Juniper Networks | Engineering Simplicity

SRX1500 Firewall Hardware Guide

Published
2024-07-23

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

SRX1500 Firewall Hardware Guide

The information in this document is current as of the date on the title page.

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

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX1500 Firewall. After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

RELATED DOCUMENTATION

- How to Set Up Your SRX1500 Services Gateway
- Transceivers Supported on SRX1500 Services Gateways

1

CHAPTER

Fast Track: Initial Installation

Fast Track to Rack Installation and Power

SUMMARY

This procedure guides you through the simplest steps to install your SRX1500 Firewall in a rack and connect it to power. Have more complex installation needs? See "Installing the SRX1500 Firewall in a Rack" on page 44.

IN THIS SECTION

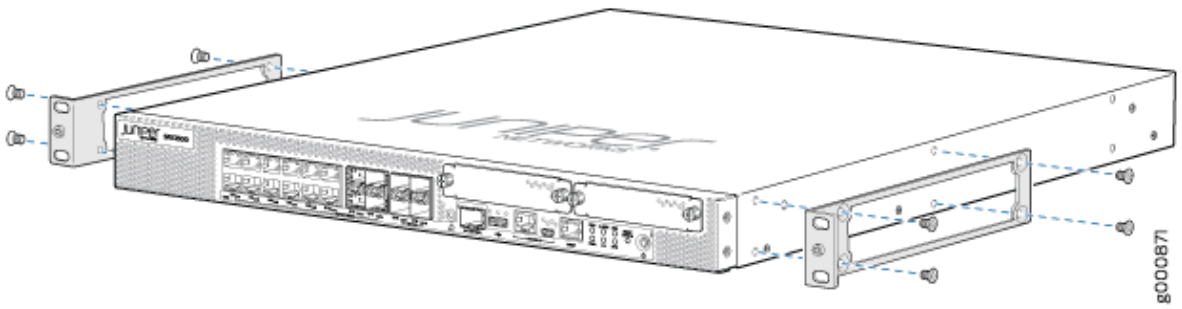
Install the SRX1500 in a Rack

You can install the SRX1500 Firewall in a two-post rack or cabinet. We'll walk you through the steps to install an AC-powered firewall in a two-post rack.

Before you install, review the following:

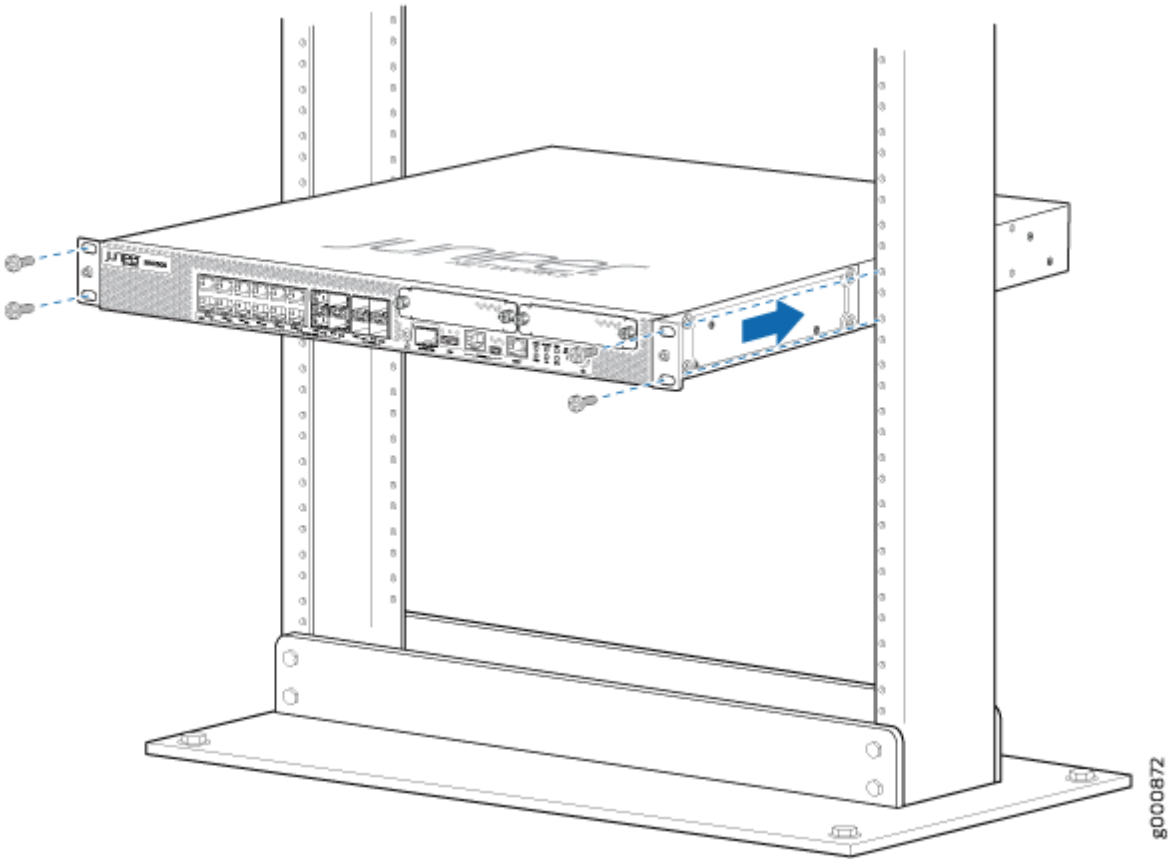
- "SRX1500 Site Guidelines and Requirements" on page 28.
- General Safety Guidelines and Warnings.
- "Unpacking the SRX1500 Firewall" on page 42.

1. Wrap and fasten one end of the electrostatic discharge (ESD) grounding strap around your bare wrist, and connect the other end to a site ESD point.
2. Attach the mounting brackets to the sides of the SRX1500 using the eight M4x6-mm Phillips flat-head mounting screws.



3. Lift the SRX1500 and position it in the rack. Line up the bottom hole in each mounting bracket with a hole in each mounting rail, making sure the SRX1500 is level.

4. While you're holding the SRX1500 in place, have a second person insert and tighten the rack mount screws to secure the mounting brackets to the mounting rails. Make sure they tighten the screws in the two bottom holes first and then tighten the screws in the two top holes.



5. Double-check that the mounting brackets on each side of the rack are level.

Connect to Power

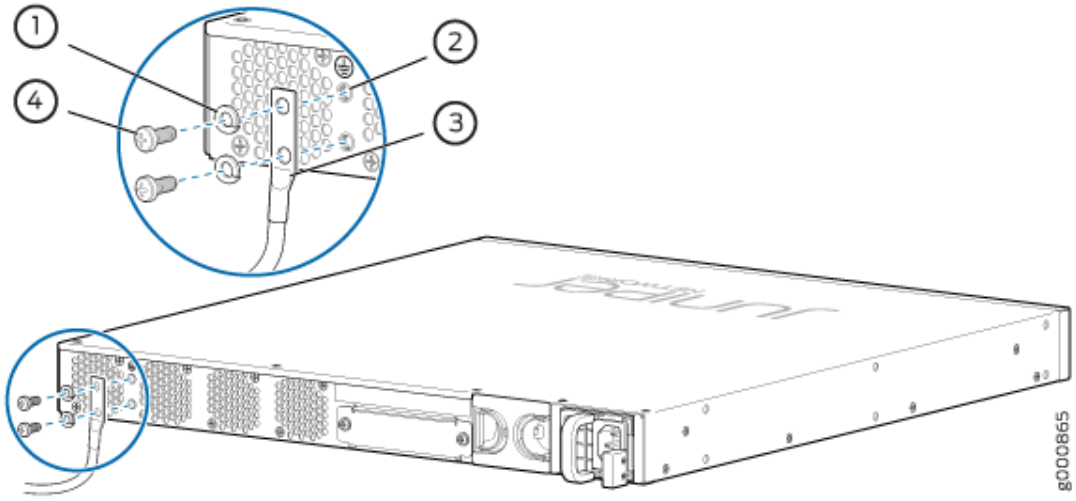
IN THIS SECTION

To connect the SRX1500 Firewall to AC power, you must do the following:

Ground the SRX1500 Firewall

To ground the SRX1500 Firewall, do the following:

1. Attach an ESD grounding strap to your bare wrist, and then connect the strap to the ESD point on the SRX1500 front panel.
2. Connect the grounding cable to a proper earth ground, such as the rack in which you mount the device.
3. Attach the grounding cable to the SRX1500's grounding points on the rear panel.
4. Dress the grounding cable. Ensure that the cable doesn't block access to or come in contact with other device components, and that it doesn't drape where people could trip over it.

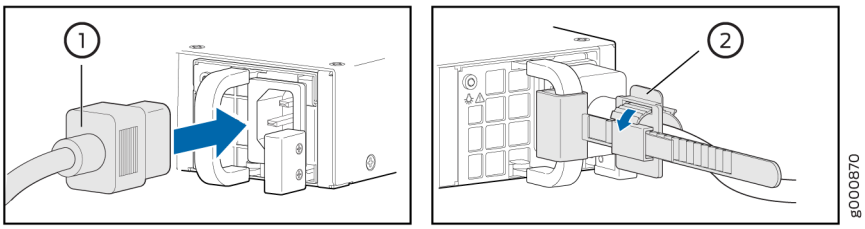


Connect the Power Cord and Power On the Firewall

For information about the supported AC power cord specifications, see "SRX1500 Firewall Supported AC Power Cords" on page 21.

To connect the power cord, do the following:

1. Ensure that the power supply is fully inserted in the rear panel of the firewall.
2. Plug the power cord into the SRX1500 rear panel. Use a power cord retainer (not included) to hold the power cord in place.



3. If the AC power source outlet has a power switch, turn it off.
4. Plug the power cord into an AC power source outlet.
5. If the AC power source outlet has a power switch, turn it on. The firewall doesn't have a power switch and powers on as soon as you plug it in.

Claim, Onboard, and Configure SRX1500

SUMMARY

This topic provides you the pointers to claim, onboard, and configure SRX1500 firewalls using Mist or Juniper® Security Director, or configure SRX1500 firewalls using J-Web or Junos OS CLI.

If you have a Mist Wired Assurance license, you can follow a few simple steps to get an SRX1500 up and running in the Juniper® Mist AI cloud portal. See Table 1 on page 5.

Table 1: Claim, Onboard, and Configure SRX1500 Using Mist

If you want to	Then
Claim and onboard to Mist	See Cloud-Ready SRX Series Firewalls with Mist
Configure Wired Assurance	See Juniper Mist Wired Assurance Configuration Guide
See all documentation available for Wired Assurance	Visit Wired Assurance Documentation

If you have a Juniper® Security Director license, you can follow a few simple steps to get an SRX1500 up and running on the Juniper® Security Director Cloud portal. See Table 2 on page 6 for more information.

Table 2: Onboard and Configure SRX1500 Using Juniper® Security Director

If you want to	Then
Claim and onboard to Juniper® Security Director Cloud	See Onboard SRX Series Firewalls to Security Director Cloud
Configure additional features	See Juniper Security Director Cloud User Guide

You can configure the SRX1500 using the J-Web GUI. See Table 3 on page 6 for more information.

Table 3: Configure SRX1500 Using J-Web

If you want to	Then
Customize basic configuration	See "Configuring the SRX1500 Firewall Using J-Web" on page 57
Configure additional features using J-Web	See J-Web for SRX Series Documentation
Set up your SRX1500 with advanced security measures to protect and defend your network	See SRX Series Up and Running with Advanced Security Features
See, automate, and protect your network with Juniper Security	Visit the Security Design Center
Download, activate, and manage your software licenses to unlock additional features for your SRX firewall	See Activate Junos Licenses in the Juniper Licensing Guide

You can also configure the SRX1500 using the Junos OS CLI. See Table 4 on page 7 for more information.

Table 4: Configure SRX1500 Using Junos OS CLI

If you want to	Then
Customize basic configuration	See "Accessing the CLI on the SRX1500 Firewall" on page 61
Explore the software features supported on the SRX1500	See Feature Explorer
Configure Junos features on the SRX1500	See User Guides

2

CHAPTER

Overview

SRX1500 Firewall Overview

IN THIS SECTION

SRX1500 Firewall Overview

Juniper Networks SRX1500 Firewall expands the SRX Series family of security platforms. The SRX1500 Firewall is a mid-range dynamic services gateway that consolidates security functionality and uncompromised performance for small to medium enterprises. With advanced security and threat mitigation capabilities, the SRX1500 Firewall provides campus edge Integrated Security Appliance (ISA) support.

The SRX1500 Firewall has a modular 1U chassis with twelve 1G Ethernet ports, four 1G SFP ports, and four 10G SFP+ ports. It contains two slots for WAN Physical Interface Modules (PIMs), one slot for an SSD device, and two slots for power supplies.

The SRX1500 Firewall is available in two models:

- SRX1500 (AC)–SRX1500 Firewall with a 120 GB SSD (with 100 GB usable space) and AC power supply
- SRX1500 (DC)–SRX1500 Firewall with a 120 GB SSD (with 100 GB usable space) and DC power supply

The SRX1500 Firewall runs the Junos operating system (Junos OS) and supports the following features:

- Firewall support with key features such as IPsec and VPN
- Advanced security services (IPS, AppID, Content Security) and threat mitigation capabilities
- High availability
- QoS
- Secure boot

- Juniper Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud)

The services gateway runs the Junos OS and can be managed using the CLI, Junos Space, and J-Web.

SRX1500 Firewall Field Replaceable Units Overview

Field-replaceable units (FRUs) are components that you can replace at your site. The power supplies are the only FRUs on the SRX1500 Firewall. The power supplies (if redundant) are hot-swappable. You can remove and replace the power supply without powering off the services gateway or disrupting the services gateway functions.

SEE ALSO

Required Tools and Parts for Replacing the SRX1500 Firewall Components | 71

Replacing an AC Power Supply on the SRX1500 Firewall | 72

Replacing a DC Power Supply on the SRX1500 Firewall | 75

Benefits of the SRX1500 Firewall

- **High performance**—The SRX1500 supports up to 9-Gbps of firewall throughput and is suited for enterprise campus and data center edge deployments.
- **Simplified deployment with minimal manual intervention**—The Zero Touch Provisioning (ZTP) feature enables you to provision and configure the SRX1500 automatically, thereby reducing operational complexity and simplifying the provisioning of new sites.
- **Advanced threat protection**—The SRX1500 supports the intrusion prevention system (IPS), Juniper Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud), antivirus, and antispam features, which protect against potential vulnerabilities. Juniper ATP Cloud protects against zero-day attacks and other unknown threats.

RELATED DOCUMENTATION

SRX1500 Firewall Installation Overview | 41

SRX1500 Chassis

IN THIS SECTION

SRX1500 Firewall Chassis Overview

The SRX1500 Firewall chassis is a rigid sheet metal structure that houses all the other hardware components. The chassis weighs 15 lb. and measures 1.75 in. high, 17.5 in. wide, and 18.2 in. deep. The chassis installs in standard 600-mm deep (or larger) enclosed cabinets or 19-in. equipment racks.

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 device.

The services gateway must be connected to earth ground during normal operation. The protective earthing terminal on the rear of the chassis is provided to connect the services gateway to ground. Additional grounding is provided to an AC-powered services gateway when you plug its power supply into a grounded AC power receptacle.

SRX1500 Firewall Front Panel

IN THIS SECTION

Figure 1 on page 12 shows the front panel of the SRX1500 Firewall. The front panel contains LEDs, Power and Reset Config buttons, and various ports.

Figure 1: SRX1500 Firewall Front Panel

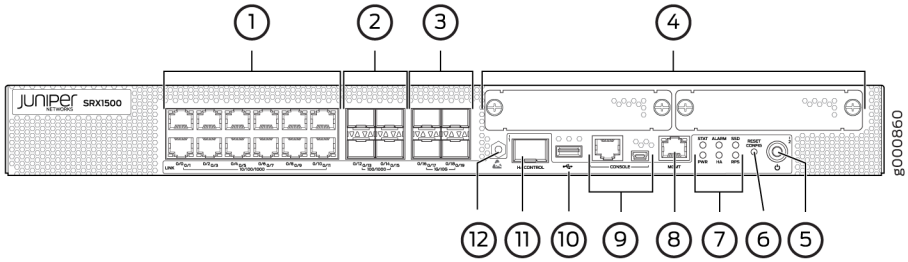


Table 5 on page 12 provides information about the front panel components of the services gateway.

Table 5: SRX1500 Firewall Front Panel Components

Callout	Component	Description
1	10/100/1000 Base-T ports	Twelve 10/100/1000 Base-T ports. Top: 0/0, 0/2, 0/4, 0/6, 0/8, and 0/10 Bottom: 0/1, 0/3, 0/5, 0/7, 0/9, and 0/11 The ports have the following characteristics: • Use an RJ-45 connector. • Operate in full-duplex and half-duplex modes. • Support flow control. • Support autonegotiation. The ports can be used to: • Function as front-end network ports. • Provide LAN and WAN connectivity to hubs, switches, local servers, and workstations. • Forward incoming data packets to the services gateway. • Receive outgoing data packets from the services gateway

Table 5: SRX1500 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
2	100/1000 SFP ports	Four 1-Gigabit Ethernet small form-factor pluggable (SFP) ports for network traffic Top: 0/12 and 0/14 Bottom: 0/13 and 0/15
3	1G/10G SFP+ ports	Four 1-Gigabit Ethernet/10-Gigabit Ethernet enhanced small form-factor pluggable (SFP+) ports for network traffic Top: 0/16 and 0/18 Bottom: 0/17 and 0/19
4	WAN PIM slots	Two WAN PIM slots. WAN PIMs are used to add WAN interfaces to the services gateway. **NOTE**: The WAN PIMs are currently not available for ordering.
5	Power button	Use the Power button to shut down the services gateway. On a services gateway that has been previously shut down using the Power button, when the power button is pressed again the services gateway starts up.
6	Reset config button	Returns the services gateway to the factory-default configuration.
7	LEDs	Indicate component and system status and troubleshooting information at a glance. See Table 6 on page 14.
8	Management port	Use the management (MGMT) port to connect to the device over the network.
9	Console port	• Serial—Connects a laptop to the services gateway for CLI management. The port uses an RJ-45 serial connection, is configured as DTE, and supports the RS-232 (EIA-232) standard. • USB—Connects a laptop to the services gateway for CLI management through a USB interface. The port accepts a Mini-B type USB cable plug. A USB cable with Mini-B and Type A USB plugs is supplied with the services gateway. To use the mini-USB console port, you must download a USB driver to the management device from the Silicon Labs page.

Table 5: SRX1500 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
10	USB port	The services gateway has one USB port that accepts a USB storage device.
11	HA control port	Dedicated Gigabit Ethernet SFP port to synchronize data and maintain state information in a chassis cluster setup.
12	ESD point	For personal safety, while working on the services gateway, use the ESD outlet to plug in an ESD grounding strap to prevent your body from sending static charges to the services gateway.

NOTE: For information on supported transceivers, see the Hardware Compatibility Tool.

Figure 2 on page 14 shows the SRX1500 Firewall LEDs.

Figure 2: SRX1500 Firewall Front Panel LEDs

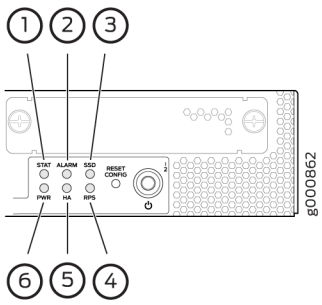


Table 6 on page 14 lists the SRX1500 Firewall LEDs.

Table 6: SRX1500 Firewall LEDs

Callout	LED	Description
1	STAT	• Solid green—operating normally

Table 6: SRX1500 Firewall LEDs *(Continued)*

Callout	LED	Description
2	ALARM	• Solid amber—noncritical alarm • Solid red—critical alarm • Off—no alarms
3	SSD	• Blinking green—the services gateway is transferring data to or from the SSD storage device • Off—SSD storage device not present
4	RPS	• Solid green—the redundant power supply is operating normally • Solid red—the redundant power supply is not operating normally • Off—no redundant power supply
5	HA	• Off—HA is disabled. • Solid green—all HA links are available. • Solid amber—some HA links are unavailable. • Solid red—device is inoperable due to a monitor failure
6	PWR	• Solid green—receiving power • Blinking green—receiving power. The services gateway is in the bootup phase before OS initialization. • Solid red—power supply unit failure

Management Port LEDs

The management port has two LEDs that indicate link activity and status of the management port.

Table 7 on page 16 describes the LEDs.

Table 7: Management Port LEDs

LED	Description
Link (LED on the left)	• Solid green—A link is established. • Off—There is no link established.
Activity (LED on the right)	• Blinking green—There is activity on the link. • Off—There is no link activity.

Network Port LEDs

The SFP and Ethernet ports have two status LEDs, LINK and ACT, located above the port.

Table 8: Network Port LEDs

LED	Description
LINK (LED on the left)	• Solid green—A link is established. • Off—There is no link established.
ACT (LED on the right)	• Blinking green—There is activity on the 1 G link. • Off—There is no link activity.

HA Port LEDs

The HA port has two LEDs located above the port to indicate status.

Table 9: HA Port LEDs

LED	Description
Link (LED on the left)	• Solid green—A link is established. • Off—There is no link established.
Activity (LED on the right)	• Blinking green—There is activity on the link. • Off—There is no link activity.

SRX1500 Firewall Back Panel

Figure 3 on page 17 shows the back panel of the SRX1500 Firewall and Table 10 on page 17 lists the back panel components.

Figure 3: SRX1500 Firewall Back Panel

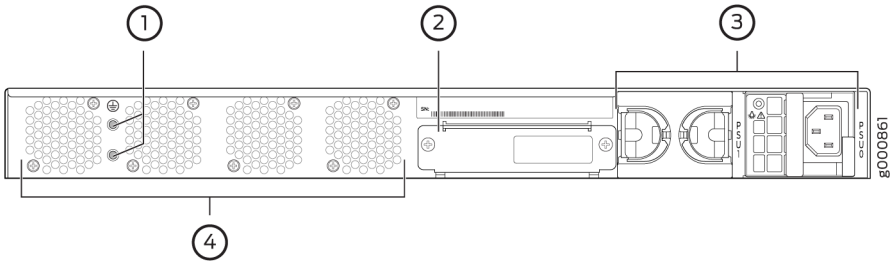


Table 10: SRX1500 Firewall Back Panel Components

Callout	Component	Description
1	Grounding point	Connects the services gateway chassis to earth ground.
2	SSD slot	Contains the SSD storage device.

Table 10: SRX1500 Firewall Back Panel Components *(Continued)*

Callout	Component	Description
3	Power supply	Two power supply slots. Each power supply contains a power cord outlet. One 400 W AC or 650 W DC power supply is provided with the services gateway.
4	Fans	Four fans for cooling the services gateway and its components.

RELATED DOCUMENTATION

SRX1500 Firewall Installation Overview | 41

SRX1500 Cooling System

The services gateway has a single fan tray that contains four fixed fans. The fan controller constantly monitors the temperature of the services gateway and its components. Under normal operating conditions, the fans function at lower than full speed. Note that the fan tray is not field-replaceable.

If any one of the four fans fails, the services gateway generates a warning but keeps the system running. If the temperature keeps rising, the services gateway lowers the power consumption by reducing the performance or shutting down some of the chassis components. However, if the ambient maximum temperature exceeds the warning level and the system cannot be adequately cooled, then the services gateway shuts down the system and hardware components completely.

RELATED DOCUMENTATION

SRX1500 Firewall Clearance Requirements for Airflow and Hardware Maintenance | 32

SRX1500 Power System

IN THIS SECTION

SRX1500 Firewall Power Supply

The power supplies are located on the rear of the chassis. The SRX1500 Firewall uses either one AC or one DC power supply unit.

A second AC or DC power supply can be used with its matching type of power supply to provide redundancy. Each power supply provides power to all components in the services gateway. When two power supplies are present, they share power almost equally within a fully populated system. The two power supplies provide power redundancy. If one power supply fails or is removed, the remaining power supply redistributes the electrical load without interruption. The services gateway reassesses the power required to support its configuration and issues errors if the available power is insufficient.

Each power supply is cooled by its own internal cooling system.

NOTE: Only redundant power supplies (AC or DC) support hot-swappable functionality.

Figure 4 on page 20 shows the AC power supply.

Figure 4: AC Power Supply for the SRX1500 Firewall

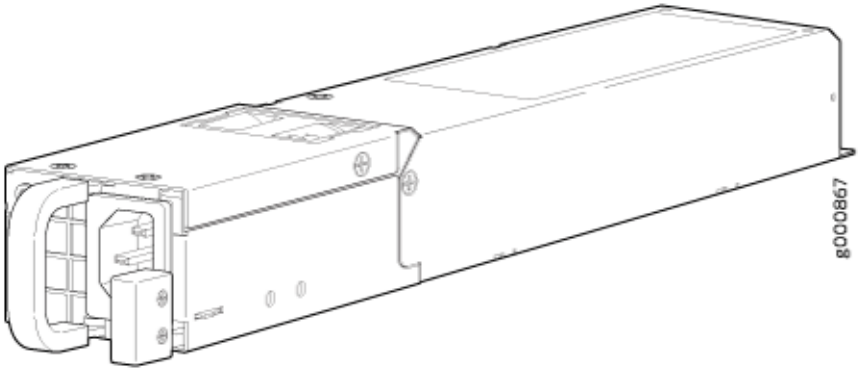
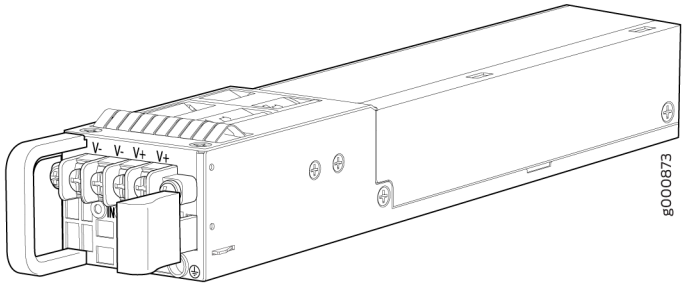


Figure 5 on page 20 shows the DC power supply.

Figure 5: DC Power Supply for the SRX1500 Firewall



CAUTION: Do not mix AC and DC power supplies within the same services gateway. Damage to the device might occur.

The power supplies produce and distribute different output voltages to the services gateway components according to their voltage requirements.

Table 11 on page 20 lists the power consumption values for the power supplies.

Table 11: Component Power Output/Consumption

Power Supply	Output/Consumption
400 W AC power supply	400 W @12 V

Table 11: Component Power Output/Consumption *(Continued)*

Power Supply	Output/Consumption
650 W DC power supply	650 W @12 V

SEE ALSO

Powering On the SRX1500 Services Gateway | 51

Powering Off the SRX1500 Firewall | 52

SRX1500 Firewall Supported AC Power Cords

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

NOTE: In North America, AC power cords must not exceed 4.5 m (approximately 14.75 ft) in length, to comply with National Electrical code (NEC) Section 400-8 (NFPA 75, 5-2.2) and 210-52, and Canadian Electrical Code (CEC) Section 4-010(3).

Table 12 on page 21 provides power cord specifications, and Figure 6 on page 22 depicts the plug on the AC power cord provided for each country or region.

Table 12: AC Power Cord Specifications

Country	Electrical Specification	Plug Standards
Australia	250 VAC, 10 A, 50 Hz	AS/NZ 3112-1993
China	250 VAC, 10 A, 50 Hz	GB2099.1 1996 and GB 1002 1996 (CH1-10P)
Europe (except Italy and United Kingdom)	250 VAC, 10 A, 50 Hz	CEE (7) VII

Table 12: AC Power Cord Specifications *(Continued)*

Country	Electrical Specification	Plug Standards
Italy	250 VAC, 10 A, 50 Hz	CEI 23-16/VII
Japan	125 VAC, 12 A, 50 or 60 Hz	JIS 8303
North America	125 VAC, 10 A, 60 Hz	NEMA 5-15
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363A

Figure 6: AC Plug Types

NOTE: Power cords and cables must not block access to services gateway components or drape where people might trip on them.

SRX1500 Firewall AC Power Supply Electrical Specifications

Table 13 on page 22 lists the AC power supply electrical specifications for the SRX1500 Firewall.

Table 13: AC Power Supply Electrical Specifications for the SRX1500 Firewall

Power Requirement	Specification
AC input voltage	100 to 127 V ~ 2.5 A, 200 to 240 V ~ 1.3 A

Table 13: AC Power Supply Electrical Specifications for the SRX1500 Firewall *(Continued)*

Power Requirement	Specification
AC input line frequency	47 to 63 Hz

SRX1500 Firewall DC Power Supply Electrical Specifications

Table 14 on page 23 lists the DC power supply electrical specifications for the SRX1500 Firewall.

Table 14: DC Power Supply Electrical Specifications for the SRX1500 Firewall

Power Requirement	Specification
DC input voltage	–44 to –72 VDC
DC system current rating	6.2 A maximum

SRX1500 Firewall DC Power Cable Specifications

The DC power supply in slot 0 must be powered by dedicated power feeds derived from feed A, and the DC power supply in slot 1 must be powered by dedicated power feeds derived from feed B. This configuration provides the commonly deployed A/B feed redundancy for the system.

CAUTION: You must ensure that power connections maintain the proper polarity. The power source cables might be labeled **(+)** and **(–)** to indicate their polarity. There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply.

WARNING: For field-wiring connections, use copper conductors only. For other electrical safety information, see "SRX1500 Services Gateway Electrical Wiring Guidelines" on page 29.

CAUTION: Power cords and cables must not block access to services gateway components or drape where people could trip on them.

Table 15 on page 24 summarizes the specifications for the power cable(s), which you must supply.

Table 15: SRX1500 Firewall DC Power Cable Specification

Cable Type	Quantity and Specification
Power	14-16 AWG, minimum 60° C wire, or as permitted by the local code

RELATED DOCUMENTATION

SRX1500 Firewall Electrical Wiring Guidelines | 29

3

CHAPTER

Site Planning, Preparation, and Specifications

Site Preparation Checklist for the SRX1500 Firewall

Table 16 on page 26 provides a checklist of tasks you need to perform when preparing a site for installing the SRX1500 Firewall.

Table 16: Site Preparation Checklist for SRX1500 Firewall Installation

Item or Task	Additional Information	Performed By	Date	Notes
Power				
Measure distance between external power sources and device installation site.	"SRX1500 Services Gateway Electrical Wiring Guidelines" on page 29			
Locate sites for connection of system grounding.	"Connecting the SRX1500 Services Gateway Grounding Cable" on page 46			
Calculate the power consumption and requirements.	"SRX1500 Services Gateway AC Power Supply Electrical Specifications" on page 22 and "SRX1500 Services Gateway DC Power Supply Electrical Specifications" on page 23			
Environment				
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX1500 Services Gateway Environmental Specifications" on page 29			
Rack Installation				
Verify that your rack meets the minimum requirements.	"Rack Requirements" on page 34			

Table 16: Site Preparation Checklist for SRX1500 Firewall Installation *(Continued)*

Item or Task	Additional Information	Performed By	Date	Notes
Plan rack location, including required space clearances.				
If a rack is used, secure the rack to the floor and building structure.				
Cabinet Installation				
Verify that your cabinet meets the minimum requirements.	"Cabinet Requirements" on page 35			
Plan the cabinet location, including required space clearances.				
Cables				
Acquire cables and connectors.	"SRX1500 Services Gateway Supported AC Power Cords" on page 21 and "SRX1500 Services Gateway DC Power Cable Specifications" on page 23			
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.				

RELATED DOCUMENTATION

SRX1500 Firewall Installation Overview | 41

SRX1500 Site Guidelines and Requirements

IN THIS SECTION

SRX1500 Firewall General Site Installation Guidelines

The following precautions help you plan an acceptable operating environment for your SRX1500 Firewall and avoid environmentally caused equipment failures:

- For the cooling system to function properly, 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. For more information, see *Prevention of Electrostatic Discharge Damage*.
- Ensure that the blank panels are installed into empty slots to prevent any interruption or reduction in the flow of air across internal components.

NOTE: Install the services gateway only in restricted areas, such as dedicated equipment rooms and equipment closets, in accordance with Articles 110–16, 110–17, and 110–18 of the National Electrical Code, ANSI/NFPA 70.

SRX1500 Firewall Environmental Specifications

Table 17 on page 29 provides the required environmental conditions for normal SRX1500 Firewall operations. In addition, the site must be as dust-free as possible because dust can clog air intake vents, reducing the efficiency of the cooling system.

Table 17: SRX1500 Firewall Environmental Specifications

Description	Value
Altitude	No performance degradation to 10,000 ft (3048 m)
Relative humidity	Normal operation ensured in relative humidity range of 5% to 90%, noncondensing
Temperature	• Normal operation ensured in temperature range of 32° F (0° C) to 104° F (40° C) • Nonoperating storage temperature in shipping container: –40° F (–40° C) to 158° F (70° C)
Maximum thermal output	614 BTU/hour
Average heat dissipation	512 BTU / hour
Noise level	66.5 dBA

SRX1500 Firewall Electrical Wiring Guidelines

Table 18 on page 30 describes the factors you must consider while planning the electrical wiring for the SRX1500 Firewall at your site.

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

Table 18: Site Electrical Wiring Guidelines for the SRX1500 Firewall

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 **TIP**: If your site is susceptible to problems with EMC, particularly from lightning or radio transmitters, you might want to seek expert advice.

WARNING: Some ports are designed for use as intrabuilding interfaces only Type 2 or Type 4 ports, the battery return connection is to be treated as an Isolated DC return (that is, DC-I), as defined in GR-1089-CORE and require isolation from the exposed OSP cabling. To comply with NEBS requirements and protect against lightning surges and

commercial power disturbances, the intrabuilding port(s) of the device MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring. The intrabuilding port(s) of the device is suitable for connection to intrabuilding or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

SRX1500 Firewall Grounding Specifications

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, the SRX1500 Firewall must be adequately grounded before power is connected. You must provide a grounding lug to connect the services gateway to earth ground.

WARNING: Before you connect power to the services gateway, a licensed electrician must attach a cable lug to the grounding and power cables that you supply. A cable with an incorrectly attached lug can damage the services gateway (for example, by causing a short circuit).

The services gateway chassis has one grounding point on the back panel. The grounding point consists of two threaded holes spaced 0.625 in. (15.86 mm) apart.

Table 19 on page 31 lists the specifications of the grounding cable used with the device.

You must install the SRX1500 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX1500 has a two-hole protective grounding terminal provided on the chassis. Under all circumstances, use this grounding connection to ground the chassis. For AC-powered systems, you must also use the grounding wire in the AC power cord along with the two-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the two-hole protective grounding terminal.

Table 19: Grounding Cable Specifications for the SRX1500 Firewall

Grounding Requirement	Specification
Grounding cable	14 AWG single-strand wire cable
Amperage of grounding cable	Up to 25A

SEE ALSO

Connecting the SRX1500 Firewall Grounding Cable | 46

Powering On the SRX1500 Services Gateway | 51

Powering Off the SRX1500 Firewall | 52

SRX1500 Firewall Physical Specifications

Table 20 on page 32 lists the physical specifications for the services gateway.

Table 20: Physical Specifications for the SRX1500 Firewall

Physical Specification of Chassis	Value
Height	1.75 in.
Width	17.28 in.
Depth	18.2 in.
Weight	15 lb.

SEE ALSO

SRX1500 Firewall Overview | 9

SRX1500 Firewall Front Panel | 11

SRX1500 Firewall Back Panel | 17

SRX1500 Firewall Clearance Requirements for Airflow and Hardware Maintenance

When planning the installation site for the SRX1500 Firewall, you need to allow sufficient clearance around the rack. Consider the following:

- For the cooling system to function properly, the airflow around the chassis must be unrestricted. The fan tray contains four fans and provides front-to-back chassis cooling. Figure 7 on page 34 shows the direction of airflow through the chassis.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the services gateway as indicated in Table 21 on page 33.
- If you are mounting the services gateway in a rack with other equipment, ensure that the exhaust from other equipment does not blow into the intake vents of the chassis.

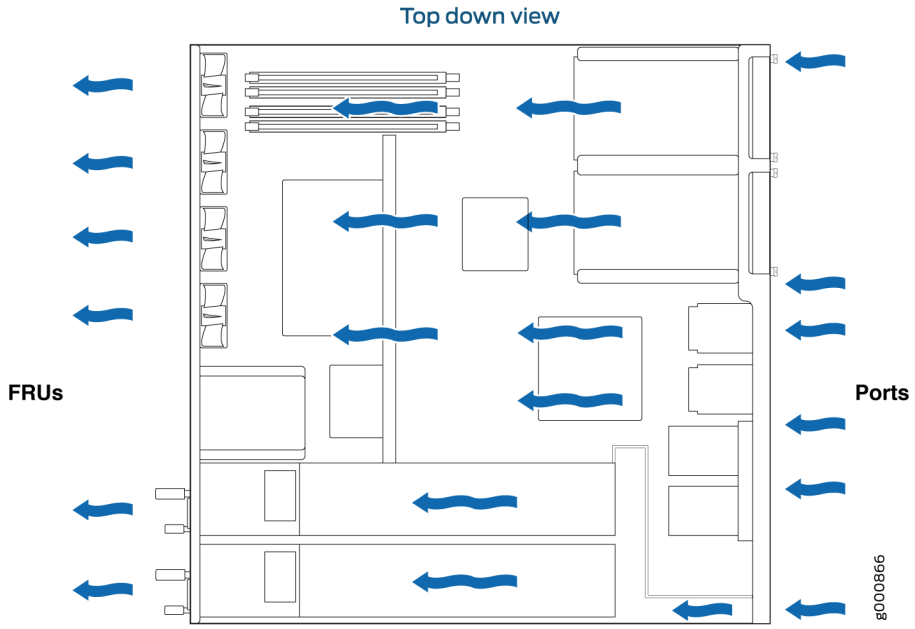
Table 21 on page 33 provides information about the clearance requirements for maintaining optimum airflow and the distances necessary to facilitate easy maintenance of the services gateway.

Table 21: Clearance Requirements for the SRX1500 Firewall

Location	Recommended Clearance	Requirement for Clearance
Front of the chassis	8.7 in. (22 cm)	Space for service personnel to remove and install hardware components
Rear of the chassis	17.4 in. (44.2 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 both sides of the chassis and any non-heat-producing surface such as a wall or cabinet side	6.0 in. (15.24 cm)	Space for the cooling system to function properly and to maintain unrestricted airflow around the chassis

Figure 7 on page 34 shows the airflow through the chassis.

Figure 7: Airflow Through the Chassis



Rack Requirements

When installing the services gateway in a rack, you must ensure that the rack complies with a 1U (19 in. or 48.7 cm) rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D), published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html).

When selecting a rack, ensure that the physical characteristics of the rack comply with the following specifications:

- 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.

The spacing of the mounting brackets and flange holes on the rack and device mounting brackets are as follows:

- The holes within each rack set are spaced at 1 U (1.75 in. or 4.5 cm).
- 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).

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.

Cabinet Requirements

You can install the services gateway in a 19 in. (48.7 cm) cabinet as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronic Industries Alliance (http://www.ecaus.org/eia/site/index.html). You must mount the services gateway horizontally in the cabinet using appropriate rack adapters.

When selecting a cabinet, ensure that it meets the following specifications:

- The cabinet is at least 1U (3.50 in. or 8.89 cm) and can accommodate the services gateway.
- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.7 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: A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

When you mount the services gateway in a cabinet, you must ensure that ventilation through the cabinet is sufficient to prevent overheating. Consider the following when planning for chassis cooling:

- Ensure that the cool air supply you provide through the cabinet can adequately dissipate the thermal output of the services gateway.
- Install the services gateway 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.

SRX1500 Transceiver Specifications and Pinouts

IN THIS SECTION

SRX1500 Transceiver Support

You can find information about the pluggable transceivers supported on your Juniper Networks device by using the Hardware Compatibility Tool. In addition to transceiver and connector type, the optical and cable characteristics—where applicable—are documented for each transceiver. The Hardware Compatibility Tool enables you to search by product, displaying all the transceivers supported on that device, or category, by interface speed or type. The list of supported transceivers for the SRX1500 is located at https://apps.juniper.net/hct/product/#prd=SRX1500.

RJ-45 Connector Pinouts for the SRX1500 Firewall Ethernet Port

The port on the front panel labeled MGMT is an autosensing 10/100/1000-Mbps Ethernet RJ-45 receptacle that accepts an Ethernet cable for connecting the services gateway to a management LAN (or other device that supports out-of-band management). Table 22 on page 36 describes the RJ-45 connector pinouts for the Ethernet port.

Table 22: RJ-45 Connector Pinouts for Services Gateway Ethernet Port

Pin	Signal
1	TX+
2	TX-

Table 22: RJ-45 Connector Pinouts for Services Gateway Ethernet Port *(Continued)*

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

RJ-45 Connector Pinouts for the SRX1500 Firewall Console Port

The SRX1500 Firewall has two console ports: an RJ-45 Ethernet port and a mini-USB Type-B port. The port on the front panel labeled CONSOLE is an asynchronous serial interface that accepts an RJ-45 connector. Table 23 on page 37 describes the RJ-45 connector pinouts for the console port.

Table 23: 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

Table 23: RJ-45 Connector Pinouts for the Services Gateway Console Port *(Continued)*

Pin	Signal	Description
5	Ground	Signal Ground
6	RXD	Receive Data
7	DSR/DCD	Data Set Ready
8	CTS	Clear to Send

Mini-USB Connector Pinouts for the SRX1500 Firewall Console Port

The SRX1500 Firewall has two console ports: an RJ-45 Ethernet port and a mini-USB Type-B port. If your management device (laptop or PC) does not have a DB-9 plug connector pin or an RJ-45 connector pin, you can connect your management device to the Mini-USB Type-B console port of the services gateway by using a cable that has a standard Type-A USB connector on one end and a Mini-USB Type-B (5-pin) connector on the other end. Table 24 on page 38 describes the Mini-USB Type-B connector pinouts for the console port.

NOTE: By design, the mini-USB console port has higher priority over the RJ-45 console port. If both mini-USB and RJ-45 console ports are connected, then the mini-USB console port will be active.

Table 24: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port

Pin	Signal	Cable Color	Description
1	VCC	Red	+5 VDC
2	D-	White	Data -

Table 24: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port *(Continued)*

Pin	Signal	Cable Color	Description
3	D+	Green	Data +
X	N/C		Could be not connected (N/C), connected to ground (GND), or used as an attached device presence indicator
4	GND	Black	Ground

RELATED DOCUMENTATION

SRX1500 Firewall Front Panel | **11**

CHAPTER 4

Initial Installation and Configuration

SRX1500 Firewall Installation Overview

After you have prepared the site for installation and unpacked the SRX1500 Firewall, you are ready to install the device. It is important to proceed through the installation process in the following order:

1. Review the safety guidelines explained in "General Electrical Safety Guidelines and Warnings" on page 110.
2. Prepare the services gateway for installation as described in "Preparing the SRX1500 Services Gateway for Rack-Mount Installation" on page 43.
3. Install the services gateway as described in "Installing the SRX1500 Services Gateway in a Rack" on page 44.
4. Connect cables to external devices as described in "Connecting the SRX1500 Services Gateway to a Network for Out-of-Band Management" on page 53 and "Connecting the SRX1500 Services Gateway to a Management Console" on page 54.
5. Connect the grounding cable as described in "Connecting the SRX1500 Services Gateway Grounding Cable" on page 46.
6. Power on the services gateway as described in "Powering On the SRX1500 Services Gateway" on page 51.

Unpacking and Mounting the SRX1500

IN THIS SECTION

Unpacking the SRX1500 Firewall

The SRX1500 Firewall is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick-start instructions.

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

To unpack the SRX1500 Firewall:

1. Move the cardboard carton to a staging area as close to the installation site as possible, where you have enough room to remove the components from the chassis.
2. Position the cardboard carton with the arrows pointing up.
3. Carefully open the top of the cardboard carton.
4. Remove the foam covering the top of the services gateway.
5. Remove the accessory box.
6. Verify the parts received against the lists in "Verifying Parts Received with the SRX1500 Services Gateway" on page 42.
7. Store the brackets and bolts inside the accessory box.
8. Save the shipping carton and packing materials in case you need to move or ship the services gateway at a later time.

Verifying Parts Received with the SRX1500 Firewall

The SRX1500 Firewall 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 carries a brief description of each part in your order.

If any part is missing, contact a customer service representative.

A fully configured services gateway contains the chassis with installed components, listed in Table 25 on page 43, and an accessory box, which contains the parts listed in Table 26 on page 43.

> **NOTE**: The parts shipped with your services gateway can vary depending on the configuration you ordered.

Table 25: Parts List for a Fully Configured SRX1500 Firewall

Component	Quantity
1U SRX1500 Firewall chassis with 12 Gigabit Ethernet LAN ports, four 1G SFP ports, four 1G/10G SFP ports, two power supply slots, four fans, and one SSD (includes blank covers for WAN PIM)	1
Front-mount rack-mount kit	1
Documentation Roadmap and Product Warranty	1
400 W AC or 650 W DC power supply **NOTE**: The shipment includes one power cord appropriate for your geographical location.	1

Two power supplies must be installed in the services gateway for redundancy.

Table 26: Accessory/Upgrade Parts List for the SRX1500 Firewall

Part	Quantity
RoHS Card	1
End User License Agreement	1

Preparing the SRX1500 Firewall for Rack-Mount Installation

You can mount an SRX1500 Firewall on four-post (telco) racks, enclosed cabinets, and open-frame racks. Center-mount racks are not supported.

Before mounting the SRX1500 Firewall in a rack:

- Verify that the site meets the requirements described in "Site Preparation Checklist for the SRX1500 Services Gateway" on page 26.
- Verify that you have the following parts available in your rack-mounting kit for the SRX1500 Firewall:
  - Rack-mounting brackets

- Screws

- Verify that the racks or cabinets meet the specific requirements described in SRX1500 Services Gateway Rack Requirements.
- 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 "Cabinet Requirements" on page 35.
- Remove the gateway chassis from the shipping carton. For unpacking instructions, see "Unpacking the SRX1500 Services Gateway" on page 42.

Installing the SRX1500 Firewall in a Rack

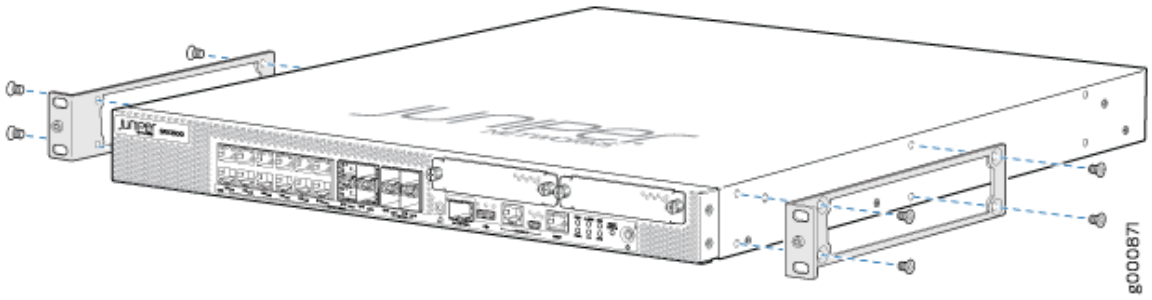
You can front-mount the SRX1500 Firewall in a rack. Many types of racks are acceptable, including four-post (telco) racks, enclosed cabinets, and open-frame racks.

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

To install the services gateway in a rack:

1. Position a mounting bracket on each side of the chassis.
2. Use a number 2 Phillips screwdriver to install the screws that secure the mounting brackets to the chassis.

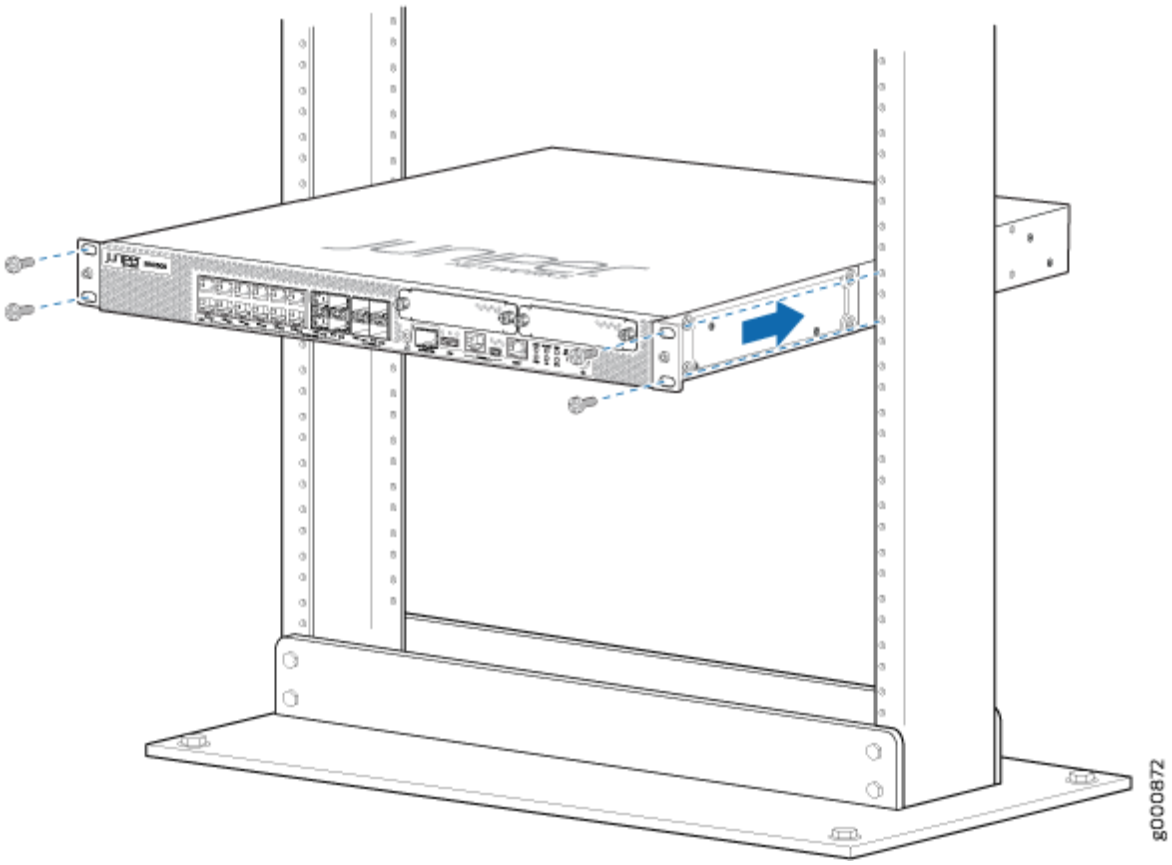
Figure 8: Installing the Mounting Brackets on the SRX1500 Firewall



3. Have one person grasp the sides of the services gateway, lift it, and position it in the rack.

4. Align the bottom hole in each mounting bracket with a hole in each rack rail, making sure the chassis is level.
5. Have a second person install a mounting screw into each of the two aligned holes. Use a number 2 Phillips screwdriver to tighten the screws.
6. Install the second screw in each mounting bracket.

Figure 9: Installing the SRX1500 Firewall in a Rack



7. Verify that the mounting screws on one side of the rack are aligned with the mounting screws on the opposite side and that the services gateway is level.

Connecting the SRX1500 to Power

IN THIS SECTION

Required Tools and Parts for Grounding the SRX1500 Services Gateway

To ground and to provide power to the services gateway, you need the following tools:

- Phillips (+) screwdrivers, numbers 1 and 2
- Electrostatic discharge (ESD) grounding wrist strap
- Wire cutters

Connecting the SRX1500 Firewall Grounding Cable

You ground the services gateway by connecting a grounding cable to earth ground and then attaching it to the chassis grounding points located on the back panel of the device using two #10-32, 0.5 inch-long grounding screws. You must install the SRX1500 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX1500 has a two-hole protective grounding terminal provided on the chassis. See Figure 10 on page 47. Under all circumstances, use this grounding connection to ground the chassis. For AC-powered systems, you must also use the grounding wire in the AC power cord along with the two-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the two-hole protective grounding terminal.

You must provide the following items:

- Two #10-32, 0.5 inch-long grounding screws

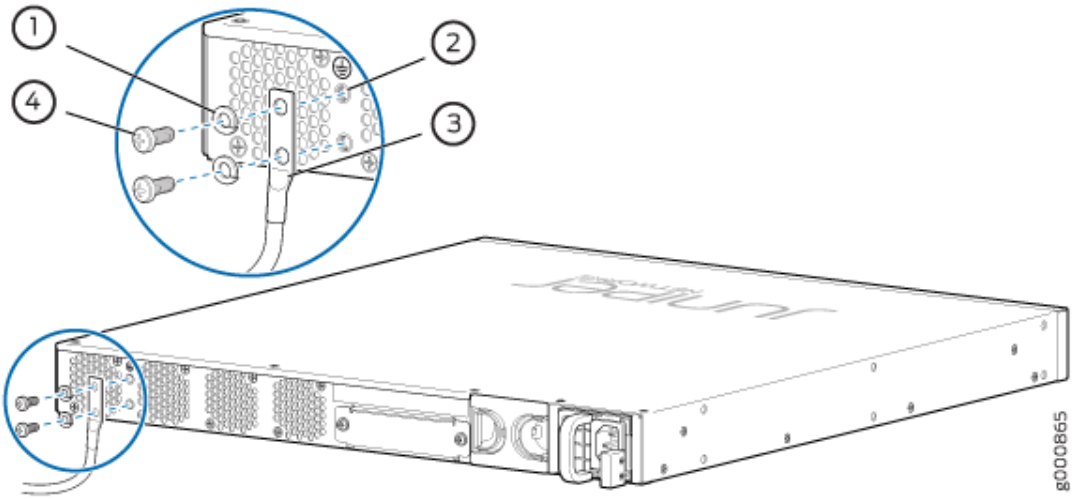
- Grounding cables
- Cable lugs (for example, Panduit LCC6-10A-L)

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

To ground the services gateway:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the chassis. For more details, see *Prevention of Electrostatic Discharge Damage*.
2. Ensure that all grounding surfaces are clean and brought to a bright finish before grounding connections are made.
3. Connect the grounding cable to a proper earth ground.
4. Place the grounding cable lugs over the grounding points (sized for #10-32, 0.5 inch-long grounding screws).

Figure 10: Connecting the Grounding Cable to the SRX1500 Firewall



5. Secure the grounding cable lugs to the grounding points, first with the washers, then with the screws.
6. 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.

Connecting the SRX1500 Firewall to an AC Power Supply

CAUTION: Do not mix AC and DC power supplies within the same services gateway. Damage to the device might occur.

You connect AC power to the services gateway by attaching the power cord from the AC power source to the AC appliance inlet located on the power supply.

To connect the services gateway to an AC power supply:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to the ESD point on the front of the chassis.
2. Insert the appliance coupler end of the power cord into the appliance inlet on the power supply.
3. Insert the power cord plug into an external AC power source receptacle.

   NOTE: Each power supply must be connected to a dedicated AC power feed and a dedicated external circuit breaker. We recommend that you use a 15 A (250 VAC) minimum, or as permitted by local code.

4. Dress the power cord appropriately. Verify that the power cord does not block the air exhaust and access to services gateway components or drape where people could trip on it.

NOTE: The services gateway must be connected to earth ground during normal operation. The protective earthing terminal on the side of the chassis is provided to connect the services gateway to ground.

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

Connecting the SRX1500 Firewall to a DC Power Supply

You connect DC power to the services gateway by attaching power cables from the external DC power sources to the terminal studs on the power supply faceplates.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the services gateway chassis before connecting power. See "Connecting the SRX1500 Services Gateway Grounding Cable" on page 46 for instructions.

WARNING: Before performing the following procedure, ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position (0), and tape the switch handle of the circuit breaker in the OFF position.

CAUTION: Do not mix AC and DC power supplies within the same services gateway. Damage to the services gateway might occur.

CAUTION: Before you connect power to the services gateway, a licensed electrician must attach appropriate cable lugs 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).

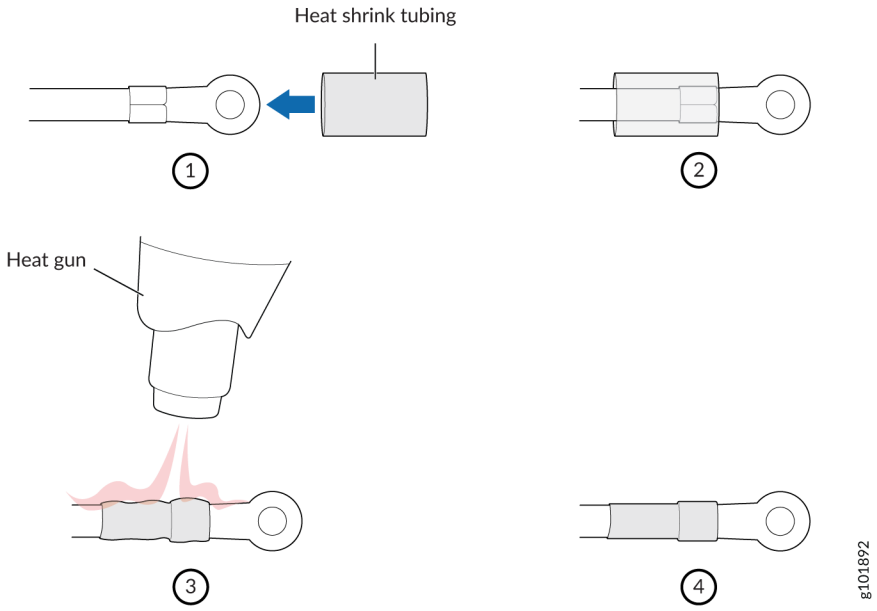
To connect the DC source power cables to the services gateway for each power supply:

1. Switch off the dedicated facility circuit breakers. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.
2. Install heat-shrink tubing insulation around the power cables:
   a. Slide the tubing over the portion of the cable where it is attached to the lug barrel. Ensure that the tubing covers the end of the wire and the barrel of the lug attached to it.
   b. Shrink the tubing with a heat gun. Ensure that you heat all sides of the tubing evenly so that it shrinks around the cable tightly.

      NOTE: Do not overheat the tubing.

      Figure 11 on page 50 shows how to install heat-shrink tubing.

Figure 11: How to Install Heat-Shrink Tubing



3. Remove the clear plastic cover that protects the terminal studs on the faceplate.
4. Verify that the DC power cables are correctly labeled before making connections to the power supply.

   In a typical power distribution scheme where the return is connected to chassis ground at the battery plant, you can use a multimeter to verify the ohm output of the -48V and RTN DC cables to chassis ground. The cable with very large resistance (indicating an open circuit) to chassis ground will be -48V, and the cable with very low resistance (indicating a closed circuit) to chassis ground will be RTN.

   CAUTION: You must ensure that power connections maintain the proper polarity. The power source cables might be labeled **(+)** and **(–)** to indicate their polarity. There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply.

5. Remove the screws and square washers from the terminals, using a Phillips (+) screwdriver, number 2.
6. Secure each power cable lug to the terminals with the square washers and the screws. Apply between 23 in.-lb (2.6 Nm) and 25 in.-lb (2.8 Nm) of torque to each screw.
   - Secure each positive (+) DC source power cable lug to a RTN (return) terminal.
   - Secure each negative (–) DC source power cable lug to a -48V (input) terminal.

7. Replace the clear plastic cover over the terminal studs on the faceplate.
8. Verify that the power cables are connected correctly, that they are not touching or blocking access to services gateway components, and they do not cause a tripping hazard.
9. Repeat Steps 1 through 8 for the second power supply, if you are installing one.

NOTE: If power is lost to the services gateway, the Power-On/Power-Off state is retained. For example, if the services gateway loses power while the device is on, when power returns, the device will still be in the On state.

Powering On the SRX1500 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 or DC power source receptacle.
   a. Using AC power supply—Insert the appliance coupler end of the power cord into the appliance inlet on the power supply and the power cord plug into an external AC power source receptacle.
   b. Using DC power supply—Connect DC power cables to the A+ and A- terminals and the other ends to an external DC power source. If you have two DC power sources and wish to deploy A/B feed redundancy for the services gateway, also connect DC power cables to the B+ and B- terminals and the other ends to an external DC power source.

   ⚠ **CAUTION**: You must ensure that power connections maintain the proper polarity. The power source cables might be labeled (+) and (–) to indicate their polarity. There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminals on the power supply.
3. Turn on the power to the AC or DC power receptacle.

The device starts automatically as the power supply completes its startup sequence. The PWR LED (on the front panel of the chassis) lights up during startup and remains solid when the services gateway is operating normally.

Powering Off the SRX1500 Firewall

To power off the device, press the Power button on the front of the device and hold it for 10 seconds. To remove power completely from the services gateway, unplug the AC power cord or DC power supply cable.

NOTE: Graceful shutdown is not supported on the SRX1500 Firewall.

After powering off a power supply, wait at least 60 seconds before turning it back on. After powering on a power supply, wait at least 10 seconds before turning it off.

When the system is completely powered off and you turn on the power supply, the services gateway starts as the power supply completes its startup sequence. If the services gateway finishes starting and you need to power off the system again, first issue the `request system halt` command.

NOTE: The fans in the power supply continue to rotate even after you power off the SRX1500 Firewall. To stop the fans, remove the power cord from the power supply. The fans stop in a few seconds.

After a power supply is turned on, it can take up to 60 seconds for status indicators—such as the POWER LED (on the front panel of the chassis) and the `show chassis` command display—to indicate that the power supply is functioning normally. Ignore error indicators that appear during the first 60 seconds.

Connecting the SRX1500 to External Devices

IN THIS SECTION

Required Tools and Parts for Connecting the SRX1500 Services Gateway

To connect the services gateway, you need the following tools and parts:

- Electrostatic discharge (ESD) grounding wrist strap
- Phillips (+) screwdrivers, numbers 1 and 2
- 2.5-mm flat-blade (-) screwdriver

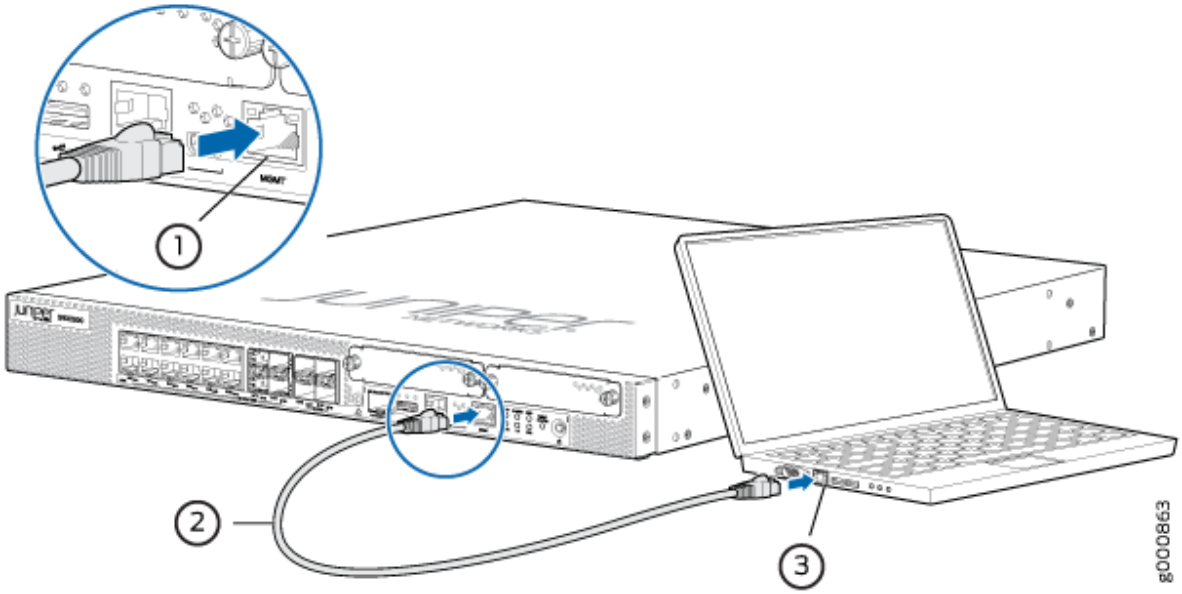
Connecting the SRX1500 Firewall to a Network for Out-of-Band Management

Use the MGMT port on the services gateway to connect to a network for out-of-band management.

To connect the management device to the SRX1500 Firewall:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Plug one end of the Ethernet cable into the MGMT port as shown in Figure 12 on page 53.

Figure 12: Connecting the SRX1500 Firewall to a Network for Out-of-Band Management



3. Plug the other end of the cable into the management device.

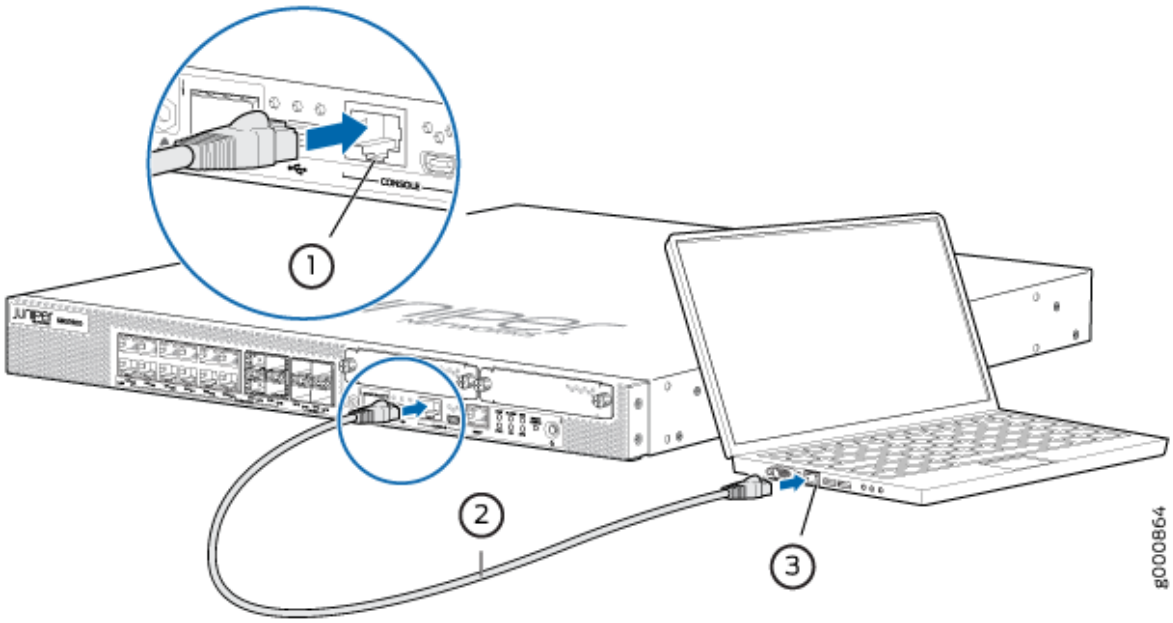
Connecting the SRX1500 Firewall to a Management Console

Use the CONSOLE port on the services gateway to connect to a management console.

To connect the SRX1500 Firewall to a management console, use an RJ-45 cable:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the strap to one of the ESD points on the chassis.
2. Plug the RJ-45 end of the cable into the CONSOLE port on the SRX1500 Firewall as shown in Figure 13 on page 54.

Figure 13: Connecting the SRX1500 Firewall to a Management Console



3. Connect the other end of the Ethernet cable to the Ethernet port on the management device.

   If the management device has a serial port, use the RJ-45 to DB-9 serial port adapter. Use the following values to configure the serial port:

   - Baud rate—9600
   - Parity—N
   - Data bits—8
   - Stop bits—1
   - Flow control—none

NOTE: Alternately, you can use the USB cable to connect to the mini-USB console port on the services gateway. To use the USB console port, you must download a USB driver to the management device from the Silicon Labs page.

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

Configuring Junos OS on the SRX1500

IN THIS SECTION

SRX1500 Firewall Software Configuration Overview

The SRX1500 Firewall is shipped with Junos OS preinstalled and ready to be configured when the services gateway is powered on. If you are setting up the services gateway for the first time, use the command-line interface (CLI) to perform the initial configuration.

Gather the following information before configuring the services gateway:

- Root authentication
- IP address of the management interface
- Default route

Understanding SRX1500 Firewall Factory-Default Settings

Your SRX1500 comes configured with a factory-default configuration. The default configuration includes the following security configuration:

- Two security zones are created: trust and untrust.
- Interfaces ge-0/0/0 and ge-0/0/15 are in the untrust zone, while interfaces ge-0/0/1 through ge-0/0/3 are in the trust zone.
- A security policy is created that permits outbound traffic from the trust zone to the untrust zone.
- Source Network Address Translation (NAT) is configured on the trust zone.

If the current active configuration fails, you can use the `load factory-default` command to revert to the factory-default configuration.

Viewing SRX1500 Firewall Factory-Default Settings

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

1. Log in as the root user and provide your credentials.
2. View the list of default config files:

```
root@srx1500>file list /etc/config
```

3. View the required default config file.

```
root@srx1500> file show /etc/config/<config
file name>
```

Accessing J-Web on the SRX1500 Services Gateway

The J-Web interface is a Web-based graphical interface that allows you to operate a services gateway without commands. Before you can use J-Web to configure your device, you must access the CLI to perform the initial configuration.

NOTE: To access the J-Web interface, your management device requires one of the following supported browsers:

- Microsoft Internet Explorer version 8.0, 9.0, or 10.0
- Mozilla Firefox version 23+
- Google Chrome version 28+

To access J-Web:

1. Open a Web browser on the management device and enter the device management IP address in the address field.
2. Specify the default username as root and enter the password.

Configuring the SRX1500 Firewall Using J-Web

IN THIS SECTION

Configuring Root Authentication and the Management Interface from the CLI

Before you can use J-Web to configure your device, you must access the CLI to perform the initial configuration.

To configure root authentication and the management interface:

1. Log in as root. There is no password.
2. Start the CLI and enter configuration mode.

```
root@% cli
root@>configure
root@#
```

3. 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
```

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

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

5. Configure the IP address and prefix length for the Ethernet management interface on the device.

```
[edit]
root@# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

6. Configure the default route.

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

7. Enable Web access to launch J-Web.

```
[edit]
root@# set system services web-management http
```

8. Commit the configuration changes.

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

Configuring Interfaces, Zones, and Policies with J-Web

IN THIS SECTION

You can configure hostnames, interfaces, zones, and security policies using J-Web.

Before you begin:

- Ensure you have configured the IP address, root authentication, and default route.
- Enable HTTP on the device to access J-Web.

  See "Configuring Root Authentication and the Management Interface from the CLI" on page 57.

Configure the device with J-Web using the following procedures.

Configuring the Hostname

To configure the hostname:

1. Launch a Web browser from the management device.
2. Enter the IP address of the device in the URL address field.
3. Specify the default username as root and enter the password. See "Configuring the SRX1500 Firewall Using J-Web" on page 57.

4. Click **Log In**. The J-Web Dashboard page appears.
5. Select **Configure>System Properties>System Identity**, and then select **Edit**. The Edit System Identity dialog box appears.
6. Enter the hostname and click **OK**.
7. Select **Commit Options>Commit** to apply the configuration changes.

You have successfully configured the hostname for the system.

Configuring Interfaces

To configure two physical interfaces:

1. From the J-Web Dashboard page, select **Configure>Interfaces** and select a physical interface you want to configure.
2. Select **Add>Logical Interface**. The Add interface dialog box appears.
3. Set **Unit** = **0**.
4. Select the check box for **IPv4 Address** to enable IPv4 addressing.
5. Click **Add** and enter the IPv4 address.
6. Click **OK**.

   A message appears after your configuration changes are validated successfully.
7. Click **OK**.
8. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
9. Click **OK**.

You have successfully configured the physical interface. Repeat these steps to configure the second physical interface for the device.

Configuring Zones and Assigning Interfaces

To assign interfaces within a trust zone and an untrust zone:

1. From the J-Web Dashboard page, select **Configure>Security>Zones/Screens** and click **Add**. The Add Zone dialog box appears.
2. In the Main tab, enter **trust** for zone name and enter the description.
3. Set the zone type to **Security**.
4. Select the interfaces listed under Available and move them under Selected.
5. Click **OK**.

   A message appears after your configuration changes are validated successfully.
6. Click **OK**.

7. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
8. Click **OK**.
9. Repeat Step 1 through Step 8 and assign another interface to an untrust zone.

You have successfully configured interfaces in a trust zone and in an untrust zone.

Configuring Security Policies

To configure security policies:

1. From the J-Web Dashboard page, select **Configure>Security>Security Policy** and click **Add**. The Add Policy dialog box appears.
2. In the Policy tab, enter the policy name and set the policy action to **permit**. Then select **Zone** and set the From Zone to **trust** and the To Zone to **untrust**.
3. Configure the source IP address by selecting **any** listed under Available and moving it under Selected.
4. Configure the destination IP address by selecting **any** listed under Available and moving it under Selected.
5. Configure the application by selecting **any** listed under Available and moving it under Selected.
6. Click **OK**.

   A message appears after your configuration changes are validated successfully.
7. Click **OK**.
8. Select **Commit Options>Commit** to apply the configuration changes.

   A message appears after your configuration changes are applied successfully.
9. Click **OK**.

You have successfully configured the security policy.

Accessing the CLI on the SRX1500 Firewall

To access the CLI on the SRX1500 Firewall:

1. Plug one end of the Ethernet cable into the RJ-45 to DB-9 serial port adapter.
2. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device.
3. Connect the other end of the Ethernet cable to the serial console port on the services gateway.

NOTE: Alternately, you can use the USB cable to connect to the mini-USB console port on the services gateway. To use the USB console port, you must download a USB driver to the management device from the Silicon Labs page.

NOTE: We no longer include the console cable as part of the device package. If the console cable and adapter are not included in your device package, or if you need a different type of adapter, you can order the following separately:

- RJ-45 to DB-9 adapter (JNP-CBL-RJ45-DB9)
- RJ-45 to USB-A adapter (JNP-CBL-RJ45-USBA)
- RJ-45 to USB-C adapter (JNP-CBL-RJ45-USBC)

If you want to use RJ-45 to USB-A or RJ-45 to USB-C adapter you must have X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

4. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate COM port to use (for example, COM1).
5. Configure the serial port settings with the following values:
   - Baud rate—9600
   - Parity—N
   - Data bits—8
   - Stop bits—1
   - Flow control—none
6. Power on the services gateway. You can start performing initial software configuration on the services gateway after the device is up.

Connecting to the SRX1500 Firewall from the CLI Remotely

To connect the services gateway to a network for out-of-band management:

1. Plug one end of an Ethernet cable with RJ-45 connectors into the MGMT port on the front panel of the services gateway.

2. Plug the other end of the cable into the management device.

Configuring the SRX1500 Firewall Using the CLI

This sample procedure explains how you can create an initial configuration using CLI commands to connect the SRX1500 Firewall to the network.

1. Verify that the device is powered on.
2. Log in as the root user. Do not enter a 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. When you are prompted, enter the password for the administrator account.

```
[edit]
root# set system login user admin class super-user authentication plain-text-password
New password: password
Retype new password: password
```

7. Commit the configuration to activate it on the services gateway.

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

8. Log in as the administrative user you configured in Step 6.
9. Configure the name of the services gateway. If the name includes spaces, enclose the name in quotation marks (“ ”).

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

10. Configure the IP address and prefix length for the services gateway Ethernet interface.

```
[edit]
admin# set interfaces fxp0 unit 0 family inet address address/prefix-length
```

11. Configure the traffic interface.

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

NOTE: The ge-0/0/0 interface is for the LAN, and the ge-0/0/1 interface is for the ISP.

12. Configure the default route.

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

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

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

14. 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
admin# set security policies from-zone trust to-zone untrust policy policy-name then permit
admin# set security policies from-zone untrust to-zone trust policy policy-name match
source-address any destination-address any application any
admin# set security policies from-zone untrust to-zone trust policy policy-name then permit
```

NOTE: The actual configuration of the policies depends on your requirements.

15. Check the configuration for validity.

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

16. Commit the configuration to activate it on the services gateway.

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

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

NOTE: This is a sample output. The actual output might vary depending on your configuration requirements.

```
admin@# show
system {
            host-name forge02;
            root-authentication {
                encrypted-password "$1$ZUlES4dp$OUwWo1g7cLoV/aMWpHUnC/"; ## SECRET-DATA
            }

            services {
```

```
                ssh;
                web-management {
                    http {
                         interface fxp0.0;

                    }
                }
            }
            syslog {
                user * {
                    any emergency;
                }
                file messages {
                    any any;
                    authorization info;
                }
                file interactive-commands {
                    interactive-commands any;
                }
            }


    security {
         policies {
             from-zone trust to-zone untrust {
                 policy trust-pol {
                     match {
                          source-address any;
                             destinataion-address any;
                         application any;
                           }
                           then {
                              permit;
                           }
                     }
               }


               from-zone untrust to-zone trust {
                     policy untrust-pol {
                         match {
                             source-address any;
                                destinataion-address any;
```

```
                           application any;
                       }
                       then {
                            permit;
                       }
                   }
                }
            }

            zones {
                security-zone trust {
                    interfaces {
                        ge-0/0/0.0;
                    }
                }
                security-zone untrust {
                    interfaces {
                        ge-0/0/1.0;
                    }
                }
             }
          }
interfaces {
    ge-0/0/0 {
        unit 0 {
             family inet {
                 address 9.0.0.254/8;
             }
         }
     }
     ge-0/0/1 {
        unit 0 {
             family inet {
                 address 10.0.0.254/8;
             }
         }
     }
     fxp0 {
        unit 0 {
             family inet {
                 address 10.157.80.85/19;
             }
         }
```

```
    }
}
```

18. Commit the configuration to activate it on the services gateway.

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

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

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

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

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

NOTE: To access the device using J-Web for the first time, enter configuration mode in the CLI, and set the management option using the command **set system services web-management http**.

Launch a Web browser from the management device and access the services gateway using the URL http://<device management IP address>. The J-Web login page is displayed. This indicates that you have successfully completed the initial configuration, and your SRX1500 Firewall is ready for use.

CHAPTER 5

Maintaining Components

Maintaining the SRX1500 Components

IN THIS SECTION

Required Tools and Parts for Maintaining the SRX1500 Services Gateway

The following tools and parts are required to maintain the hardware components of the services gateway:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade screw-blade screwdriver, approximately 1/8 in. (3 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Routine Maintenance Procedures for the SRX1500 Services Gateway

For optimum performance of the services gateway, perform the following preventive maintenance procedures regularly:

- Inspect the installation site for moisture, loose wires or cables, and excessive dust.
- Make sure that airflow is unobstructed around the services gateway and into the air intake vents.
- Check the status LEDs on the front panel of the services gateway.

Maintaining the SRX1500 Power System

IN THIS SECTION

Maintaining the SRX1500 Firewall Power Supply

To maintain the power supplies of the services gateway:

- Make sure that all power and grounding cables are arranged so that they do not obstruct access to other services gateway components.
- Routinely check the PWR LED on the front panel. If this LED is solid green, the power supplies are functioning normally.
- Periodically inspect the site to ensure that the grounding and power cables connected to the services gateway are securely in place and that there is no moisture accumulating near the services gateway.

Required Tools and Parts for Replacing the SRX1500 Firewall Components

The following tools and parts are required to replace hardware components.

- 3/8 in. nut driver or pliers
- Blank panels (if component is not reinstalled)
- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade (–) screwdriver

- Phillips (+) screwdrivers, numbers 1 and 2
- Wire cutters

Replacing an AC Power Supply on the SRX1500 Firewall

IN THIS SECTION

Disconnecting an AC Power Cord from the SRX1500 Firewall

WARNING: Before working on an AC-powered device or near power supplies, unplug the power cord.

To disconnect the AC power cord:

1. Unplug the power cord from the power source receptacle.
2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
3. Unplug the power cord from the appliance inlet on the power supply.

Removing an AC Power Supply from the SRX1500 Firewall

Up to two power supplies can be located at the rear of the chassis on the right side. Each AC power supply weighs 2.20 lb (1 kg).

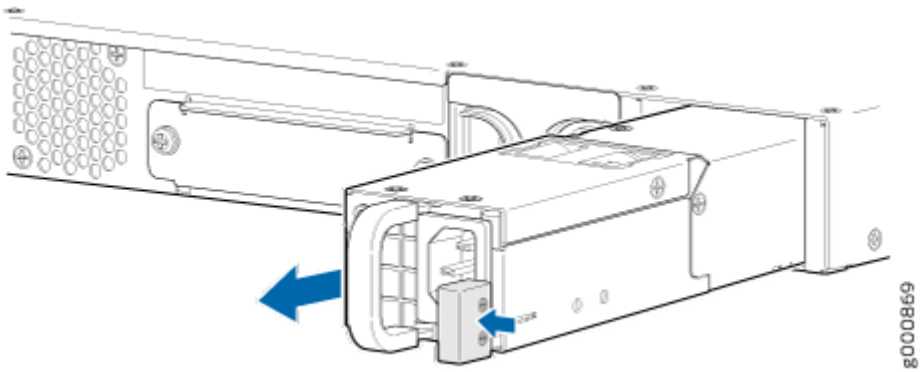
CAUTION: Do not leave a power supply slot empty for more than 30 minutes while the services gateway is operational. For proper airflow, the power supply must remain in the chassis, or a blank panel must be used in the empty slot.

NOTE: After powering off a power supply, wait at least 60 seconds before turning it back on.

To remove an AC power supply:

1. Switch off the dedicated facility circuit breaker for the power supply, and remove the power cord from the AC power source. Follow the electrostatic discharge (ESD) and disconnection instructions for your site.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
3. Remove the power cord from the power supply.
4. Press the latch to the left of the power outlet (see Figure 14 on page 73).
5. Pull the power supply straight out of the chassis.

Figure 14: Removing an AC Power Supply from the SRX1500 Firewall

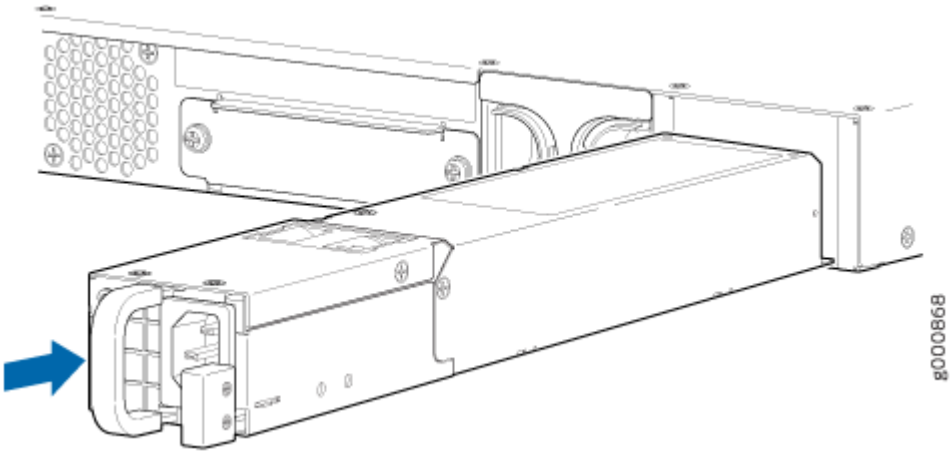


Installing an AC Power Supply on the SRX1500 Services Gateway

To install an AC power supply:

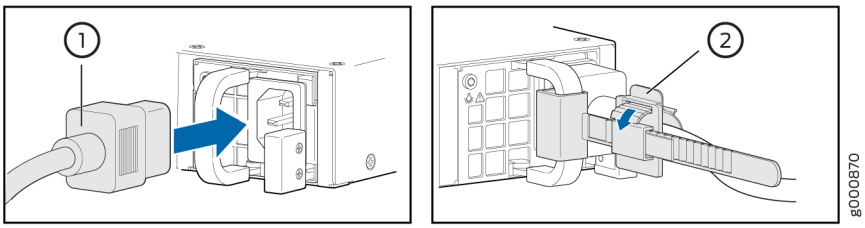
1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
2. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate should be flush with any adjacent power supply faceplate (see Figure 2).

Figure 15: Installing an AC Power Supply on the SRX1500 Services Gateway



3. Attach the power cord to the power supply. Use a power cord retainer to hold the power cord in place.

Figure 16: Connecting the AC Power Cord on the SRX1500 Services Gateway



4. Attach the power cord to the AC power source, and switch on the dedicated facility circuit breaker for the power supply. Follow the ESD and connection instructions for your site. If the power supply is correctly installed and functioning normally, the PWR LED glows steadily.

NOTE: If more than one power supply is being installed, ensure the following:

- Connect power cords to both the power supplies.
- Connect each power supply to a DC power feed.

If both power supplies are plugged in and receiving power, the RPS LED glows solid green.

RELATED DOCUMENTATION

SRX1500 Firewall Power Supply | 19

SRX1500 Firewall AC Power Supply Electrical Specifications | 22

Replacing a DC Power Supply on the SRX1500 Firewall

IN THIS SECTION

Removing a DC Power Supply Cable from the SRX1500 Firewall

To remove a power supply cable connected to a DC power supply:

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to an approved site ESD grounding point. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
2. Switch off the external circuit breakers for all the cables attached to the power supply. Make sure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cables might become active during the removal process.
3. Remove the power cable from the DC power source.
4. Attach an ESD grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
5. Make sure the cable is not touching or in the way of any services gateway components and that it does not drape where people could trip on it.
6. Remove the clear plastic cover protecting the terminal studs on the faceplate.
7. Attach the power cable to the DC power source.
8. Verify that the DC source power cabling is correct. If the power cable is correctly installed and the power supply is functioning normally, the POWER LED on the front panel glows solid green.

Removing a DC Power Supply on the SRX1500 Firewall

Up to two power supplies can be located at the rear of the chassis on the right side. Each DC power supply weighs approximately 2.20 lbs (1 kg).

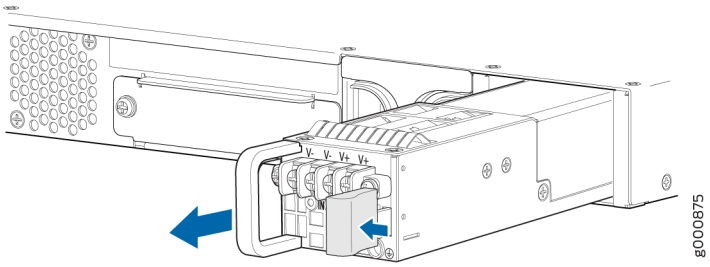
CAUTION: Do not leave a power supply slot empty for more than 30 minutes while the services gateway is operational. For proper airflow, the power supply must remain in the chassis, or a blank panel must be used in the empty slot.

NOTE: After powering off a power supply, wait at least 60 seconds before turning it back on.

To remove a DC power supply:

1. Switch off the dedicated facility circuit breaker for the power supply. Follow the electrostatic discharge (ESD) and disconnection instructions for your site.
2. Make sure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cables might become active during the removal process.
3. Attach an ESD grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
4. Remove the clear plastic cover protecting the terminal studs on the faceplate.
5. Remove the screws and washers from the terminals. Use a number 2 Phillips screwdriver to loosen and remove the screws.
6. Remove the cable lugs from the terminal studs.
7. Carefully move the power cables out of the way.
8. Push the Tab latch on the right edge of the power supply to the left.
9. Pull the power supply straight out of the chassis.

Figure 17: Removing a DC Power Supply from the SRX1500 Firewall



Installing a DC Power Supply on the SRX1500 Services Gateway

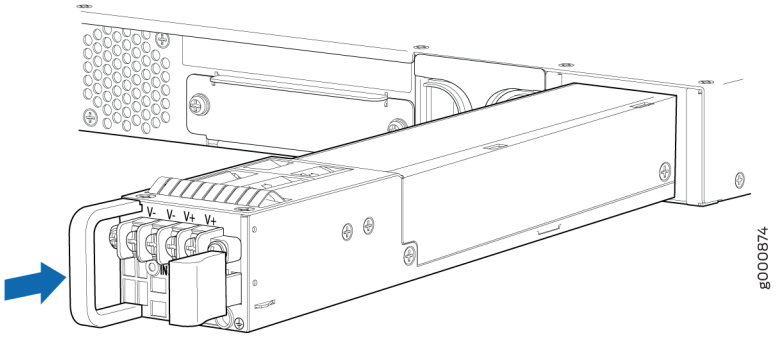
To install a DC power supply:

1. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation. To ensure that all power is off, locate

the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position (**O**), and tape the switch handle of the circuit breaker in the OFF position.

2. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to one of the ESD points on the chassis. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
3. Orient the power supply so that the locking lever is on the left as shown in Figure 5.

Figure 18: Installing a DC Power Supply on an SRX1500 Services Gateway



4. Using both hands, slide the power supply straight into the chassis until the power supply is fully seated in the chassis slot. The power supply faceplate should be flush with any adjacent power supply faceplate.
5. Tighten the captive screws on the lower edge of the power supply faceplate.
6. Remove the clear plastic cover protecting the terminal studs on the faceplate.
7. Verify that the DC power cables are correctly labeled before making connections to the power supply. In a typical power distribution scheme where the return is connected to chassis ground at the battery plant, you can use a multimeter to verify the ohm output of the –48V and RTN DC cables to chassis ground. The cable with very large resistance (indicating an open circuit) to chassis ground will be –48V and the cable with very low resistance (indicating a closed circuit) to chassis ground will be RTN.

> ⚠ **CAUTION**: You must ensure that power connections maintain the proper polarity. The power source cables might be labeled **(+)** and **(–)** to indicate their polarity. There is no standard color coding for DC power cables. The color coding used by the external DC power source at your site determines the color coding for the leads on the power cables that attach to the terminal studs on each power supply.

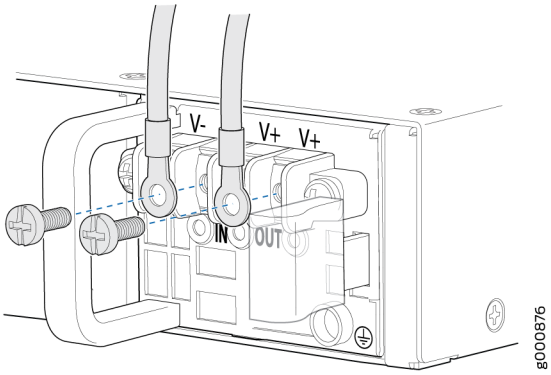
8. Using a number 2 Phillips screwdriver, remove the screws and square washers from the terminal studs.

9. Secure each power cable lug to the terminal studs, first with the square washer, then with the screw. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each screw.

   a. Attach the positive (+) DC source power cable lug to the RTN (return) terminal.

   b. Attach the negative (–) DC source power cable lug to the –48V (input) terminal.

Figure 19: Securing the Power Cables



10. Replace the clear plastic cover over the terminal studs on the faceplate.
11. Verify that the power cables are connected correctly, that they are not touching or blocking access to services gateway components, and that they do not drape where people could trip on them.
12. Remove the tape from the switch handle of the circuit breaker on the panel board that services the DC circuit and switch the circuit breaker to the ON position (|). Observe the status LEDs on the power supply faceplate. If the power supply is correctly installed and functioning normally, the POWER LED glows solid green on the services gateway front panel.

NOTE: If more than one power supply is being installed, turn on all power supplies at the same time.

If both power supplies are plugged in and receiving AC power, the RPS LED glows solid green.

RELATED DOCUMENTATION

SRX1500 Firewall Power Supply | 19

SRX1500 Firewall DC Power Supply Electrical Specifications | 23

SRX1500 Firewall DC Power Cable Specifications | 23

CHAPTER 6

Troubleshooting Hardware

Troubleshooting the SRX1500

IN THIS SECTION

Troubleshooting Resources for the SRX1500 Firewall Overview

To troubleshoot a services gateway, you use the Junos OS command-line interface (CLI) and LEDs on the components:

- LEDs—When the services gateway detects an alarm condition, the alarm LED on the interfaces glows red or yellow.
- CLI—The CLI is the primary tool for controlling and troubleshooting hardware, Junos OS, and network connectivity. Use the CLI to display more information about alarms. CLI commands display information about network connectivity derived from the ping and traceroute utilities. For information about using the CLI to troubleshoot Junos OS, see the appropriate Junos OS configuration guide.
- JTAC—If you need assistance during troubleshooting, you can contact the Juniper Networks Technical Assistance Center (JTAC) by using the Web or by telephone. If you encounter software problems, or problems with hardware components not discussed here, contact JTAC.

Troubleshooting Chassis and Interface Alarm Messages on the SRX1500 Services Gateway

When the services gateway detects an alarm condition, the alarm LED on the interfaces glows red or yellow on the front panel as appropriate. To view a more detailed description of the alarm cause, issue the `show chassis alarms` command.

There are two classes of alarm messages:

- Chassis alarms—Indicate a problem with a chassis component such as the cooling system or power supply.
- Interface alarms—Indicate a problem with a specific network interface.

For more information about the `show chassis alarms` command, see Network Management and Monitoring Guide.

Table 27 on page 81 describes alarms that can occur for a services gateway chassis component.

Table 27: Alarms for Services Gateway Chassis Components

Component	Alarm Conditions	Action	Alarm Severity
Boot media	The services gateway boots from an alternate boot device.	If the internal flash fails at startup, the services gateway automatically boots itself from the alternative boot device (USB storage device). If you configured the services gateway to boot from an alternative boot device, ignore this alarm condition. If you did not configure the services gateway to boot from an alternative boot device, contact JTAC.	Yellow (minor)
Hardware components on services gateway	The services gateway chassis temperature is too warm.	• Check the room temperature. See "SRX1500 Services Gateway Environmental Specifications" on page 29. • Check the air flow. See "Cabinet Requirements" on page 35.	Yellow (minor)

Table 27: Alarms for Services Gateway Chassis Components *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	The services gateway fan has failed.	Place your hand near the exhaust vents at the rear of the chassis to determine whether the fan is pushing air out of the chassis.	Red (major)

NOTE: For more information about alarms, see the appropriate Junos OS Monitoring and Troubleshooting for Security Devices Guide.

Troubleshooting the Power System on the SRX1500 Services Gateway

The LEDs on the services gateway enable you to determine the performance and operation of the power system. The PWR LED located on the front panel of the services gateway, as described in Table 28 on page 82, indicates the different status settings with respect to the power system.

Table 28: PWR LED Description

LED Status	LED State	Meaning	Possible Cause and Corrective Action
Green	On	The services gateway is receiving power, and all AC and/or DC power supply units (PSUs) are working properly.	Normal indication. No action is required.

Table 28: PWR LED Description *(Continued)*

LED Status	LED State	Meaning	Possible Cause and Corrective Action
Red	On	Indicates failure of one or more PSUs.	If you cannot determine the cause of the problem or need additional 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 (outside the United States).
Blinking green	On	The services gateway is receiving power - the services gateway is in the bootup phase before OS initialization.	Normal indication. No action is required.

Table 28: PWR LED Description *(Continued)*

LED Status	LED State	Meaning	Possible Cause and Corrective Action
Off	Off	Indicates that the services gateway is not receiving power.	If a red alarm condition occurs, issue the `show chassis alarms` command to determine the source of the problem. • Verify that the AC power cord and/or DC power supply cable is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable. • Verify that the source circuit breaker has the proper current rating. Each power supply must be connected to a separate source circuit breaker. • Ensure that the power socket you are plugged into is in working condition. • Connect the power supply to a different power source with a new power cord or power cables. If the power supply status LEDs indicate that the power supply is not functioning normally, the power supply is the source of the problem. Replace the power supply with a spare. **NOTE**: If the system temperature exceeds the threshold, Junos OS shuts down all power supplies so that no status is displayed. Junos OS also can shut down one of the power supplies for other reasons. In this case, the remaining power supply provides power to the services gateway, and you can still view the system status through the CLI.

Using the RESET CONFIG Button on the SRX1500 Services Gateway

If a configuration fails or denies management access to the services gateway, you can use the RESET CONFIG button to restore the services gateway to the factory-default configuration. The button is recessed to prevent it from being pressed accidentally.

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

CAUTION: Pressing and holding the RESET CONFIG button for 5 seconds or more deletes all configurations (backup configurations and rescue configuration) on the device, and loads and commits the factory configuration.

You can reset the configuration to the rescue configuration by pressing and holding the **Reset** button for a time interval ranging from 5 seconds to 15 seconds. The configuration is not reset If you configured `chassis config-button no-rescue` or if a rescue configuration is not already set.

You can reset the configuration to the factory-default configuration by pressing and holding the **Reset** button for more than 15 seconds. If you configured `chassis config-button no-clear`, then the configuration is not reset.

For details about factory-default settings, see "Viewing SRX1500 Services Gateway Factory-Default Settings" on page 56.

For details about performing initial software configuration, see "Configuring the SRX1500 Services Gateway Using the CLI" on page 63.

CHAPTER 7

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX1500 Chassis or Components

IN THIS SECTION

Contacting Customer Support

Once you have located the serial numbers of the device or component, you can return the device or component 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.

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

- Your existing service request number, if you have one

- Details of the failure or problem
- Type of activity being performed on the firewall when the problem occurred
- Configuration data displayed by one or more `show` commands
- Your name, organization name, telephone number, fax number, and shipping address

The support representative validates your request and issues a Return Materials Authorization (RMA) number for return of the device or component.

Returning a SRX1500 Firewall Component to Juniper Networks

To return an SRX1500 Firewall or component to Juniper Networks for repair or replacement:

1. Determine the part number and serial number of the services gateway or component.
2. Obtain a Return Materials Authorization (RMA) number from JTAC.

   NOTE: Do not return the services gateway 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 SRX1500 Firewall or component for shipping.

For more information about return and repair policies, see the customer support webpage 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://support.juniper.net/support/ or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

Locating the SRX1500 Firewall Chassis Serial Number and Agency Labels

The chassis serial number is located on the side of the chassis.

Listing the SRX1500 Firewall Component Details with the CLI

Before contacting Juniper Networks to request a Return Materials Authorization (RMA), you must find the serial number on the SRX1500 Firewall or component.

To list all of the SRX1500 Firewall components and their serial numbers, enter the following command-line interface (CLI) command:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                P1B_00000058      SRX1500
Midplane         REV 02   750-058562   ACMH1592          SRX1500
Pseudo CB 0
Routing Engine 0          BUILTIN      BUILTIN           SRX Routing Engine
FPC 0            REV 05   711-053832   ACMG3290          FEB
  PIC 0                   BUILTIN      BUILTIN           12x1G-T-4x1G-SFP-4x10G
    Xcvr 16      REV 01   740-031980   183363A02054      SFP+-10G-SR
    Xcvr 17      REV 01   740-031980   183363A02210      SFP+-10G-SR
    Xcvr 18      REV 01   740-031980   183363A02260      SFP+-10G-SR
    Xcvr 19      REV 01   740-031980   183363A02605      SFP+-10G-SR
Power Supply 0   REV 01   740-055217   1EDP42500JZ       PS 400W 90-264V AC in
Fan Tray 0                                              SRX1500 0, Front to Back


                              Airflow - AFO
Fan Tray 1                                              SRX1500 1, Front to Back


                              Airflow - AFO
Fan Tray 2                                              SRX1500 2, Front to Back


                         Airflow - AFO
Fan Tray 3                                              SRX1500 3, Front to Back


                         Airflow - AFO
```

NOTE: Most components also have a serial number ID label attached to the component body.

Required Tools and Parts for Packing the SRX1500 Firewall

To remove the components from the SRX1500 Firewall or to remove the services gateway from a rack, you need the following tools and parts:

- Blank panels to cover empty slots
- Electrostatic bag or antistatic mat for each component
- Electrostatic discharge (ESD) grounding wrist strap
- Flat-blade screwdriver, approximately 1/4 in. (6 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Packing the SRX1500 Firewall for Shipment

To pack the SRX1500 Firewall for shipment:

1. Retrieve the shipping carton and packing materials in which the services gateway 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. For more information about ESD, see *Prevention of Electrostatic Discharge Damage*.
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 halt
   ```

   Wait until a message appears on the console confirming that the operating system has halted.
4. Shut down power to the services gateway by pressing the Power button on the front of the services gateway.
5. Disconnect power from the services gateway.
6. Remove the cables that connect to all external devices.

7. If the services gateway is installed in a rack, have one person support the weight of the services gateway while another person unscrews and removes the mounting screws.
8. Place the services gateway in the shipping carton.
9. Cover the services gateway with an ESD bag, and place the packing foam on top of and around the device.
10. Replace the accessory box on top of the packing foam.
11. Securely tape the box closed.
12. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

Packing SRX1500 Firewall 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.
- Place the individual component in an electrostatic bag.
- 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.

CHAPTER 8

Safety and Compliance Information

Definitions of Safety Warning Levels

The documentation uses the following levels of safety warnings (there are two *Warning* formats):

NOTE: You might find this information helpful in a particular situation, or you might overlook this important information if it was not highlighted in a Note.

CAUTION: You need to observe the specified guidelines to prevent minor injury or discomfort to you or severe damage to the device.

Attention Veillez à respecter les consignes indiquées pour éviter toute incommodité ou blessure légère, voire des dégâts graves pour l'appareil.

LASER WARNING: This symbol alerts you to the risk of personal injury from a laser.

Avertissement Ce symbole signale un risque de blessure provoquée par rayon laser.

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 familiarize yourself 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.

Avertissement 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.

General Safety Guidelines and Warnings

The following guidelines help ensure your safety and protect the device from damage. The list of guidelines might not address all potentially hazardous situations in your working environment, so be alert and exercise good judgment at all times.

- Perform only the procedures explicitly described in the hardware documentation for this device. Make sure that only authorized service personnel perform other system services.
- Keep the area around the device clear and free from dust before, during, and after installation.
- Keep tools away from areas where people could trip over them while walking.

- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the device.
- 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 attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the device only when it is properly grounded.
- Follow the instructions in this guide to properly ground the device to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions are provided in the hardware documentation for this device. 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 chassis or onto any device component. Such an action could cause electrical shock or damage the device.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.
- Some parts of the chassis, including AC and DC power supply surfaces, power supply unit handles, SFB card handles, and fan tray handles might become hot. The following label provides the warning for hot surfaces on the chassis:

- Always ensure that all modules, power supplies, and cover panels are fully inserted and that the installation screws are fully tightened.

Restricted Access Warning

WARNING: This unit 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.

Avertissement 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.

Qualified Personnel Warning

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

Avertissement 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.

Prevention of Electrostatic Discharge Damage

Device components that are shipped in antistatic bags 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 when you are handling components that are subject to ESD damage, and make sure that it is in direct contact with your skin.

  If a grounding strap is not available, hold the component in its antistatic bag (see Figure 20 on page 99) in one hand and touch the exposed, bare metal of the device with the other hand immediately before inserting the component into the device.

  WARNING: For safety, periodically check the resistance value of the ESD grounding strap. The measurement must be in the range 1 through 10 Mohms.
  Avertissement Par mesure de sécurité, vérifiez régulièrement la résistance du bracelet antistatique. Cette valeur doit être comprise entre 1 et 10 mégohms (Mohms).

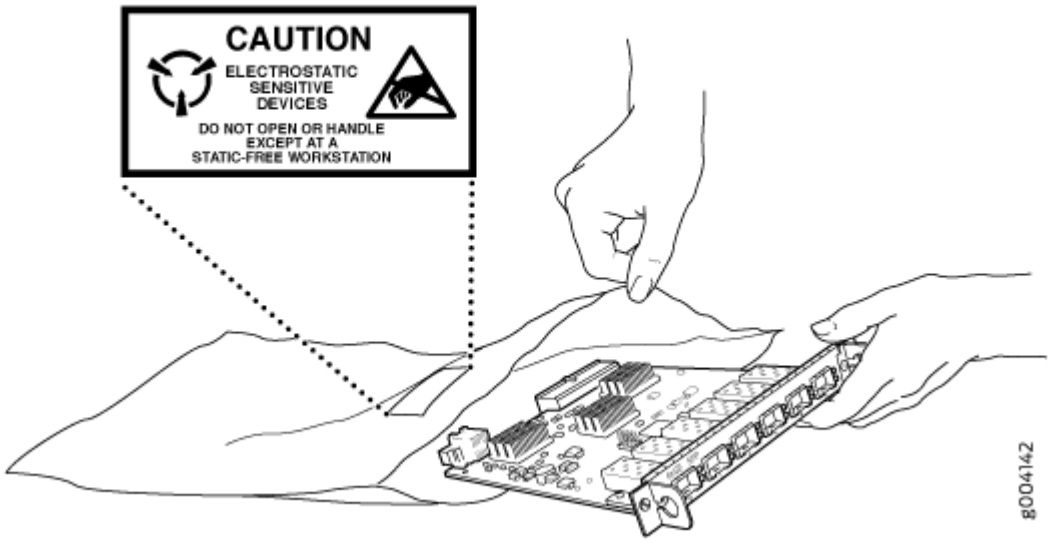
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

  If no grounding strap is available, touch the exposed, bare metal of the device to ground yourself before handling the component.

- Avoid contact between the component that is subject to ESD damage and your clothing. ESD voltages emitted from clothing can damage components.

- When removing or installing a component that is subject to ESD damage, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an antistatic bag (see Figure 20 on page 99). If you are returning a component, place it in an antistatic bag before packing it.

Figure 20: Placing a Component into an Antistatic Bag



CAUTION: ANSI/TIA/EIA-568 cables such as Category 5e and Category 6 can get electrostatically charged. To dissipate this charge, always ground the cables to a suitable and safe earth ground before connecting them to the system.

Attention Les câbles ANSI/TIA/EIA-568, par exemple Cat 5e et Cat 6, peuvent emmagasiner des charges électrostatiques. Pour évacuer ces charges, reliez toujours les câbles à une prise de terre adaptée avant de les raccorder au système.

Fire Safety Requirements

IN THIS SECTION

In the event of a fire emergency, the safety of people is the primary concern. You should 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, you should 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 you install and operate your equipment.

Fire Suppression

In the event of an electrical hazard or an electrical fire, you should first turn power off to the equipment at the source. Then use a Type C fire extinguisher, which uses noncorrosive fire retardants, to extinguish the fire.

Fire Suppression Equipment

Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide and Halotron™, are most effective for suppressing electrical fires. Type C fire extinguishers displace 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, you should use this type of inert oxygen displacement extinguisher instead of an extinguisher that leaves residues on equipment.

Do not use multipurpose Type ABC chemical fire extinguishers (dry chemical fire extinguishers). The primary ingredient in these fire extinguishers is monoammonium phosphate, which is very sticky and difficult to clean. In addition, in the presence of 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 device. 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.

Laser and LED Safety Guidelines and Warnings

IN THIS SECTION

Juniper Networks devices are equipped with laser transmitters, which are considered a Class 1 Laser Product by the U.S. Food and Drug Administration and are evaluated as a Class 1 Laser Product per IEC/EN 60825-1 requirements.

Observe the following guidelines and warnings:

General Laser Safety Guidelines

When working around ports that support optical transceivers, 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.

LASER 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.

Avertissement Les connecteurs à fibre optique sans terminaison peuvent émettre un rayonnement laser invisible. Le cristallin de l'œil humain faisant converger toute la puissance du laser sur la rétine, toute focalisation directe de l'œil sur une source laser, —même de faible puissance—, peut entraîner des lésions oculaires irréversibles.

Class 1 Laser Product Warning

LASER WARNING: Class 1 laser product.
Waarschuwing Klasse-1 laser produkt.

Varoitus Luokan 1 lasertuote.

Avertissement 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

LASER WARNING: Class 1 LED product.
Waarschuwing Klasse 1 LED-product.

Varoitus Luokan 1 valodiodituote.

Avertissement 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

LASER 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.

Avertissement 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

LASER WARNING: Because invisible radiation might 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.

Avertissement 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 an 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.

Maintenance and Operational Safety Guidelines and Warnings

IN THIS SECTION

While performing the maintenance activities for devices, observe the following guidelines and warnings:

Battery Handling Warning

WARNING: Replacing a battery incorrectly might result in an explosion. Replace a 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.

Avertissement 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.

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.

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.

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 baterían 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 can be welded 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.

Avertissement 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.

Avertissement 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 device from overheating, do not operate it in an area that exceeds the maximum recommended ambient temperature. To prevent airflow restriction, allow at least 6 in. (15.2 cm) of clearance around the ventilation openings.

Waarschuwing Om te voorkomen dat welke switch van de Juniper Networks router 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 switch-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.

Avertissement Pour éviter toute surchauffe des routeurs de la gamme Juniper Networks switch, 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 Router der switch 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 switch, 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 switch 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 switch, 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 switch se recaliente, no lo haga funcionar en un área en la que se supere la temperatura ambiente máxima recomendada de 40° 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 switch överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40° 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 device 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.

Avertissement 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.

Action to Take After an 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 device.
3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.

General Electrical Safety Guidelines and Warnings

IN THIS SECTION

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.

Grounded Equipment Warning

WARNING: The services gateway is intended to be grounded. Ensure that the services gateway is connected to earth ground during normal use.

Waarschuwing Deze apparatuur hoort geaard te worden Zorg dat de host-computer tijdens normaal gebruik met aarde is verbonden.

Varoitus Tämä laitteisto on tarkoitettu maadoitettavaksi. Varmista, että isäntälaite on yhdistetty maahan normaalikäytön aikana.

Attention Cet équipement doit être relié à la terre. S'assurer que l'appareil hôte est relié à la terre lors de l'utilisation normale.

Warnung Dieses Gerät muß geerdet werden. Stellen Sie sicher, daß das Host-Gerät während des normalen Betriebs an Erde gelegt ist.

Avvertenza Questa apparecchiatura deve essere collegata a massa. Accertarsi che il dispositivo host sia collegato alla massa di terra durante il normale utilizzo.

Advarsel Dette utstyret skal jordes. Forviss deg om vertsterminalen er jordet ved normalt bruk.

Aviso Este equipamento deverá estar ligado à terra. Certifique-se que o host se encontra ligado à terra durante a sua utilização normal.

¡Atención! Este equipo debe conectarse a tierra. Asegurarse de que el equipo principal esté conectado a tierra durante el uso normal.

Varning! Denna utrustning är avsedd att jordas. Se till att värdenheten är jordad vid normal användning.

Backplane Energy Hazard Warning

WARNING: High levels of electrical energy are distributed across the services gateway backplane. Be careful not to contact the backplane connectors, or any component connected to the backplane, with any metallic object while servicing components installed in the services gateway.

Multiple Power Supplies Disconnection Warning

WARNING: The services gateway has more than one power supply connection. All connections must be removed completely to remove power from the unit completely.

Waarschuwing Deze eenheid heeft meer dan één stroomtoevoerverbinding; alle verbindingen moeten volledig worden verwijderd om de stroom van deze eenheid volledig te verwijderen.

Varoitus Tässä laitteessa on useampia virtalähdekytkentöjä. Kaikki kytkennät on irrotettava kokonaan, jotta virta poistettaisiin täysin laitteesta.

Attention Cette unité est équipée de plusieurs raccordements d'alimentation. Pour supprimer tout courant électrique de l'unité, tous les cordons d'alimentation doivent être débranchés.

Warnung Diese Einheit verfügt über mehr als einen Stromanschluß; um Strom gänzlich von der Einheit fernzuhalten, müssen alle Stromzufuhren abgetrennt sein.

Avvertenza Questa unità ha più di una connessione per alimentatore elettrico; tutte le connessioni devono essere completamente rimosse per togliere l'elettricità dall'unità.

Advarsel Denne enheten har mer enn én strømtilkobling. Alle tilkoblinger må kobles helt fra for å eliminere strøm fra enheten.

Aviso Este dispositivo possui mais do que uma conexão de fonte de alimentação de energia; para poder remover a fonte de alimentação de energia, deverão ser desconectadas todas as conexões existentes.

¡Atención! Esta unidad tiene más de una conexión de suministros de alimentación; para eliminar la alimentación por completo, deben desconectarse completamente todas las conexiones.

Varning! Denna enhet har mer än en strömförsörjningsanslutning; alla anslutningar måste vara helt avlägsnade innan strömtillförseln till enheten är fullständigt bruten.

Power Disconnection Warning

WARNING: Before working on the services gateway or near power supplies, unplug the power cord from an AC-powered services gateway; switch off the power at the circuit breaker on a DC-powered services gateway.

Waarschuwing Voordat u aan een frame of in de nabijheid van voedingen werkt, dient u bij wisselstroom toestellen de stekker van het netsnoer uit het stopcontact te halen; voor gelijkstroom toestellen dient u de stroom uit te schakelen bij de stroomverbreker.

Varoitus Kytke irti vaihtovirtalaitteiden virtajohto ja katkaise tasavirtalaitteiden virta suojakytkimellä, ennen kuin teet mitään asennuspohjalle tai työskentelet virtalähteiden läheisyydessä.

Attention Avant de travailler sur un châssis ou à proximité d'une alimentation électrique, débrancher le cordon d'alimentation des unités en courant alternatif; couper l'alimentation des unités en courant continu au niveau du disjoncteur.

Warnung Bevor Sie an einem Chassis oder in der Nähe von Netzgeräten arbeiten, ziehen Sie bei Wechselstromeinheiten das Netzkabel ab bzw. schalten Sie bei Gleichstromeinheiten den Strom am Unterbrecher ab.

Avvertenza Prima di lavorare su un telaio o intorno ad alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all'interruttore automatico sulle unità CC.

Advarsel Før det utføres arbeid på kabinettet eller det arbeides i nærheten av strømforsyningsenheter, skal strømledningen trekkes ut p vekselstrømsenheter og strømmen kobles fra ved strømbryteren på likestrømsenheter.

Aviso Antes de trabalhar num chassis, ou antes de trabalhar perto de unidades de fornecimento de energia, desligue o cabo de alimentação nas unidades de corrente alternada; desligue a corrente no disjuntor nas unidades de corrente contínua.

¡Atención! Antes de manipular el chasis de un equipo o trabajar cerca de una fuente de alimentación, desenchufar el cable de alimentación en los equipos de corriente alterna (CA); cortar la alimentación desde el interruptor automático en los equipos de corriente continua (CC).

Varning! Innan du arbetar med ett chassi eller nära strömförsörjningsenheter skall du för växelströmsenheter dra ur nätsladden och för likströmsenheter bryta strömmen vid överspänningsskyddet.

TN Power Warning

WARNING: The services gateway is designed to work with TN power systems.

Waarschuwing Het apparaat is ontworpen om te functioneren met TN energiesystemen.

Varoitus Koje on suunniteltu toimimaan TN-sähkövoimajärjestelmien yhteydessä.

Attention Ce dispositif a été conçu pour fonctionner avec des systèmes d'alimentation TN.

Warnung Das Gerät ist für die Verwendung mit TN-Stromsystemen ausgelegt.

Avvertenza Il dispositivo è stato progettato per l'uso con sistemi di alimentazione TN.

Advarsel Utstyret er utfomet til bruk med TN-strømsystemer.

Aviso O dispositivo foi criado para operar com sistemas de corrente TN.

¡Atención! El equipo está diseñado para trabajar con sistemas de alimentación tipo TN.

Varning! Enheten är konstruerad för användning tillsammans med elkraftssystem av TN-typ.

Copper Conductors Warning

WARNING: Use copper conductors only.
Waarschuwing Gebruik alleen koperen geleiders.

Varoitus Käytä vain kuparijohtimia.

Attention Utilisez uniquement des conducteurs en cuivre.

Warnung Verwenden Sie ausschließlich Kupferleiter.

Avvertenza Usate unicamente dei conduttori di rame.

Advarsel Bruk bare kobberledninger.

Aviso Utilize apenas fios condutores de cobre.

¡Atención! Emplee sólo conductores de cobre.

Varning! Använd endast ledare av koppar.

RELATED DOCUMENTATION

- In Case of Electrical Accident
- AC Power Electrical Safety Guidelines
- *DC Power Electrical Safety Guidelines*

AC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to AC-powered devices:

- Note the following warnings printed on the device:

  "**CAUTION:** THIS UNIT HAS MORE THAN ONE POWER SUPPLY CORD. DISCONNECT ALL POWER SUPPLY CORDS BEFORE SERVICING TO AVOID ELECTRIC SHOCK."

  "**ATTENTION:** CET APPAREIL COMPORTE PLUS D'UN CORDON D'ALIMENTATION. AFIN DE PRÉVENIR LES CHOCS ÉLECTRIQUES, DÉBRANCHER TOUT CORDON D'ALIMENTATION AVANT DE FAIRE LE DÉPANNAGE."

- AC-powered devices are shipped with a three-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding must comply with local and national electrical codes.

- You must provide an external certified circuit breaker (2-pole circuit breaker or 4-pole circuit breaker based on your device) rated minimum 20 A in the building installation.

- The power cord serves as the main disconnecting device for the AC-powered device. The socket outlet must be near the AC-powered device and be easily accessible.

- For devices that have more than one power supply connection, you must ensure that all power connections are fully disconnected so that power to the device is completely removed to prevent electric shock. To disconnect power, unplug all power cords (one for each power supply).

Power Cable Warning (Japanese)

WARNING: The attached power cable is only for this product. Do not use the cable for another product.

注意

附属の電源コードセットはこの製品専用です。
他の電気機器には使用しないでください。

DC Power Electrical Safety Guidelines

IN THIS SECTION

DC Power Electrical Safety Guidelines

The following electrical safety guidelines apply to a DC-powered services gateway:

- A DC-powered services gateway is equipped with a DC terminal block that is rated for the power requirements of a maximally configured services gateway. To supply sufficient power, terminate the DC input wiring on a facility DC source capable of supplying at least 6.2 A @ -48 VDC for the system. We recommend that the 48 VDC facility DC source be equipped with a circuit breaker rated at 6.2 A (-48 VDC) minimum, or as required by local code. Incorporate an easily accessible disconnect device into the facility wiring. In the United States and Canada, the -48 VDC facility should be equipped with a circuit breaker rated a minimum of 125% of the power provisioned for the input in

accordance with the National Electrical Code in the US and the Canadian Electrical Code in Canada. Be sure to connect the ground wire or conduit to a solid office (earth) ground. A closed loop ring is recommended for terminating the ground conductor at the ground stud.

- Run two wires from the circuit breaker box to a source of 48 VDC. Use appropriate gauge wire to handle up to 6.2 A.
- A DC-powered services gateway that is equipped with a DC terminal block is intended only for installation in a restricted access location. In the United States, a restricted access area is one in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code ANSI/NFPA 70.

> **NOTE**: Primary overcurrent protection is provided by the building circuit breaker. This breaker should protect against excess currents, short circuits, and earth faults in accordance with NEC ANSI/NFPA70.

- Ensure that the polarity of the DC input wiring is correct. Under certain conditions, connections with reversed polarity might trip the primary circuit breaker or damage the equipment.
- For personal safety, connect the green and yellow wire to safety (earth) ground at both the services gateway and the supply side of the DC wiring.
- The marked input voltage of -48 VDC for a DC-powered services gateway is the nominal voltage associated with the battery circuit, and any higher voltages are only to be associated with float voltages for the charging function.
- Because the services gateway is a positive ground system, you must connect the positive lead to the terminal labeled **RETURN**, the negative lead to the terminal labeled **-48V**, and the earth ground to the chassis grounding points.

DC Power Disconnection Warning

WARNING: Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the **OFF** position, and tape the switch handle of the circuit breaker in the **OFF** position.

Waarschuwing Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te

verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

Varoitus Varmista, että tasavirtapiirissä ei ole virtaa ennen seuraavien toimenpiteiden suorittamista. Varmistaaksesi, että virta on KATKAISTU täysin, paikanna tasavirrasta huolehtivassa kojetaulussa sijaitseva suojakytkin, käännä suojakytkin KATKAISTU-asentoon ja teippaa suojakytkimen varsi niin, että se pysyy KATKAISTU-asennossa.

Attention Avant de pratiquer l'une quelconque des procédures ci-dessous, vérifier que le circuit en courant continu n'est plus sous tension. Pour en être sûr, localiser le disjoncteur situé sur le panneau de service du circuit en courant continu, placer le disjoncteur en position fermée (OFF) et, à l'aide d'un ruban adhésif, bloquer la poignée du disjoncteur en position OFF.

Warnung Vor Ausführung der folgenden Vorgänge ist sicherzustellen, daß die Gleichstromschaltung keinen Strom erhält. Um sicherzustellen, daß sämtlicher Strom abgestellt ist, machen Sie auf der Schalttafel den Unterbrecher für die Gleichstromschaltung ausfindig, stellen Sie den Unterbrecher auf AUS, und kleben Sie den Schaltergriff des Unterbrechers mit Klebeband in der AUS-Stellung fest.

Avvertenza Prima di svolgere una qualsiasi delle procedure seguenti, verificare che il circuito CC non sia alimentato. Per verificare che tutta l'alimentazione sia scollegata (OFF), individuare l'interruttore automatico sul quadro strumenti che alimenta il circuito CC, mettere l'interruttore in posizione OFF e fissarlo con nastro adesivo in tale posizione.

Advarsel Før noen av disse prosedyrene utføres, kontroller at strømmen er frakoblet likestrømkretsen. Sørg for at all strøm er slått AV. Dette gjøres ved å lokalisere strømbryteren på brytertavlen som betjener likestrømkretsen, slå strømbryteren AV og teipe bryterhåndtaket på strømbryteren i AV-stilling.

Aviso Antes de executar um dos seguintes procedimentos, certifique-se que desligou a fonte de alimentação de energia do circuito de corrente contínua. Para se assegurar que toda a corrente foi DESLIGADA, localize o disjuntor no painel que serve o circuito de corrente contínua e coloque-o na posição OFF (Desligado), segurando nessa posição a manivela do interruptor do disjuntor com fita isoladora.

¡Atención! Antes de proceder con los siguientes pasos, comprobar que la alimentación del circuito de corriente continua (CC) esté cortada (OFF). Para asegurarse de que toda la alimentación esté cortada (OFF), localizar el interruptor automático en el panel que alimenta al circuito de corriente continua, cambiar el interruptor automático a la

posición de Apagado (OFF), y sujetar con cinta la palanca del interruptor automático en posición de Apagado (OFF).

Varning! Innan du utför någon av följande procedurer måste du kontrollera att strömförsörjningen till likströmskretsen är bruten. Kontrollera att all strömförsörjning är BRUTEN genom att slå AV det överspänningsskydd som skyddar likströmskretsen och tejpa fast överspänningsskyddets omkopplare i FRÅN-läget.

DC Power Grounding Requirements and Warning

An insulated grounding conductor that is identical in size to the grounded and ungrounded branch circuit supply conductors, but is identifiable by green and yellow stripes, is installed as part of the branch circuit that supplies the unit. The grounding conductor is a separately derived system at the supply transformer or motor generator set.

WARNING: When installing the services gateway, the ground connection must always be made first and disconnected last.

Waarschuwing Bij de installatie van het toestel moet de aardverbinding altijd het eerste worden gemaakt en het laatste worden losgemaakt.

Varoitus Laitetta asennettaessa on maahan yhdistäminen aina tehtävä ensiksi ja maadoituksen irti kytkeminen viimeiseksi.

Attention Lors de l'installation de l'appareil, la mise à la terre doit toujours être connectée en premier et déconnectée en dernier.

Warnung Der Erdanschluß muß bei der Installation der Einheit immer zuerst hergestellt und zuletzt abgetrennt werden.

Avvertenza In fase di installazione dell'unità, eseguire sempre per primo il collegamento a massa e disconnetterlo per ultimo.

Advarsel Når enheten installeres, må jordledningen alltid tilkobles først og frakobles sist.

Aviso Ao instalar a unidade, a ligação à terra deverá ser sempre a primeira a ser ligada, e a última a ser desligada.

¡Atención! Al instalar el equipo, conectar la tierra la primera y desconectarla la última.

Varning! Vid installation av enheten måste jordledningen alltid anslutas först och kopplas bort sist.

DC Power Wiring Sequence Warning

WARNING: Wire the DC power supply using the appropriate lugs. When connecting power, the proper wiring sequence is ground to ground, +RTN to +RTN, then -48 V to -48 V. When disconnecting power, the proper wiring sequence is -48 V to -48 V, +RTN to +RTN, then ground to ground. Note that the ground wire should always be connected first and disconnected last.

Waarschuwing De juiste bedradingsvolgorde verbonden is aarde naar aarde, +RTN naar +RTN, en -48 V naar – 48 V. De juiste bedradingsvolgorde losgemaakt is en -48 V naar – 48 V, +RTN naar +RTN, aarde naar aarde.

Varoitus Oikea yhdistettava kytkentajarjestys on maajohto maajohtoon, +RTN varten +RTN, -48 V varten – 48 V. Oikea irrotettava kytkentajarjestys on -48 V varten – 48 V, +RTN varten +RTN, maajohto maajohtoon.

Attention Câblez l'approvisionnement d'alimentation CC En utilisant les crochets appropriés à l'extrémité de câblage. En reliant la puissance, l'ordre approprié de câblage est rectifié pour rectifier, +RTN à +RTN, puis -48 V à -48 V. En débranchant la puissance, l'ordre approprié de câblage est -48 V à -48 V, +RTN à +RTN, a alors rectifié pour rectifier. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois. Notez que le fil de masse devrait toujours être relié d'abord et débranché pour la dernière fois.

Warnung Die Stromzufuhr ist nur mit geeigneten Ringösen an das DC Netzteil anzuschliessen. Die richtige Anschlusssequenz ist: Erdanschluss zu Erdanschluss, +RTN zu +RTN und dann -48V zu -48V. Die richtige Sequenz zum Abtrennen der Stromversorgung ist -48V zu -48V, +RTN zu +RTN und dann Erdanschluss zu Erdanschluss. Es ist zu beachten dass der Erdanschluss immer zuerst angeschlossen und als letztes abgetrennt wird.

Avvertenza Mostra la morsettiera dell alimentatore CC. Cablare l'alimentatore CC usando i connettori adatti all'estremità del cablaggio, come illustrato. La corretta sequenza di cablaggio è da massa a massa, da positivo a positivo (da linea ad L) e da negativo a negativo (da neutro a N). Tenere presente che il filo di massa deve sempre venire collegato per primo e scollegato per ultimo.

Advarsel Riktig tilkoples tilkoplingssekvens er jord til jord, +RTN til +RTN, -48 V til – 48 V. Riktig frakoples tilkoplingssekvens er -48 V til – 48 V, +RTN til +RTN, jord til jord.

Aviso Ate con alambre la fuente de potencia cc Usando los terminales apropiados en el extremo del cableado. Al conectar potencia, la secuencia apropiada del cableado se muele para moler, +RTN a +RTN, entonces -48 V a -48 V. Al desconectar potencia, la

secuencia apropiada del cableado es -48 V a -48 V, +RTN a +RTN, entonces molió para moler. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último.

¡Atención! Wire a fonte de alimentação de DC Usando os talões apropriados na extremidade da fiação. Ao conectar a potência, a seqüência apropriada da fiação é moída para moer, +RTN a +RTN, então -48 V a -48 V. Ao desconectar a potência, a seqüência apropriada da fiação é -48 V a -48 V, +RTN a +RTN, moeu então para moer. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último. Anote que o fio à terra deve sempre ser conectado primeiramente e desconectado por último.

Varning! Korrekt kopplingssekvens ar jord till jord, +RTN till +RTN, -48 V till – 48 V. Korrekt kopplas kopplingssekvens ar -48 V till -48 V, +RTN till +RTN, jord till jord.

DC Power Wiring Terminations Warning

WARNING: When stranded wiring is required, use approved wiring terminations, such as closed-loop or spade-type with upturned lugs. These terminations should be the appropriate size for the wires and should clamp both the insulation and conductor.

Waarschuwing Wanneer geslagen bedrading vereist is, dient u bedrading te gebruiken die voorzien is van goedgekeurde aansluitingspunten, zoals het gesloten-lus type of het grijperschop type waarbij de aansluitpunten omhoog wijzen. Deze aansluitpunten dienen de juiste maat voor de draden te hebben en dienen zowel de isolatie als de geleider vast te klemmen.

Varoitus Jos säikeellinen johdin on tarpeen, käytä hyväksyttyä johdinliitäntää, esimerkiksi suljettua silmukkaa tai kourumaista liitäntää, jossa on ylöspäin käännetyt kiinnityskorvat. Tällaisten liitäntöjen tulee olla kooltaan johtimiin sopivia ja niiden tulee puristaa yhteen sekä eristeen että johdinosan.

Attention Quand des fils torsadés sont nécessaires, utiliser des douilles terminales homologuées telles que celles à circuit fermé ou du type à plage ouverte avec cosses rebroussées. Ces douilles terminales doivent être de la taille qui convient aux fils et doivent être refermées sur la gaine isolante et sur le conducteur.

Warnung Wenn Litzenverdrahtung erforderlich ist, sind zugelassene Verdrahtungsanschlüsse, z.B. Ringoesen oder gabelförmige Kabelschuhe mit nach oben

gerichteten Enden zu verwenden. Diese Abschlüsse sollten die angemessene Größe für die Drähte haben und sowohl die Isolierung als auch den Leiter festklemmen.

Avvertenza Quando occorre usare trecce, usare connettori omologati, come quelli a occhiello o a forcella con linguette rivolte verso l'alto. I connettori devono avere la misura adatta per il cablaggio e devono serrare sia l'isolante che il conduttore.

Advarsel Hvis det er nødvendig med flertrådede ledninger, brukes godkjente ledningsavslutninger, som for eksempel lukket sløyfe eller spadetype med oppoverbøyde kabelsko. Disse avslutningene skal ha riktig størrelse i forhold til ledningene, og skal klemme sammen både isolasjonen og lederen.

Aviso Quando forem requeridas montagens de instalação eléctrica de cabo torcido, use terminações de cabo aprovadas, tais como, terminações de cabo em circuito fechado e planas com terminais de orelha voltados para cima. Estas terminações de cabo deverão ser do tamanho apropriado para os respectivos cabos, e deverão prender simultaneamente o isolamento e o fio condutor.

¡Atención! Cuando se necesite hilo trenzado, utilizar terminales para cables homologados, tales como las de tipo "bucle cerrado" o "espada", con las lengüetas de conexión vueltas hacia arriba. Estos terminales deberán ser del tamaño apropiado para los cables que se utilicen, y tendrán que sujetar tanto el aislante como el conductor.

Varning! När flertrådiga ledningar krävs måste godkända ledningskontakter användas, t.ex. kabelsko av sluten eller öppen typ med uppåtvänd tapp. Storleken på dessa kontakter måste vara avpassad till ledningarna och måste kunna hålla både isoleringen och ledaren fastklämda.

RELATED DOCUMENTATION

Action to Take After an Electrical Accident

General Electrical Safety Guidelines and Warnings

AC Power Electrical Safety Guidelines

SRX1500 Firewall Agency Approvals

IN THIS SECTION

The services gateway complies with the following standards:

- Safety
  - CAN/CSA-C22.2 No.60950-1 (2007) Information Technology Equipment
  - UL 60950-1 (2nd Ed.) Information Technology Equipment
  - EN 60950-1:2006/A2:2013 Information Technology Equipment
  - EN 60950-1:2005/A2:2013 Information Technology Equipment
  - EN 60825-1:2007 Safety of Laser Products – Part 1: Equipment classification and requirements
- EMC
  - EN 300 386 V1.3.3 (2005) Telecom Network Equipment - EMC requirements
- EMI
  - FCC Part 15 Class A (2007) USA Radiated Emissions
  - EN 55022 Class A (2006) European Radiated Emissions
  - VCCI Class A (2007) Japanese Radiated Emissions
  - BSMI Class A (Taiwan)
  - ICES-003 Class A
  - AS/NZS CISPR 22 Class A
- Immunity
  - EN-61000-3-2 Power Line Harmonics
  - EN-61000-3-3 Voltage Fluctuations and Flicker

  - EN-61000-4-2 Electrostatic Discharge
  - EN-61000-4-3 Radiated Immunity
  - EN-61000-4-4 (2004) Electrical Fast Transients
  - EN-61000-4-5 (2006) Surge
  - EN-61000-4-6 (2007) Low Frequency Common Immunity
  - EN-61000-4-11 (2004) Voltage Dips and Sags
  - EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics
- Environmental
  - Reduction of Hazardous Substances (ROHS) 2
- Telco
  - Common Language Equipment Identifier (CLEI) code

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

RELATED DOCUMENTATION

SRX1500 Firewall Acoustic Noise Compliance Statements | 125

SRX1500 Firewall EMC Requirements | 126

SRX1500 Services Gateway General Safety Guidelines and Warnings

SRX1500 Firewall Acoustic Noise Compliance Statements

The maximum emitted sound pressure level is 70 dB(A) or less per EN ISO 7779.

German Translation:

Maschinenlärminformations-Verordnung - 3. GPSGV, der höchste Schalldruckpegel beträgt 70 dB(A) oder weniger gemäss EN ISO 7779.

RELATED DOCUMENTATION

SRX1500 Firewall Agency Approvals | 124
SRX1500 Firewall EMC Requirements | 126
SRX1500 Services Gateway General Safety Guidelines and Warnings

SRX1500 Firewall EMC Requirements

IN THIS SECTION

Canada

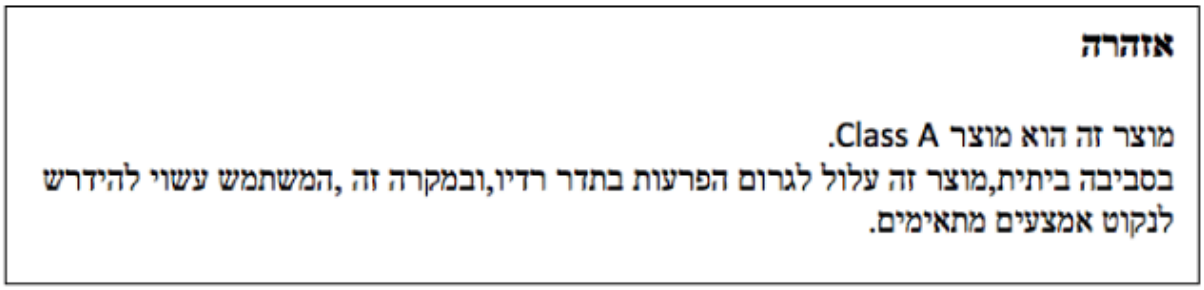
This Class A digital apparatus complies with Canadian ICES-003.

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

European Community

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

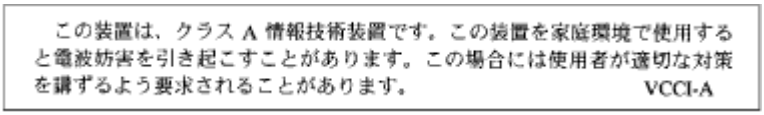
Israel



The preceding translates as follows:

This product is Class A. In residential environments, the product may cause radio interference, and in such a situation, the user may be required to take adequate measures.

Japan



The preceding translates as follows:

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

VCCI-A

United States

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

RELATED DOCUMENTATION

SRX1500 Firewall Agency Approvals | **124**

SRX1500 Firewall Acoustic Noise Compliance Statements | **125**

SRX1500 Services Gateway General Safety Guidelines and Warnings