.1.0/24 subnetwork (other than 192.168.1.1) from the device.

     NOTE: If an IP address is not assigned to the management device, manually configure an IP address in the 192.168.1.0/24 subnetwork. Do not assign the 192.168.1.1 IP address to the management device, as this IP address is assigned to the device.

4. Access the J-Web interface:

   a. Launch a Web browser from the management device.

     NOTE: To access the J-Web interface, your management device requires a supported browser: either Microsoft Internet Explorer version 7.0 (or later) or Mozilla Firefox version 3.0 (or later).

   b. Enter **192.168.1.1** in the Address box.

    c. Specify the default user name as **root**. Do not enter any value in the Password box.

    d. Press **Enter**. The J-Web Setup Wizard page opens.

5. Use the wizard to configure the basic settings, such as Hostname, Domain Name, and Root Password, for your services gateway.

The upper left area of the wizard page shows where you are in the setup process. Click a field in the wizard page to display information about that field in the lower left area of the page.

You can also use the wizard to configure the following settings:

- Default gateway

- DNS servers

- Domain search

- VLANs

- Interfaces

> **NOTE:** All network and management access settings are optional.
>
> Table 30 on page 89 and Table 31 on page 90 summarize the configuration details for the initial setup.

6. Click **Commit** on the Review & Commit page to apply the configuration.

> **NOTE:** After you configure the basic settings, the J-Web Setup wizard redirects you to the J-Web pages where you can continue working in the J-Web interface.

Configuring Basic System Properties

Table 30 on page 89 through Table 31 on page 90 summarizes the configuration details for initial setup.

Table 30: Required Setup Fields

Setup Wizard Page	Field	Your Action
Introduction		Read the introduction page for basic instructions on using the setup wizard. Click **Start** to continue.

Table 30: Required Setup Fields *(continued)*

Setup Wizard Page	Field	Your Action
Configure System: Identification		
	Host Name	Type the name of the services gateway.
	Domain Name	Type the name of the network or subnetwork to which the services gateway belongs
	Root Password (required)	Type the password that user root will use to log in to the device.
	Verify Root Password (required)	Retype the root password.
Configure J-Web Preferences		
	J-Web starting page options	Specify the tab you want to appear when J-Web starts.
	J-Web commit options	Specify when you want J-Web to commit your configuration changes.

Table 31: Optional Setup Fields

Field	Function	Your Action
Configure System: Identification		
	Default Gateway	Type the IP address of the default gateway.
	DNS Name Servers	Type the IP address of each server that maintains databases for resolving hostnames and IP addresses and click Add.
	Domain Search	Type the IP address or domain name of each domain that includes the services gateway to include it in a DNS search

Table 31: Optional Setup Fields *(continued)*

Field	Function	Your Action
Interface Groups (VLANs)		Use buttons to add, edit, or delete VLANs
Configure Interfaces		Use buttons to add, edit, or delete interfaces other than VLANs. NOTE: Make sure that you have selected the required services and protocols under Services (Inbound) and Protocols (Inbound). Select all to permit all protocols and services.
Configure System: Time		
	Current System Time	Use Reset Manually button to reset time.
	Time Zone	Choose the time zone fromthe list
	NTP Servers	Add Network Time Protocol (NTP) servers that the gateway can reach to synchronize the system time.

After you configure the basic setup, the Setup wizard is no longer available, unless you reset the device to the factory default and reboot it. To make changes to the configuration, use the J-Web interface or the command-line interface (CLI).

You can use other wizards to configure basic firewall policies, VPN settings, and NAT rules. Choose **Configure > Wizards** to use the available wizards. Use the J-Web interface or the CLI for more extensive configuration.

For more instructions on managing users and operations, monitoring network performance, upgrading software, and diagnosing common problems on an SRX100 Series Services Gateways, see the following guides:

- Initial Configuration for Security Devices
- Monitoring and Troubleshooting for Security Devices

RELATED DOCUMENTATION

Upgrading the SRX100 Services Gateway Low Memory Version to a High Memory Version

Based on your requirements, you can upgrade from an SRX100 Services Gateway Low Memory version to a High Memory version through a license key. You need not order a separate High Memory device.

The double-data-rate (DDR) memory allocation in the SRX100 Services Gateway is as follows:

- SRX100 Services Gateway High Memory - 1 GB

- SRX100 Services Gateway Low Memory - 512 MB

All SRX100 Services Gateways have a built-in DDR memory of 1 GB. The SRX100 Services Gateway Low Memory devices can utilize a maximum of 512 MB of DDR memory. To utilize 1 GB of DDR memory, you must upgrade your device to an SRX100 Services Gateway High Memory version by installing the memory upgrade license. You can install the memory license using the CLI configuration editor. For information on working with licences, see Working with License Keys for SRX Series Devices.

For more information, see the following guides:

- Initial Configuration for Security Devices

- Monitoring and Troubleshooting for Security Devices

> **NOTE:** When you install the memory upgrade license on an SRX100 Services Gateway Low Memory device, the device reboots automatically. When the device is active again, it will function as a High Memory device.

> **NOTE:** The memory upgrade license is a perpetual license. You can activate this feature on the device by directly entering the license key (provided by the licensing management system) in the CLI.

For more information on generating, installing, and managing licenses, see the following guides:

- Initial Configuration for Security Devices

- Monitoring and Troubleshooting for Security Devices

To obtain a memory license, contact your Juniper Networks customer services representative.

RELATED DOCUMENTATION

SRX100 Services Gateway Features and Functions | **4**

SRX100 Services Gateway Specifications | **21**

4

Maintaining and Troubleshooting Components

CHAPTER 15

Maintaining Components

IN THIS CHAPTER

●   Maintaining the SRX100 Services Gateway Hardware Components | 95

Maintaining the SRX100 Services Gateway Hardware Components

Table 32 on page 95 describes the common tasks for maintaining the hardware components of the services gateway.

Table 32: Maintenance Procedures for the SRX100 Services Gateway Hardware Components

Maintenance Procedures	Description
Routine maintenance	For optimum performance of the services gateway, you should regularly perform the following preventive maintenance procedures : ● Inspect the installation site for moisture, loose wires or cables, and excessive dust. ● Make sure that airflow is unobstructed around the device and into the air intake vents.
Maintaining the power supply	To maintain the power supply on the services gateway: ● Make sure that the power and grounding cables are arranged so that they do not obstruct access to other device components. ● Periodically inspect the site to ensure that the grounding and power cables connected to the device are securely in place and that there is no moisture accumulating near the device. CAUTION: We recommend using a surge protector for the power connection.

RELATED DOCUMENTATION

Monitoring the SRX100 Services Gateway Chassis Using the CLI | 97

CHAPTER 16

Troubleshooting Components

Monitoring the SRX100 Services Gateway Chassis Using the CLI

You can monitor alarms to troubleshoot hardware problems on a services gateway. The chassis properties include the status of active chassis alarms on the device and the environmental measurements of the device.

To view these chassis properties, select **Monitor**>**Chassis** in the J-Web interface, or enter the following CLI **show** commands:

- **show chassis hardware**
- **show chassis environment**
- **show chassis fpc**
- **show chassis alarms**
- **show chassis hardware detail**

Examples:

The following examples provide the sample output of commands:

- **show chassis hardware**

  user@host > show chassis hardware

```
Item                        Version  Part number  Serial number      Description

Chassis                                           AU0209AF0022       SRX100h

Routing Engine       REV 00    750-02177    BAAA0083            RE-SRX100H

FPC 0                                                                FPC

PIC 0                                                                8x FE Base PIC

Power Supply 0
```

- **show chassis hardware detail**

   user@host > show chassis hardware detail

```
Item                        Version  Part number  Serial number      Description

Chassis                                           AU0809AF0003       SRX100h

Routing Engine       REV 00    750-02177    BAAA0116            RE-SRX100H

  da0                       999 MB   ST72682                   Nand Flash
  usb0 <addr 1>             DWC OTG  root hub 0      vendor 0x0000        uhub0
  usb0 <addr 2>             product  0x005a 90      vendor 0x0409         uhub1
  usb0 <addr 3>             ST72682 High Speed Mode 64218 STMicroelectronics umass0

FPC 0                                                                FPC

PIC 0                                                                8x FE Base PIC

Power Supply 0
```

> **NOTE:** The values given in the **usb0** rows provide information for USB-level debugging. This information is about USB hub topology.

- **show chassis environment**

   user@host > show chassis environment

```
Class  Item                              Status      Measurement

Temp   Routing Engine                    OK          43 degrees C / 109 degrees F

Power  Power Supply 0                    OK
```

- **show chassis fpc**

  user@host > show chassis fpc

```
          Temp  CPU Utilization (%)   Memory     Utilization (%)

Slot State             (C)   Total  Interrupt      DRAM (MB) Heap      Buffer

   0  Online             -------------------- CPU less FPC --------------------
```

- **show chassis alarms**

  user@host > show chassis alarms

```
 No alarms currently active
```

RELATED DOCUMENTATION

Monitoring the SRX100 Services Gateway Components Using LEDs **| 100**

Monitoring the SRX100 Services Gateway Using Chassis Alarm Conditions **| 102**

Monitoring the SRX100 Services Gateway Power System **| 103**

Maintaining the SRX100 Services Gateway Hardware Components **| 95**

Using the Reset Config Button on the SRX100 Services Gateway **| 104**

Juniper Networks Technical Assistance Center **| 107**

Monitoring the SRX100 Services Gateway Components Using LEDs

describes the status of the LEDs on startup of the device.

Table 33: Services Gateway LED Status on Startup

LED	State	Description
Status LED	Amber	Indicates that the device is starting up.
Alarm LED	Amber	Indicates that the device is starting up for the first time since no rescue configuration is set. **NOTE:** When the system is up and running, if the Alarm LED is off, it indicates that no alarms are present on the device.
Power LED	Green	Indicates that the device is receiving normal power supply.
HA LED	Off	Indicates that the device is not part of chassis clustering set up.

The LEDs available on the services gateway display the status of various components. describes the LEDs.

Table 34: Component LEDs on the Services Gateway

LED	State	Meaning	Possible Causes and Corrective Actions
Status LED	Green	Indicates that the device is functioning normally.	Normal condition. No action is required.
	Amber	• Indicates that the device is starting up. • Indicates that the Reset Config button is pressed.	Normal condition. No action is required.
	Red	Indicates that an error is detected in the device.	Contact JTAC. See "Juniper Networks Technical Assistance Center" on page 107.

Table 34: Component LEDs on the Services Gateway *(continued)*

LED	State	Meaning	Possible Causes and Corrective Actions
Alarm LED	Red	Indicates a major alarm.	Major alarm indicates a critical situation on the services gateway that requires immediate action. See "Monitoring the SRX100 Services Gateway Using Chassis Alarm Conditions" on page 102.
	Amber	Indicates a minor alarm.	Minor alarm condition requires monitoring or maintenance. If left unchecked, it might cause an interruption in service or degradation in performance. See "Monitoring the SRX100 Services Gateway Using Chassis Alarm Conditions" on page 102.
	Off	Indicates that there are currently no alarms.	Normal condition. No action is required.
Power LED	Green	Indicates that the device is functioning normally.	Normal condition. No action is required.
	Amber	Indicates that the Power button has been pressed and quickly released and the device is gracefully shutting down.	Normal condition. No action is required.
	Off	Off indicates that the device is not receiving power.	Normal condition if the services gateway is switched-off. No action is required. If you have not powered off the services gateway, verify that the AC power cord from the power source to the device is not damaged, the socket is in working condition, and the device has an AC input voltage between 100 and 240 VAC. See "Monitoring the SRX100 Services Gateway Power System" on page 103.

Monitoring the SRX100 Services Gateway Using Chassis Alarm Conditions

When the services gateway detects an alarm condition, the alarm LED on the front panel turns red or amber as appropriate.

To view a more detailed description of the alarm cause, issue the **show chassis alarms** CLI command.

For more information on the **show chassis alarms** command, see the following topics:

- Initial Configuration for Security Devices

- Monitoring and Troubleshooting for Security Devices

Table 35 on page 102 describes alarms that can occur for an SRX100 Services Gateway chassis component.

Table 35: SRX100 Services Gateway Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Action	Alarm Severity
Boot media	The services gateway boots from an alternate boot device.	• If the internal flash memory fails at startup, the services gateway automatically boots itself from the alternative boot device (USB storage device). **NOTE:** If you configured your services gateway to boot from an alternative boot device, ignore this alarm condition. • Reformat the internal flash memory and install a bootable image. (See theInitial Configuration for Security Devices and Monitoring and Troubleshooting for Security Devices) • If you did not configure the services gateway to boot from an alternative boot device, contact JTAC. See "Juniper Networks Technical Assistance Center" on page 107.	Amber (minor)

Table 35: SRX100 Services Gateway Chassis Alarm Conditions and Corrective Actions *(continued)*

Component	Alarm Conditions	Action	Alarm Severity
Hardware components on the services gateway	The services gateway chassis temperature or chassis is too warm	Check the room temperature. See "SRX100 Services Gateway Specifications" on page 21.	Amber (minor)
	The services gateway temperature is too high, either because of an internal overheating condition or because the maximum recommended room temperature has been exceeded.	The services gateway shuts down automatically in 4 minutes.	Red (major)

RELATED DOCUMENTATION

Monitoring the SRX100 Services Gateway Power System

The LEDs on the services gateway enable you to determine the performance and operation. The Power LED, located on the front panel of the services gateway, indicates the different settings with respect to the power system.

Table 36 on page 104 describes different Power LED status settings and their corrective actions.

Table 36: Services Gateway Power LED Status

LED Status	Meaning	Possible Cause and Corrective Action
Green	Device is receiving power, and the internal power supply is functional.	Normal indication. No action is required.
Amber	Indicates that the power button has been pressed and quickly released.	Normal indication. No action is required.
Off	Indicates that the device is not receiving power.	• Verify that the AC power cord from the power source to the device is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable. • Ensure that the socket you plug in is in working condition. • Ensure the device has an AC input voltage between 100 and 240 VAC. • If you cannot determine the cause of the problem or need additional assistance, see "Juniper Networks Technical Assistance Center" on page 107.

RELATED DOCUMENTATION

Using the Reset Config Button on the SRX100 Services Gateway

If a configuration fails or denies management access to the services gateway, you can use the RESET CONFIG button to restore the device to the factory-default configuration or a rescue configuration. For example, if someone inadvertently commits a configuration that denies management access to a services

gateway, you can delete the invalid configuration and replace it with a rescue configuration by pressing the RESET CONFIG button.

> **NOTE:** The RESET CONFIG button is recessed to prevent it from being pressed accidentally.

The rescue configuration is a previously committed, valid configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI.

To press the RESET CONFIG button, insert a small probe (such as a straightened paper clip) into the pinhole on the front panel.

- By default, pressing and quickly releasing the RESET CONFIG button loads and commits the rescue configuration through the J-Web interface or the CLI. The Status LED is solid amber during this time.

- By default, pressing and holding the RESET CONFIG button for 15 seconds or more—until the Status LED is solid amber — deletes all configurations on the device, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

  For details about factory-default settings, see *Viewing Factory Default Settings of the SRX240 Services Gateway*.

  For details about performing initial software configuration, see the following topics:

  - *Performing Initial Software Configuration on the SRX240 Services Gateway Using the J-Web Interface*

  - *Performing Initial Software Configuration on the SRX240 Services Gateway Using the CLI*

RELATED DOCUMENTATION

Changing the Reset Config Button Behavior on the SRX100 Services Gateway

You can change the default operation of the RESET CONFIG button by limiting how the button resets the services gateway:

- To prevent the RESET CONFIG button from setting the device to the factory-default configuration and deleting all other configurations:

  admin@host# **set chassis config-button no-clear**

  You can still press and quickly release the button to reset it to the rescue configuration.

- To prevent the RESET CONFIG button from setting the device to the rescue configuration:

  admin@host# **set chassis config-button no-rescue**

  You can still press and hold the button for 15 seconds or more to reset the gateway to the factory-default configuration.

- To disable the button and prevent the device from resetting to either configuration:

  admin@host# **set chassis config-button no-clear no-rescue**

The **no-clear** option prevents the RESET CONFIG button from deleting all configurations on the services gateway. The **no-rescue** option prevents the RESET CONFIG button from loading the rescue configuration.

To return the function of the RESET CONFIG button to its default behavior, remove the **config-button** statement from the device configuration.

RELATED DOCUMENTATION

Juniper Networks Technical Assistance Center

If you need assistance while troubleshooting a services gateway, open a support case using the Case Manager link at https://www.juniper.net/support/ , or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (from outside the United States).

5
PART

Replacing Components

CHAPTER 17

Contacting Customer Support and Returning Components

IN THIS CHAPTER

Contacting Customer Support

Once you have located the serial numbers of the services gateway or component, you can return them for repair or replacement. For this, you need to contact Juniper Networks Technical Assistance Center (JTAC).

You can contact JTAC 24 hours a day, 7 days a week, using any of the following methods:

- On the Web: Using the Service Request Manager link at https://support.juniper.net/support/
- By telephone:
  - From the US and Canada: 1-888-314-JTAC
  - From all other locations: 1-408-745-9500

> **NOTE:** If contacting JTAC by telephone, enter your 12-digit service request number followed by the pound (#) key if this is an existing case, or press the star (*) key to be routed to the next available support engineer.

Return Procedure for the SRX100 Services Gateway

To return an SRX100 Services Gateway or component to Juniper Networks for repair or replacement:

1. Determine the part number and serial number of the device or component. See "Locating the SRX100 Services Gateway Component Serial Number and Agency Labels" on page 111.

2. Obtain a Return Materials Authorization (RMA) number from JTAC. See "Contacting Customer Support" on page 109.

   NOTE: Do not return the device or any component to Juniper Networks unless you have first obtained an RMA number. Juniper Networks reserves the right to refuse shipments that do not have an RMA. Refused shipments are returned to the customer via collect freight.

3. Pack the SRX100 Services Gateway or component for shipping. See "Packing the SRX100 Services Gateway and Components for Shipment" on page 113.

For more information about return and repair policies, see the customer support Web page at https://www.juniper.net/support/guidelines.html.

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

Information You Might Need to Supply to Juniper Networks Technical Assistance Center

If you are returning a services gateway or hardware component to Juniper Networks for repair or replacement, obtain a Return Materials Authorization (RMA) number from Juniper Networks Technical Assistance Center (JTAC).

When requesting support from JTAC by telephone, be prepared to provide the following information:

- Your existing case number, if you have one

- Details of the failure or problem

- Type of activity being performed on the services gateway when the problem occurred

- Configuration data displayed by one or more **show** commands

- Your name, organization name, telephone number, fax number, and shipping address

Locating the SRX100 Services Gateway Component Serial Number and Agency Labels

Listing the SRX100 Services Gateway and Component Details with the CLI

Before contacting Juniper Networks to request an RMA, you must find the serial number on the SRX100 Services Gateway or component.

To list all of the SRX100 Services Gateway components and their serial numbers, enter the following CLI **show** command:

`user@host>` **show chassis hardware**

The output is as follows:

```
Hardware inventory:
Item                     Version   Part number   Serial number        Description

Chassis                                          AU0209AF0022         SRX100h

Routing Engine           REV 00    750-02177     BAAA0083             RE-SRX100-HIGHMEM

FPC 0                                                                 FPC

PIC 0                                                                 8x FE Base PIC

Power Supply 0
```

SRX100 Services Gateway Chassis Serial Number and Agency Labels

The SRX100 Services Gateway has a serial number ID and agency labels on the bottom of the chassis as shown in Figure 17 on page 112.

Figure 17: Location of SRX100 Services Gateway Serial Number and Agency Labels

Serial number ID label
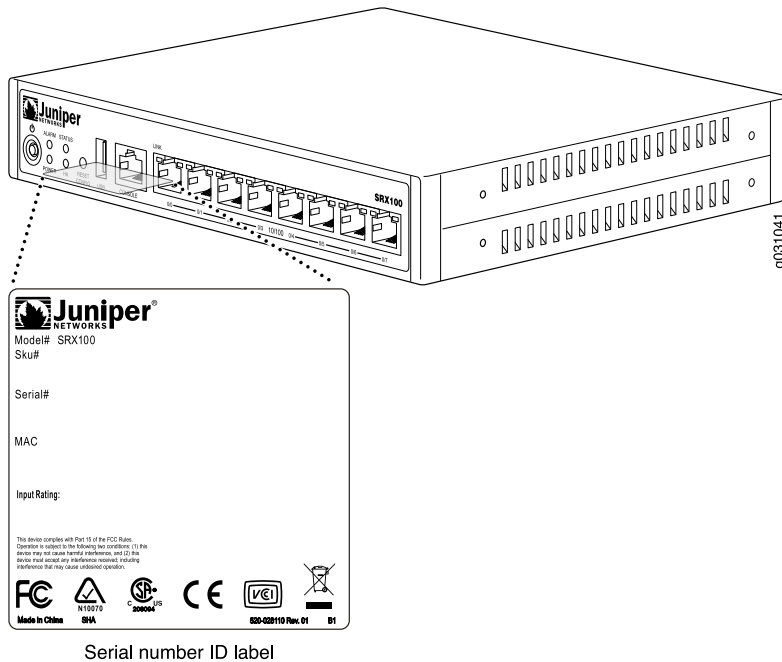
RELATED DOCUMENTATION

Return Procedure for the SRX100 Services Gateway | 110

Packing the SRX100 Services Gateway and Components for Shipment

This topic describes how to pack the services gateway or components for shipment.

Packing the Services Gateway for Shipment

To pack the services gateway for shipment:

1. Retrieve the shipping carton and packing materials in which the device was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.

2. Attach an electrostatic discharge (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.

3. On the console or other management device connected to the services gateway, enter CLI operational mode and issue the following command to shut down the services gateway software:

   user@host> request system power-off

   Wait until a message appears on the console confirming that the operating system has halted.

4. Shut down power to the device by pressing the Power button on the front panel of the device.

5. Disconnect power from the device.

6. Remove the cables that connect to all external devices.

7. Remove all field-replaceable units (FRUs) from the device.

8. If the device is installed on a wall or rack, have one person support the weight of the device while another person unscrews and removes the mounting screws.

9. Place the device in the shipping carton.

10. Cover the device with an ESD bag, and place the packing foam on top of and around the device.

11. Replace the accessory box on top of the packing foam.

12. Securely tape the box closed.

13. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

Packing the Components for Shipment

Follow these guidelines for packing and shipping individual components of the services gateway:

- When you return a component, make sure that it is adequately protected with packing materials and packed so that the pieces are prevented from moving around inside the carton.

- Use the original shipping materials if they are available.

- Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

⚠️ **CAUTION:** Do not stack any of the services gateway components during packing.

RELATED DOCUMENTATION

6

PART

Safety and Regulatory Compliance Information

General Safety Guidelines and Warnings

IN THIS CHAPTER

SRX100 Services Gateway Definition of Safety Warning Levels

This topic defines the following four levels of safety warnings used in Juniper Networks technical publications:

> **NOTE:** You might find this information helpful in a particular situation or might otherwise overlook it.

> **CAUTION:** You need to observe the specified guidelines to avoid minor injury or discomfort to you or severe damage to the services gateway.

> **WARNING:** This symbol is used with laser warnings. Unterminated optical connectors can emit invisible laser radiation. Focusing your eye directly on a laser source—even a low-power laser—could permanently damage the eye.

WARNING: This symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

Waarschuwing Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen.

Varoitus Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista.

Attention Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents.

Warnung Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt.

Avvertenza Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti.

Advarsel Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du vare oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker.

Aviso Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos físicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes.

¡Atención! Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes.

> **Varning!** Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador.

RELATED DOCUMENTATION

SRX100 Services Gateway General Safety Guidelines and Warnings

IN THIS SECTION

This topic includes the following sections:

General Safety Guidelines and Warnings

The following guidelines help ensure your safety and protect the services gateway from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so it is important that you remain alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in these topics. Ensure that only authorized service personnel perform other system services.

- Keep the area around the chassis clear and free from dust before, during, and after installation.

- Keep tools away from areas where people could trip on them.

- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.

- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.

- Never install or manipulate wiring during electrical storms.

- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.

- Do not open or remove chassis covers or sheet metal parts unless instructions are provided in this guide. Such an action could cause severe electrical shock.

- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.

- Avoid spilling liquid onto the services gateway chassis or onto any services gateway component. Such an action could cause electrical shock or damage the services gateway.

- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.

Qualified Personnel Warning

WARNING: Only trained and qualified personnel should install or replace the services gateway.

Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

Varoitus Ainoastaan koulutettu ja pätevä henkilökunta saa asentaa tai vaihtaa tämän laitteen.

Attention Tout installation ou remplacement de l'appareil doit être réalisé par du personnel qualifié et compétent.

Warnung Gerät nur von geschultem, qualifiziertem Personal installieren oder auswechseln lassen.

Avvertenza Solo personale addestrato e qualificato deve essere autorizzato ad installare o sostituire questo apparecchio.

Advarsel Kun kvalifisert personell med riktig opplæring bør montere eller bytte ut dette utstyret.

Aviso Este equipamento deverá ser instalado ou substituído apenas por pessoal devidamente treinado e qualificado.

¡Atención! Estos equipos deben ser instalados y reemplazados exclusivamente por personal técnico adecuadamente preparado y capacitado.

Varning! Denna utrustning ska endast installeras och bytas ut av utbildad och kvalificerad personal.

Restricted Access Area Warning

WARNING: The services gateway is intended for installation in restricted access areas. A restricted access area is an area to which access can be gained only by service personnel through the use of a special tool, lock and key, or other means of security, and which is controlled by the authority responsible for the location.

Waarschuwing Dit toestel is bedoeld voor installatie op plaatsen met beperkte toegang. Een plaats met beperkte toegang is een plaats waar toegang slechts door servicepersoneel verkregen kan worden door middel van een speciaal instrument, een slot en sleutel, of een ander veiligheidsmiddel, en welke beheerd wordt door de overheidsinstantie die verantwoordelijk is voor de locatie.

Varoitus Tämä laite on tarkoitettu asennettavaksi paikkaan, johon pääsy on rajoitettua. Paikka, johon pääsy on rajoitettua, tarkoittaa paikkaa, johon vain huoltohenkilöstö pääsee jonkin erikoistyökalun, lukkoon sopivan avaimen tai jonkin muun turvalaitteen avulla ja joka on paikasta vastuussa olevien toimivaltaisten henkilöiden valvoma.

Attention Cet appareil est à installer dans des zones d'accès réservé. Ces dernières sont des zones auxquelles seul le personnel de service peut accéder en utilisant un outil spécial, un mécanisme de verrouillage et une clé, ou tout autre moyen de sécurité. L'accès aux zones de sécurité est sous le contrôle de l'autorité responsable de l'emplacement.

Warnung Diese Einheit ist zur Installation in Bereichen mit beschränktem Zutritt vorgesehen. Ein Bereich mit beschränktem Zutritt ist ein Bereich, zu dem nur Wartungspersonal mit einem Spezialwerkzeugs, Schloß und Schlüssel oder anderer Sicherheitsvorkehrungen Zugang hat, und der von dem für die Anlage zuständigen Gremium kontrolliert wird.

Avvertenza Questa unità deve essere installata in un'area ad accesso limitato. Un'area ad accesso limitato è un'area accessibile solo a personale di assistenza tramite un'attrezzo speciale, lucchetto, o altri dispositivi di sicurezza, ed è controllata dall'autorità responsabile della zona.

Advarsel Denne enheten er laget for installasjon i områder med begrenset adgang. Et område med begrenset adgang gir kun adgang til servicepersonale som bruker et spesielt verktøy, lås og nøkkel, eller en annen sikkerhetsanordning, og det kontrolleres av den autoriteten som er ansvarlig for området.

Aviso Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado, que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.

¡**Atención!** Esta unidad ha sido diseñada para instalarse en áreas de acceso restringido. Área de acceso restringido significa un área a la que solamente tiene acceso el personal de servicio mediante la utilización de una herramienta especial, cerradura con llave, o algún otro medio de seguridad, y que está bajo el control de la autoridad responsable del local.

Varning! Denna enhet är avsedd för installation i områden med begränsat tillträde. Ett område med begränsat tillträde får endast tillträdas av servicepersonal med ett speciellt verktyg, lås och nyckel, eller annan säkerhetsanordning, och kontrolleras av den auktoritet som ansvarar för området.

Preventing Electrostatic Discharge Damage to the Services Gateway

Many services gateway hardware components are sensitive to damage from static electricity. Some components can be impaired by voltages as low as 30 V. You can easily generate potentially damaging static voltages whenever you handle plastic or foam packing material or if you move components across plastic or carpets. Observe the following guidelines to minimize the potential for electrostatic discharge (ESD) damage, which can cause intermittent or complete component failures:

- Always use an ESD wrist strap or ankle strap, and verify that it is in direct contact with your skin.

> ⚠️ **CAUTION:** For safety, periodically check the resistance value of the ESD strap. The measurement should be in the range of 1 to 10 Mohms.

- When handling any component that is removed from the chassis, verify that the equipment end of your ESD strap is attached to one of the ESD points on the chassis.

- Avoid contact between the component and your clothing. ESD voltages emitted from clothing can still damage components.

- When removing or installing a component, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an electrostatic bag. If you are returning a component, place it into an electrostatic bag before packing it. See Figure 18 on page 125.

Figure 18: Placing a Component into an Electrostatic Bag
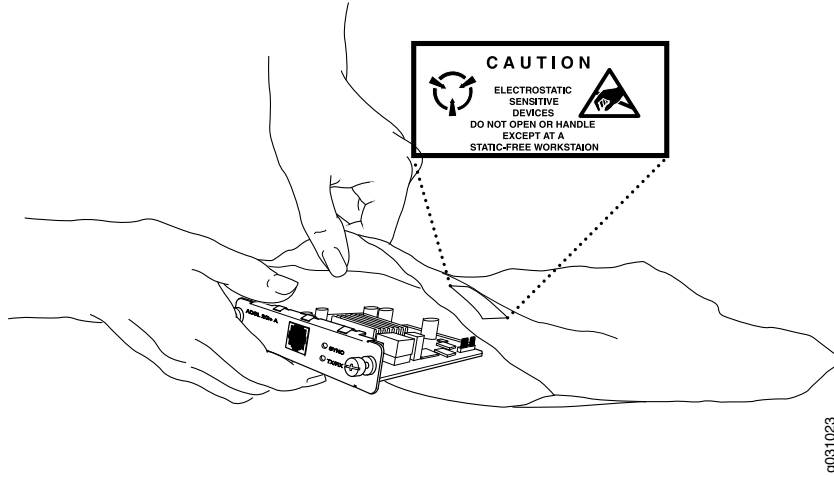
RELATED DOCUMENTATION

SRX100 Services Gateway Definition of Safety Warning Levels | **116**

SRX100 Services Gateway Fire Safety Requirements | **127**

SRX100 Services Gateway Safety Requirements, Warnings, and Guidelines

To avoid harm to yourself or the services gateway as you install and maintain it, follow the guidelines for working with and near electrical equipment, as well as the safety procedures for working with devices. For a discussion of how to make the installation site a safe environment along with a list of safety warnings, see Appendix A, Safety and Regulatory Compliance Information.

> **NOTE:** Providing an exhaustive set of guidelines for working with electrical equipment is beyond the scope of this guide.

RELATED DOCUMENTATION

SRX100 Services Gateway General Safety Guidelines and Warnings | **119**

SRX100 Services Gateway Electrical Safety Guidelines and Warnings | **150**

Required Tools and Parts for Installing and Maintaining the SRX100 Services Gateway | **37**

Fire Safety Requirements

IN THIS CHAPTER

SRX100 Services Gateway Fire Safety Requirements

In the event of a fire emergency involving devices and other network equipment, the safety of people is the primary concern. Establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire-control equipment and fire extinguishers.

In addition, establish procedures to protect your equipment in the event of a fire emergency. Juniper Networks products should be installed in an environment suitable for electronic equipment. We recommend that fire suppression equipment be available in the event of a fire in the vicinity of the equipment and that all local fire, safety, and electrical codes and ordinances be observed when installing and operating your equipment.

In the event of an electrical hazard or an electrical fire, first turn power off to the equipment at the source. Then use a Type C fire extinguisher to extinguish the fire. Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide (CO_2) and Halotron, are most effective for suppressing electrical fires. Type C fire extinguishers displace the oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, use this type of inert oxygen displacement extinguisher instead of an extinguisher that leaves residue on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers) near Juniper Networks equipment. The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in minute amounts of moisture, monoammonium phosphate can become highly corrosive and corrodes most metals.

Any equipment in a room in which a chemical fire extinguisher has been discharged is subject to premature failure and unreliable operation. The equipment is considered to be irreparably damaged.

> **NOTE:** To keep warranties effective, do not use a dry chemical fire extinguisher to control a fire at or near a Juniper Networks services gateway. If a dry chemical fire extinguisher is used, the unit is no longer eligible for coverage under a service agreement.

We recommend that you dispose of any irreparably damaged equipment in an environmentally responsible manner.

RELATED DOCUMENTATION

SRX100 Services Gateway General Safety Guidelines and Warnings | **119**

SRX100 Services Gateway Installation Safety Guidelines and Warnings | **129**

CHAPTER 20

Installation Safety Guidelines and Warnings

IN THIS CHAPTER

SRX100 Services Gateway Installation Safety Guidelines and Warnings

Installation Instructions Warning

WARNING: Read the installation instructions before you connect the services gateway to a power source.

Waarschuwing Raadpleeg de installatie-aanwijzingen voordat u het systeem met de voeding verbindt.

Varoitus Lue asennusohjeet ennen järjestelmän yhdistämistä virtalähteeseen.

Attention Avant de brancher le système sur la source d'alimentation, consulter les directives d'installation.

Warnung Lesen Sie die Installationsanweisungen, bevor Sie das System an die Stromquelle anschließen.

Avvertenza Consultare le istruzioni di installazione prima di collegare il sistema all'alimentatore.

Advarsel Les installasjonsinstruksjonene før systemet kobles til strømkilden.

Aviso Leia as instruções de instalação antes de ligar o sistema à sua fonte de energia.

¡Atención! Ver las instrucciones de instalación antes de conectar el sistema a la red de alimentación.

Varning! Läs installationsanvisningarna innan du kopplar systemet till dess strömförsörjningsenhet.

Rack-Mounting Requirements and Warnings

Ensure that the equipment rack into which the services gateway is installed is evenly and securely supported to avoid the hazardous condition that could result from uneven mechanical loading.

WARNING: To prevent bodily injury when mounting or servicing the services gateway in a rack, take the following precautions to ensure that the system remains stable. The following directives help maintain your safety:

- The services gateway must be installed into a rack that is secured to the building structure.

- The services gateway should be mounted at the bottom of the rack if it is the only unit in the rack.

- When mounting the services gateway in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the services gateway in the rack.

Waarschuwing Om lichamelijk letsel te voorkomen wanneer u dit toestel in een rek monteert of het daar een servicebeurt geeft, moet u speciale voorzorgsmaatregelen nemen om ervoor te zorgen dat het toestel stabiel blijft. De onderstaande richtlijnen worden verstrekt om uw veiligheid te verzekeren:

- De Juniper Networks services gateway moet in een stellage worden geïnstalleerd die aan een bouwsel is verankerd.

- Dit toestel dient onderaan in het rek gemonteerd te worden als het toestel het enige in het rek is.

- Wanneer u dit toestel in een gedeeltelijk gevuld rek monteert, dient u het rek van onderen naar boven te laden met het zwaarste onderdeel onderaan in het rek.

- Als het rek voorzien is van stabiliseringshulpmiddelen, dient u de stabilisatoren te monteren voordat u het toestel in het rek monteert of het daar een servicebeurt geeft.

Varoitus Kun laite asetetaan telineeseen tai huolletaan sen ollessa telineessä, on noudatettava erityisiä varotoimia järjestelmän vakavuuden säilyttämiseksi, jotta vältytään loukkaantumiselta. Noudata seuraavia turvallisuusohjeita:

- Juniper Networks services gateway on asennettava telineeseen, joka on kiinnitetty rakennukseen.

- Jos telineessä ei ole muita laitteita, aseta laite telineen alaosaan.

- Jos laite asetetaan osaksi täytettyyn telineeseen, aloita kuormittaminen sen alaosasta kaikkein raskaimmalla esineellä ja siirry sitten sen yläosaan.

- Jos telinettä varten on vakaimet, asenna ne ennen laitteen asettamista telineeseen tai sen huoltamista siinä.

Attention Pour éviter toute blessure corporelle pendant les opérations de montage ou de réparation de cette unité en casier, il convient de prendre des précautions spéciales afin de maintenir la stabilité du système. Les directives ci-dessous sont destinées à assurer la protection du personnel:

- Le rack sur lequel est monté le Juniper Networks services gateway doit être fixé à la structure du bâtiment.

- Si cette unité constitue la seule unité montée en casier, elle doit être placée dans le bas.

- Si cette unité est montée dans un casier partiellement rempli, charger le casier de bas en haut en plaçant l'élément le plus lourd dans le bas.

- Si le casier est équipé de dispositifs stabilisateurs, installer les stabilisateurs avant de monter ou de réparer l'unité en casier.

Warnung Zur Vermeidung von Körperverletzung beim Anbringen oder Warten dieser Einheit in einem Gestell müssen Sie besondere Vorkehrungen treffen, um sicherzustellen, daß das System stabil bleibt. Die folgenden Richtlinien sollen zur Gewährleistung Ihrer Sicherheit dienen:

- Der Juniper Networks services gateway muß in einem Gestell installiert werden, das in der Gebäudestruktur verankert ist.

- Wenn diese Einheit die einzige im Gestell ist, sollte sie unten im Gestell angebracht werden.

- Bei Anbringung dieser Einheit in einem zum Teil gefüllten Gestell ist das Gestell von unten nach oben zu laden, wobei das schwerste Bauteil unten im Gestell anzubringen ist.

- Wird das Gestell mit Stabilisierungszubehör geliefert, sind zuerst die Stabilisatoren zu installieren, bevor Sie die Einheit im Gestell anbringen oder sie warten.

Avvertenza Per evitare infortuni fisici durante il montaggio o la manutenzione di questa unità in un supporto, occorre osservare speciali precauzioni per garantire che il sistema rimanga stabile. Le seguenti direttive vengono fornite per garantire la sicurezza personale:

- Il Juniper Networks services gateway deve essere installato in un telaio, il quale deve essere fissato alla struttura dell'edificio.

- Questa unità deve venire montata sul fondo del supporto, se si tratta dell'unica unità da montare nel supporto.

- Quando questa unità viene montata in un supporto parzialmente pieno, caricare il supporto dal basso all'alto, con il componente più pesante sistemato sul fondo del supporto.

- Se il supporto è dotato di dispositivi stabilizzanti, installare tali dispositivi prima di montare o di procedere alla manutenzione dell'unità nel supporto.

Advarsel Unngå fysiske skader under montering eller reparasjonsarbeid på denne enheten når den befinner seg i et kabinett. Vær nøye med at systemet er stabilt. Følgende retningslinjer er gitt for å verne om sikkerheten:

- Juniper Networks services gateway må installeres i et stativ som er forankret til bygningsstrukturen.

- Denne enheten bør monteres nederst i kabinettet hvis dette er den eneste enheten i kabinettet.

- Ved montering av denne enheten i et kabinett som er delvis fylt, skal kabinettet lastes fra bunnen og opp med den tyngste komponenten nederst i kabinettet.

- Hvis kabinettet er utstyrt med stabiliseringsutstyr, skal stabilisatorene installeres før montering eller utføring av reparasjonsarbeid på enheten i kabinettet.

Aviso Para se prevenir contra danos corporais ao montar ou reparar esta unidade numa estante, deverá tomar precauções especiais para se certificar de que o sistema possui um suporte estável. As seguintes directrizes ajudá-lo-ão a efectuar o seu trabalho com segurança:

- O Juniper Networks services gateway deverá ser instalado numa prateleira fixa à estrutura do edificio.

- Esta unidade deverá ser montada na parte inferior da estante, caso seja esta a única unidade a ser montada.

- Ao montar esta unidade numa estante parcialmente ocupada, coloque os itens mais pesados na parte inferior da estante, arrumando-os de baixo para cima.

- Se a estante possuir um dispositivo de estabilização, instale-o antes de montar ou reparar a unidade.

¡Atención! Para evitar lesiones durante el montaje de este equipo sobre un bastidor, o posteriormente durante su mantenimiento, se debe poner mucho cuidado en que el sistema quede bien estable. Para garantizar su seguridad, proceda según las siguientes instrucciones:

- El Juniper Networks services gateway debe instalarse en un bastidor fijado a la estructura del edificio.

- Colocar el equipo en la parte inferior del bastidor, cuando sea la única unidad en el mismo.

- Cuando este equipo se vaya a instalar en un bastidor parcialmente ocupado, comenzar la instalación desde la parte inferior hacia la superior colocando el equipo más pesado en la parte inferior.

- Si el bastidor dispone de dispositivos estabilizadores, instalar éstos antes de montar o proceder al mantenimiento del equipo instalado en el bastidor.

Varning! För att undvika kroppsskada när du installerar eller utför underhållsarbete på denna enhet på en ställning måste du vidta särskilda försiktighetsåtgärder för att försäkra dig om att systemet står stadigt. Följande riktlinjer ges för att trygga din säkerhet:

- Juniper Networks services gateway måste installeras i en ställning som är förankrad i byggnadens struktur.

- Om denna enhet är den enda enheten på ställningen skall den installeras längst ned på ställningen.

- Om denna enhet installeras på en delvis fylld ställning skall ställningen fyllas nedifrån och upp, med de tyngsta enheterna längst ned på ställningen.

- Om ställningen är försedd med stabiliseringsdon skall dessa monteras fast innan enheten installeras eller underhålls på ställningen.

RELATED DOCUMENTATION

CHAPTER 21

Laser and LED Safety Guidelines and Warnings

SRX100 Services Gateway Laser and LED Safety Guidelines and Warnings

Observe the following guidelines and warnings when working around the SRX100 Services Gateway:

Laser and LED Safety Guidelines and Warnings

General Laser Safety Guidelines

When working around devices, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.

- Do not examine unterminated optical ports with optical instruments.

- Avoid direct exposure to the beam.

> **WARNING:** Unterminated optical connectors can emit invisible laser radiation. The lens in the human eye focuses all the laser power on the retina, so focusing the eye directly on a laser source—even a low-power laser—could permanently damage the eye.

Class 1 Laser Product Warning

WARNING: Class 1 laser product.

Waarschuwing Klasse-1 laser produkt.

Varoitus Luokan 1 lasertuote.

Attention Produit laser de classe I.

Warnung Laserprodukt der Klasse 1.

Avvertenza Prodotto laser di Classe 1.

Advarsel Laserprodukt av klasse 1.

Aviso Produto laser de classe 1.

¡Atención! Producto láser Clase I.

Varning! Laserprodukt av klass 1.

Class 1 LED Product Warning

WARNING: Class 1 LED product.

Waarschuwing Klasse 1 LED-product.

Varoitus Luokan 1 valodiodituote.

Attention Alarme de produit LED Class I.

Warnung Class 1 LED-Produktwarnung.

Avvertenza Avvertenza prodotto LED di Classe 1.

Advarsel LED-produkt i klasse 1.

Aviso Produto de classe 1 com LED.

¡Atención! Aviso sobre producto LED de Clase 1.

Varning! Lysdiodprodukt av klass 1.

Laser Beam Warning

> **WARNING:** Do not stare into the laser beam or view it directly with optical instruments.
>
> **Waarschuwing** Niet in de straal staren of hem rechtstreeks bekijken met optische instrumenten.
>
> **Varoitus** Älä katso säteeseen äläkä tarkastele sitä suoraan optisen laitteen avulla.
>
> **Attention** Ne pas fixer le faisceau des yeux, ni l'observer directement à l'aide d'instruments optiques.
>
> **Warnung** Nicht direkt in den Strahl blicken und ihn nicht direkt mit optischen Geräten prüfen.
>
> **Avvertenza** Non fissare il raggio con gli occhi né usare strumenti ottici per osservarlo direttamente.
>
> **Advarsel** Stirr eller se ikke direkte p strlen med optiske instrumenter.
>
> **Aviso** Não olhe fixamente para o raio, nem olhe para ele directamente com instrumentos ópticos.
>
> **¡Atención!** No mirar fijamente el haz ni observarlo directamente con instrumentos ópticos.
>
> **Varning!** Rikta inte blicken in mot strålen och titta inte direkt på den genom optiska instrument.

Radiation from Open Port Apertures Warning

WARNING: Because invisible radiation may be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.

Waarschuwing Aangezien onzichtbare straling vanuit de opening van de poort kan komen als er geen fiberkabel aangesloten is, dient blootstelling aan straling en het kijken in open openingen vermeden te worden.

Varoitus Koska portin aukosta voi emittoitua näkymätöntä säteilyä, kun kuitukaapelia ei ole kytkettynä, vältä säteilylle altistumista äläkä katso avoimiin aukkoihin.

Attention Des radiations invisibles à l'il nu pouvant traverser l'ouverture du port lorsqu'aucun câble en fibre optique n'y est connecté, il est recommandé de ne pas regarder fixement l'intérieur de ces ouvertures.

Warnung Aus der Port-Öffnung können unsichtbare Strahlen emittieren, wenn kein Glasfaserkabel angeschlossen ist. Vermeiden Sie es, sich den Strahlungen auszusetzen, und starren Sie nicht in die Öffnungen!

Avvertenza Quando i cavi in fibra non sono inseriti, radiazioni invisibili possono essere emesse attraverso l'apertura della porta. Evitate di esporvi alle radiazioni e non guardate direttamente nelle aperture.

Advarsel Unngå utsettelse for stråling, og stirr ikke inn i åpninger som er åpne, fordi usynlig stråling kan emiteres fra portens åpning når det ikke er tilkoblet en fiberkabel.

Aviso Dada a possibilidade de emissão de radiação invisível através do orifício da via de acesso, quando esta não tiver nenhum cabo de fibra conectado, deverá evitar a exposição à radiação e não deverá olhar fixamente para orifícios que se encontrarem a descoberto.

¡Atención! Debido a que la apertura del puerto puede emitir radiación invisible cuando no existe un cable de fibra conectado, evite mirar directamente a las aperturas para no exponerse a la radiación.

Varning! Osynlig strålning kan avges från en portöppning utan ansluten fiberkabel och du bör därför undvika att bli utsatt för strålning genom att inte stirra in i oskyddade öppningar.

RELATED DOCUMENTATION

CHAPTER 22

Maintenance and Operational Safety Guidelines and Warnings

IN THIS CHAPTER

SRX100 Services Gateway Maintenance and Operational Safety Guidelines and Warnings

IN THIS SECTION

As you maintain the services gateway, observe the following guidelines and warnings:

Safety Guidelines and Warnings

Battery Handling Warning

WARNING: Replacing the battery incorrectly might result in an explosion. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Waarschuwing Er is ontploffingsgevaar als de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type dat door de fabrikant aanbevolen is. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften weggeworpen te worden.

Varoitus Räjähdyksen vaara, jos akku on vaihdettu väärään akkuun. Käytä vaihtamiseen ainoastaan saman- tai vastaavantyyppistä akkua, joka on valmistajan suosittelema. Hävitä käytetyt akut valmistajan ohjeiden mukaan.

Attention Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

Warnung Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Avvertenza Pericolo di esplosione se la batteria non è installata correttamente. Sostituire solo con una di tipo uguale o equivalente, consigliata dal produttore. Eliminare le batterie usate secondo le istruzioni del produttore.

Advarsel Det kan være fare for eksplosjon hvis batteriet skiftes på feil måte. Skift kun med samme eller tilsvarende type som er anbefalt av produsenten. Kasser brukte batterier i henhold til produsentens instruksjoner.

Aviso Existe perigo de explosão se a bateria for substituída incorrectamente. Substitua a bateria por uma bateria igual ou de um tipo equivalente recomendado pelo fabricante. Destrua as baterias usadas conforme as instruções do fabricante.

¡Atención! Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

Varning! Explosionsfara vid felaktigt batteribyte. Ersätt endast batteriet med samma batterityp som rekommenderas av tillverkaren eller motsvarande. Följ tillverkarens anvisningar vid kassering av använda batterier.

Jewelry Removal Warning

WARNING: Before working on equipment that is connected to power lines, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.

Waarschuwing Alvorens aan apparatuur te werken die met elektrische leidingen is verbonden, sieraden (inclusief ringen, kettingen en horloges) verwijderen. Metalen voorwerpen worden warm wanneer ze met stroom en aarde zijn verbonden, en kunnen ernstige brandwonden veroorzaken of het metalen voorwerp aan de aansluitklemmen lassen.

Varoitus Ennen kuin työskentelet voimavirtajohtoihin kytkettyjen laitteiden parissa, ota pois kaikki korut (sormukset, kaulakorut ja kellot mukaan lukien). Metalliesineet kuumenevat, kun ne ovat yhteydessä sähkövirran ja maan kanssa, ja ne voivat aiheuttaa vakavia palovammoja tai hitsata metalliesineet kiinni liitäntänapoihin.

Attention Avant d'accéder à cet équipement connecté aux lignes électriques, ôter tout bijou (anneaux, colliers et montres compris). Lorsqu'ils sont branchés à l'alimentation et reliés à la terre, les objets métalliques chauffent, ce qui peut provoquer des blessures graves ou souder l'objet métallique aux bornes.

Warnung Vor der Arbeit an Geräten, die an das Netz angeschlossen sind, jeglichen Schmuck (einschließlich Ringe, Ketten und Uhren) abnehmen. Metallgegenstände erhitzen sich, wenn sie an das Netz und die Erde angeschlossen werden, und können schwere Verbrennungen verursachen oder an die Anschlußklemmen angeschweißt werden.

Avvertenza Prima di intervenire su apparecchiature collegate alle linee di alimentazione, togliersi qualsiasi monile (inclusi anelli, collane, braccialetti ed orologi). Gli oggetti metallici si riscaldano quando sono collegati tra punti di alimentazione e massa: possono causare ustioni gravi oppure il metallo può saldarsi ai terminali.

Advarsel Fjern alle smykker (inkludert ringer, halskjeder og klokker) før du skal arbeide på utstyr som er koblet til kraftledninger. Metallgjenstander som er koblet til kraftledninger og jord blir svært varme og kan forårsake alvorlige brannskader eller smelte fast til polene.

Aviso Antes de trabalhar em equipamento que esteja ligado a linhas de corrente, retire todas as jóias que estiver a usar (incluindo anéis, fios e relógios). Os objectos metálicos aquecerão em contacto com a corrente e em contacto com a ligação à terra, podendo causar queimaduras graves ou ficarem soldados aos terminais.

¡Atención! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando

se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

Varning! Tag av alla smycken (inklusive ringar, halsband och armbandsur) innan du arbetar på utrustning som är kopplad till kraftledningar. Metallobjekt hettas upp när de kopplas ihop med ström och jord och kan förorsaka allvarliga brännskador; metallobjekt kan också sammansvetsas med kontakterna.

Lightning Activity Warning

WARNING: Do not work on the system or connect or disconnect cables during periods of lightning activity.

Waarschuwing Tijdens onweer dat gepaard gaat met bliksem, dient u niet aan het systeem te werken of kabels aan te sluiten of te ontkoppelen.

Varoitus Älä työskentele järjestelmän parissa äläkä yhdistä tai irrota kaapeleita ukkosilmalla.

Attention Ne pas travailler sur le système ni brancher ou débrancher les câbles pendant un orage.

Warnung Arbeiten Sie nicht am System und schließen Sie keine Kabel an bzw. trennen Sie keine ab, wenn es gewittert.

Avvertenza Non lavorare sul sistema o collegare oppure scollegare i cavi durante un temporale con fulmini.

Advarsel Utfør aldri arbeid på systemet, eller koble kabler til eller fra systemet når det tordner eller lyner.

Aviso Não trabalhe no sistema ou ligue e desligue cabos durante períodos de mau tempo (trovoada).

¡Atención! No operar el sistema ni conectar o desconectar cables durante el transcurso de descargas eléctricas en la atmósfera.

Varning! Vid åska skall du aldrig utföra arbete på systemet eller ansluta eller koppla loss kablar.

Operating Temperature Warning

WARNING: To prevent the services gateway from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature of 104°F (40°C). To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Waarschuwing Om te voorkomen dat welke services gateway van de Juniper Networks services gateway dan ook oververhit raakt, dient u deze niet te bedienen op een plaats waar de maximale aanbevolen omgevingstemperatuur van 40°C wordt overschreden. Om te voorkomen dat de luchtstroom wordt beperkt, dient er minstens 15,2 cm speling rond de ventilatie-openingen te zijn.

Varoitus Ettei Juniper Networks services gateway-sarjan reititin ylikuumentuisi, sitä ei saa käyttää tilassa, jonka lämpötila ylittää korkeimman suositellun ympäristölämpötilan 40°C. Ettei ilmanvaihto estyisi, tuuletusaukkojen ympärille on jätettävä ainakin 15,2 cm tilaa.

Attention Pour éviter toute surchauffe des routeurs de la gamme Juniper Networks services gateway, ne l'utilisez pas dans une zone où la température ambiante est supérieure à 40°C. Pour permettre un flot d'air constant, dégagez un espace d'au moins 15,2 cm autour des ouvertures de ventilations.

Warnung Um einen services gateway der services gateway vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene Maximum von 40°C überschreitet. Um Lüftungsverschluß zu verhindern, achten Sie darauf, daß mindestens 15,2 cm lichter Raum um die Lüftungsöffnungen herum frei bleibt.

Avvertenza Per evitare il surriscaldamento dei services gateway, non adoperateli in un locale che ecceda la temperatura ambientale massima di 40°C. Per evitare che la circolazione dell'aria sia impedita, lasciate uno spazio di almeno 15.2 cm di fronte alle aperture delle ventole.

Advarsel Unngå overoppheting av eventuelle rutere i Juniper Networks services gateway Disse skal ikke brukes på steder der den anbefalte maksimale omgivelsestemperaturen overstiger 40°C (104°F). Sørg for at klaringen rundt lufteåpningene er minst 15,2 cm (6 tommer) for å forhindre nedsatt luftsirkulasjon.

Aviso Para evitar o sobreaquecimento do encaminhador Juniper Networks services gateway, não utilize este equipamento numa área que exceda a temperatura máxima recomendada de 40°C. Para evitar a restrição à circulação de ar, deixe pelo menos um espaço de 15,2 cm à volta das aberturas de ventilação.

¡Atención! Para impedir que un encaminador de la serie Juniper Networks services gateway se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40$^\text{o}$C. Para impedir la restricción de la entrada de aire, deje un espacio mínimo de 15,2 cm alrededor de las aperturas para ventilación.

Varning! Förhindra att en Juniper Networks services gateway överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40$^\text{o}$C överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.

Product Disposal Warning

WARNING: Disposal of this product must be handled according to all national laws and regulations.

Waarschuwing Dit produkt dient volgens alle landelijke wetten en voorschriften te worden afgedankt.

Varoitus Tämän tuotteen lopullisesta hävittämisestä tulee huolehtia kaikkia valtakunnallisia lakeja ja säännöksiä noudattaen.

Attention La mise au rebut définitive de ce produit doit être effectuée conformément à toutes les lois et réglementations en vigueur.

Warnung Dieses Produkt muß den geltenden Gesetzen und Vorschriften entsprechend entsorgt werden.

Avvertenza L'eliminazione finale di questo prodotto deve essere eseguita osservando le normative italiane vigenti in materia

Advarsel Endelig disponering av dette produktet må skje i henhold til nasjonale lover og forskrifter.

Aviso A descartagem final deste produto deverá ser efectuada de acordo com os regulamentos e a legislação nacional.

¡Atención! El desecho final de este producto debe realizarse según todas las leyes y regulaciones nacionales

Varning! Slutlig kassering av denna produkt bör skötas i enlighet med landets alla lagar och föreskrifter.

RELATED DOCUMENTATION

Electrical Safety Guidelines and Warnings

IN THIS CHAPTER

SRX100 Services Gateway Electrical Safety Guidelines and Warnings

IN THIS SECTION

When working on equipment powered by electricity, follow the guidelines described in the following topics:

Electrical Safety Guidelines and Warnings

In Case of Electrical Accident

If an electrical accident results in an injury, take the following actions in this order:

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.

2. Disconnect power from the services gateway.

3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, then call for help.

General Electrical Safety Guidelines and Warnings

- Install the services gateway in compliance with the following local, national, or international electrical codes:

- United States—National Fire Protection Association (NFPA 70), United States National Electrical Code

- Canada—Canadian Electrical Code, Part 1, CSA C22.1

- Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7

- Evaluated to the TN power system

- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.

- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.

- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.

- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.

- Operate the services gateway within marked electrical ratings and product usage instructions.

- For the services gateway and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

RELATED DOCUMENTATION

SRX100 Services Gateway Electrical and Power Requirements | 29

SRX100 Services Gateway Maintenance and Operational Safety Guidelines and Warnings | 141

SRX100 Services Gateway Agency Approvals | 152

Grounding the SRX100 Services Gateway | 52

CHAPTER 24

Agency Approvals and Regulatory Compliance Information

SRX100 Services Gateway Agency Approvals

The services gateway complies with the following standards:

- Safety

  - CSA 60950-1 (2003) Safety of Information Technology Equipment

  - UL 60950-1 (2003) Safety of Information Technology Equipment

  - EN 60950-1 (2001) Safety of Information Technology Equipment

  - IEC 60950-1 (2001) Safety of Information Technology Equipment (with country deviations)

  - EN 60825-1 +A1+A2 (1994) Safety of Laser Products - Part 1: Equipment Classification

  - EN 60825-2 (2000) Safety of Laser Products - Part 2: Safety of Optical Fiber Comm. Systems

- EMC

  - EN 300 386 V1.3.3 (2005) Telecom Network Equipment - EMC requirements

- EMI

  - FCC Part 15 Class B (2007) USA Radiated Emissions

  - EN 55022 Class B (2006) European Radiated Emissions

  - VCCI Class B (2007) Japanese Radiated Emissions

- Immunity

  - EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics

  - EN-61000-3-2 (2006) Power Line Harmonics

  - EN-61000-3-3 +A1 +A2 +A3 (1995) Power Line Voltage Fluctuations

  - EN-61000-4-2 +A1 +A2 (1995) Electrostatic Discharge

  - EN-61000-4-3 +A1+A2 (2002) Radiated Immunity

  - EN-61000-4-4 (2004) Electrical Fast Transients

  - EN-61000-4-5 (2006) Surge

  - EN-61000-4-6 (2007) Immunity to Conducted Disturbances

  - EN-61000-4-11 (2004) Voltage Dips and Sags

RELATED DOCUMENTATION

SRX100 Services Gateway Compliance Statements for EMC Requirements

IN THIS SECTION

This topic includes the following sections:

Canada

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Community

This is a Class B product.

Japan

The preceding translates as follows:

This is a Class B product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this product is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Korean

This is a Class B product.

이 기기는 가정용(B급) 전자파적합기기로서 주
로 가정에서 사용하는 것을 목적으로 하며, 모
든 지역에서 사용할 수 있습니다.

Korean Class B Warning g040914

United States

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference

to radio communications. 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.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

RELATED DOCUMENTATION

SRX100 Services Gateway Compliance Statements for Environmental Requirements

This topic includes the compliance statement for the following environmental requirement:

Lithium Battery

Batteries in this product are not based on mercury, lead, or cadmium substances. The batteries used in this product are in compliance with EU Directives 91/157/EEC, 93/86/EEC, and 98/101/EEC. The product documentation includes instructional information about the proper method of reclamation and recycling.

RELATED DOCUMENTATION