Juniper Networks | Engineering Simplicity

SRX4700 Firewall Hardware Guide

Published
2026-02-11

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

SRX4700 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 SRX4700 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.

1

CHAPTER

Fast Track: Initial Installation

IN THIS CHAPTER

Fast Track to Rack Installation and Power

SUMMARY

This procedure guides you through the simplest steps to install your Juniper Networks® SRX4700 Firewall in a rack and connect it to power. For more complex installation needs, see "Install the SRX4700 in a Rack" on page 61.

IN THIS SECTION

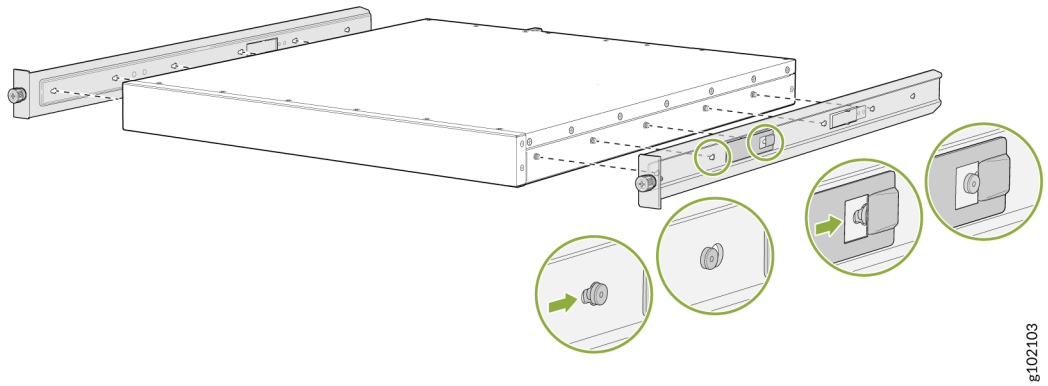
Install the SRX4700 in a Rack

You can install the SRX4700 Firewall in a four-post rack or cabinet. Here, we'll walk you through the steps to install an AC-powered firewall device in a square-hole four-post rack.

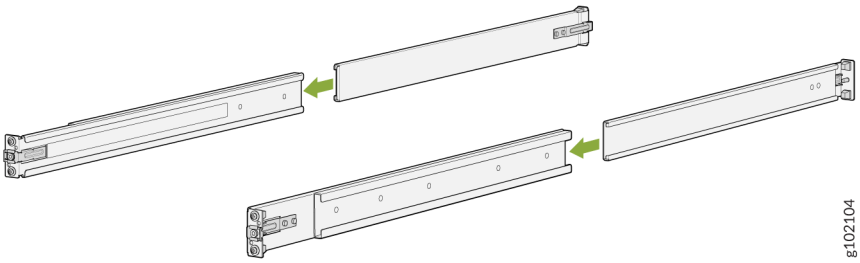
Before you install, review the following:

- "Site Guidelines and Requirements for SRX4700" on page 38.
- General Safety Guidelines and Warnings.
- "Unpack the SRX4700" on page 59.

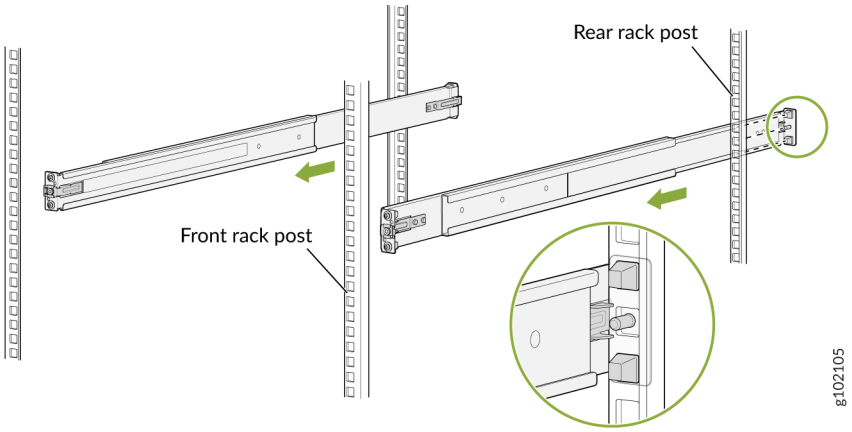
1. Wrap and fasten one end of the electrostatic discharge (ESD) cable grounding strap around your bare wrist, and connect the other end to a site ESD point.
2. Attach the side-mounting brackets to the chassis. Align the keyholes of the mounting brackets over the shoulder screws of the chassis and slide the mounting brackets towards the rear of the chassis.



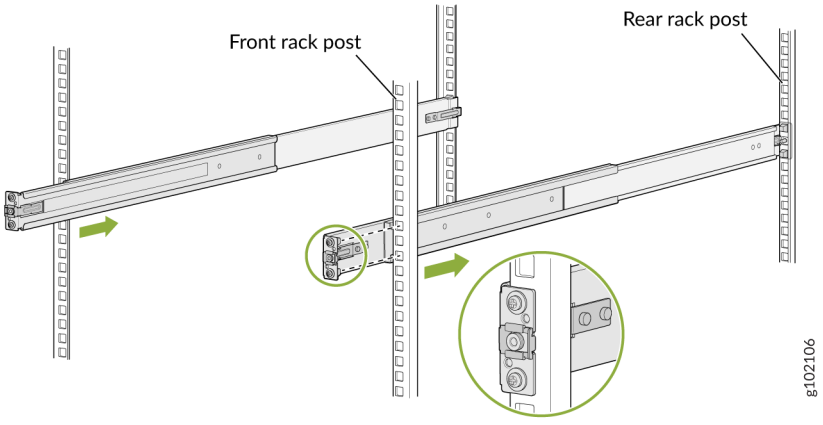
3. Assemble the mounting rails by sliding the rear rails into the front rails.



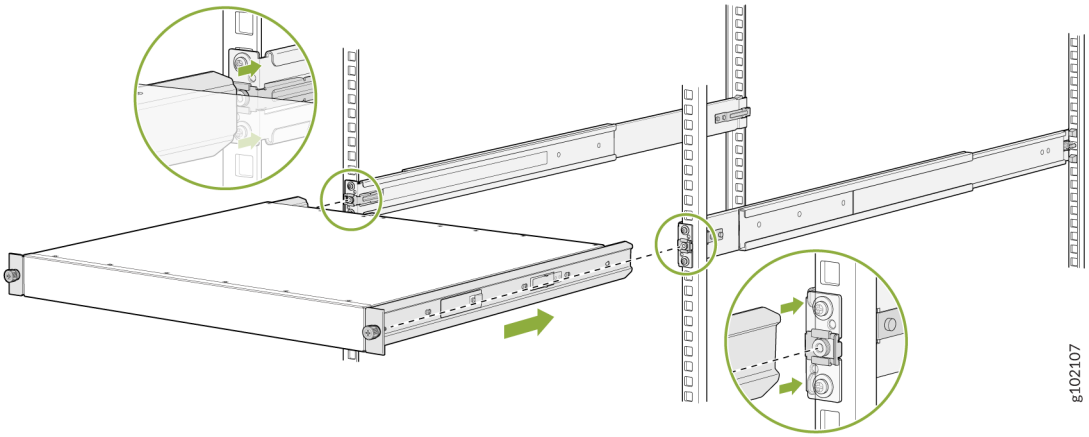
4. Align the guide blocks of the rear-mounting rail with the rear-post holes. Pull the rear-mounting rail toward the front of the rack to lock the rail in place. You'll hear a distinct click when the latch locks into the rack holes.



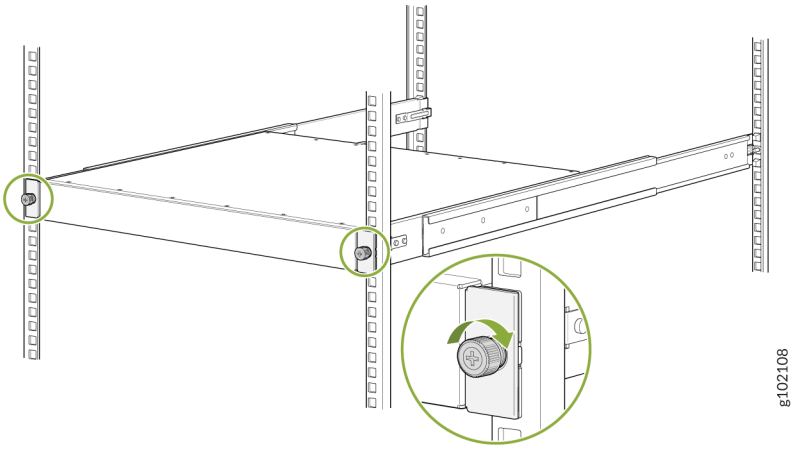
5. Align the guide blocks of the front-mounting rail with the front-post holes. Push the front-mounting rail toward the rear of the rack to lock the rail in place. You'll hear a distinct click when the latch locks into the rack holes.



6. Ensure that the front and rear latches on the mounting rails are locked in place.
7. Lift the device and position it in the rack, aligning the side-mounting brackets with the mounting rails. Slide the device into the channels of the mounting rails.



8. Tighten the two thumbscrews to secure the device.



Connect to Power

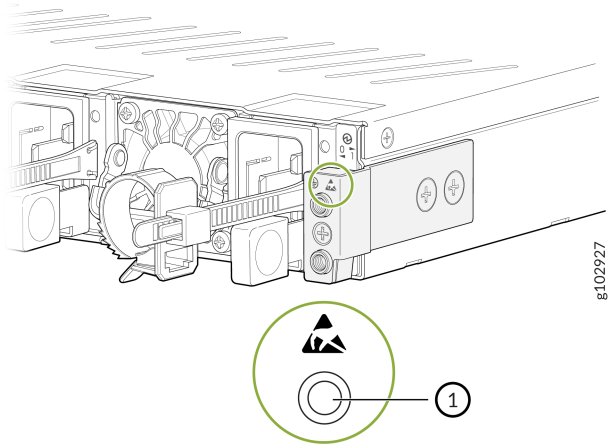
IN THIS SECTION

To connect the SRX4700 Firewall to AC power, you must do the following:

Ground the SRX4700 Firewall

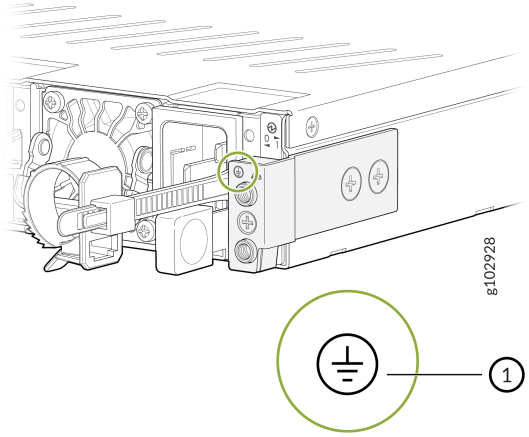
To ground the SRX4700 Firewall:

1. Wrap and fasten one end of the electrostatic discharge (ESD) cable grounding strap around your bare wrist, and connect the other end to a site ESD point or to the ESD point on your device.



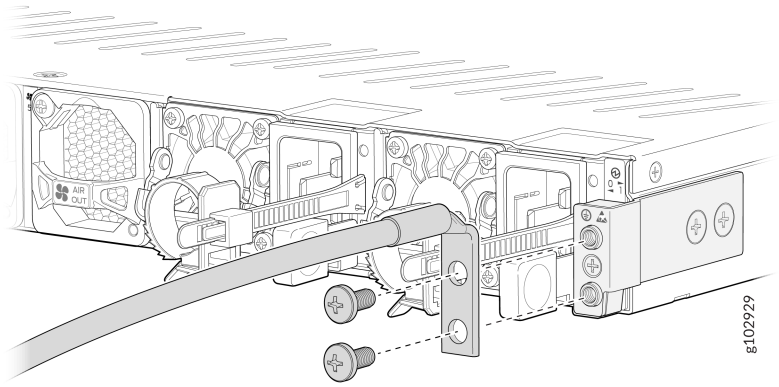
1	Chassis ESD point

2. Connect the grounding cable to a proper earth ground, such as the rack in which you will mount the device.
3. Place the grounding cable terminal attached to the grounding cable over the grounding point.



1	Chassis grounding point

4. Secure the grounding cable terminal to the grounding point using the M5 screws.



5. 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

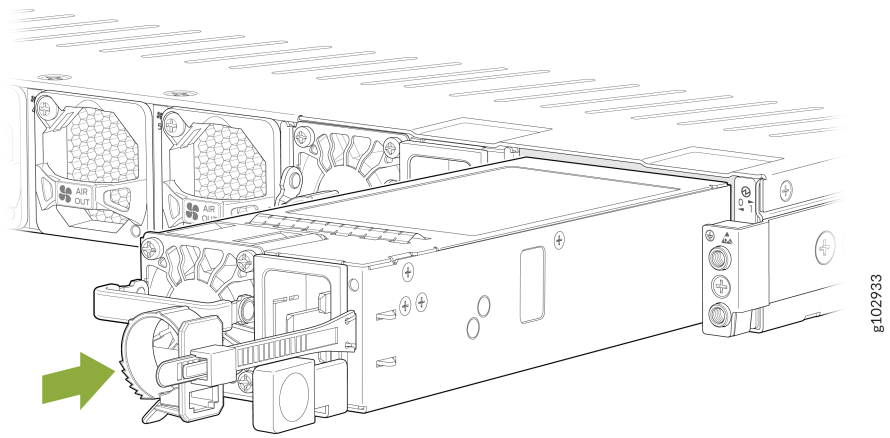
The AC-powered SRX4700 firewall comes with two AC power supply units (PSUs) preinstalled on the rear panel.

NOTE: Each PSU must be connected to a dedicated AC power feed and a dedicated customer-site circuit breaker. We recommend using a circuit breaker rated for 16 A (250 VAC) minimum, or as required by local code.

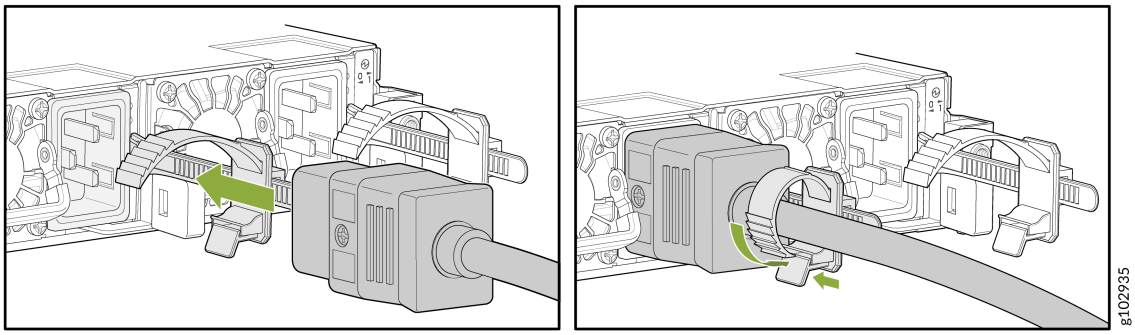
For information about the supported AC power cord specifications, see "Supported AC Power Cords" on page 29.

To connect the power cord and power on the firewall:

1. Ensure that the PSU is fully inserted in the rear panel of the firewall.



2. Insert the coupler end of the power cord into the AC power cord socket.
3. Push the retainer clip through the loop and tighten it until it fits snug around the power cord.



4. Route the power cord so that it doesn't block the air exhaust and access to firewall components, or drape where people could trip on it.
5. If the AC power source outlet has a power switch, turn it off.
6. Plug the power cord into an AC power source outlet.
7. 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 SRX4700

SUMMARY

This topic provides you the pointers to onboard the SRX4700 firewalls and configure them using Juniper® Mist, Juniper® Security Director, J-Web, and Junos OS CLI.

The SRX4700 is a cloud-ready device, and you can manage it using the Mist AI cloud portal. If you have a Mist WAN Assurance license, you can follow a few simple steps to get the SRX4700 up and running in the Mist AI cloud portal.

Table 1: Claim, Onboard and Configure the SRX4700 using Mist

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

If you have a Juniper® Security Director license, you can follow a few simple steps to get an SRX4700 up and running on the Juniper® Security Director Cloud portal.

Table 2: Onboard and Configure SRX4700 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 SRX4700 using the J-Web GUI. See Table 3 on page 9 for more information.

Table 3: Configure SRX4700 Using J-Web

If you want to	Then
Customize basic configuration	See "Configure the SRX4700 Using J-Web " on page 84
Configure additional features using J-Web	See J-Web for SRX Series Documentation
Set up your SRX4700 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 SRX4700 using the Junos OS CLI. See Table 4 on page 9 for more information.

Table 4: Configure SRX4700 Using Junos OS CLI

If you want to	Then
Customize basic configuration	See "Configure Root Authentication and the Management Interface from the CLI" on page 85
Explore the software features supported on the SRX4700	See Feature Explorer
Configure Junos features on the SRX4700	See User Guides

2

CHAPTER

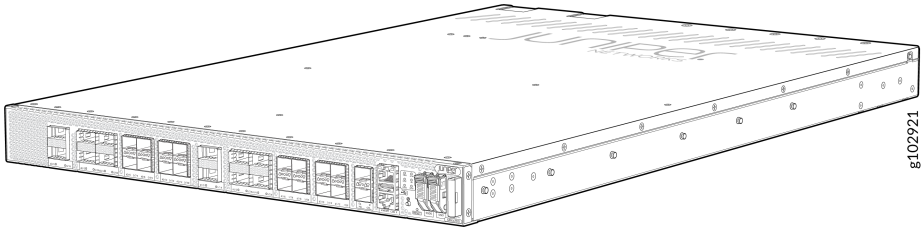
Overview

IN THIS CHAPTER

SRX4700 Firewall Overview

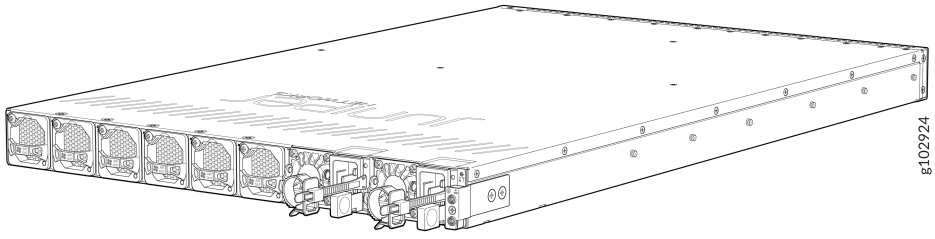
IN THIS SECTION

The Juniper Networks SRX4700 Firewall is a compact 1-U fixed form factor, high-performance, next-generation firewall device that offers scalable security services. The firewall supports 1.4-Tbps Internet Mix (IMIX) throughput, is suited for service providers, cloud providers, and large enterprises. In addition, enterprises can deploy the SRX4700 as data center core and data center edge firewalls and as a secure software-defined WAN (SD-WAN) hub.

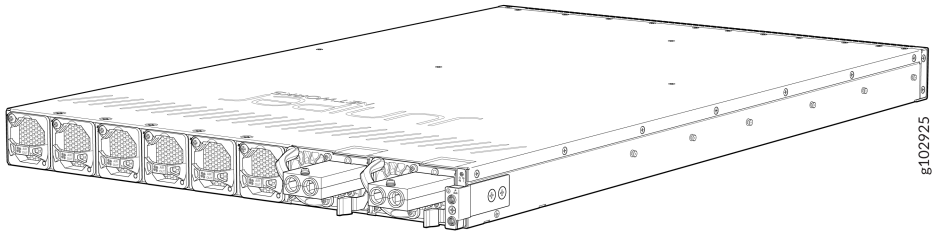


The firewall is available in both AC-powered and DC-powered models.

- SRX4700 (AC)—SRX4700 Firewall with dual AC power supplies



- SRX4700 (DC)—SRX4700 Firewall with dual DC power supplies



The SRX4700 Firewall is shipped with two field-replaceable solid-state drives (SSDs): one 1 TB SSD and one 2 TB SSD.

Field-Replaceable Units

Field-replaceable units (FRUs) are components that you can replace at your site. The following FRUs in the firewall are hot-removable and hot-insertable—that is, you can remove and replace them without powering off the firewall or disrupting the firewall functions:

- Fan modules
- Power Supply Units
- Transceivers
- Solid-state drives (SSDs) are FRUs that are not hot-removable and hot-insertable. You need to power off the firewall to replace them.

NOTE: If you have a Juniper J-Care service contract, register any addition, change, or upgrade of hardware components at https://www.juniper.net/customers/support/tools/updateinstallbase/ . Failure to do so can result in significant delays if you need replacement parts. This note does not apply if you replace existing components with the same type of component.

System Software

Junos® operating system (Junos OS) powers the SRX4700 Firewall, and Juniper Security Director Cloud manages it. Juniper Security Director Cloud is a unified management experience that connects the organization's current deployments with future architectural rollouts.

Juniper Security Director Cloud uses a single policy framework that enables the implementation of consistent security policies across any environment. The policy framework also expands zero trust to all parts of the network from the edge to the data center.

Benefits

- **High availability hardware**—We've engineered the SRX4700 with hardware redundancy for cooling and power supply. With the firewall's high availability, service providers can maintain an always-on infrastructure base that helps meet stringent service-level agreements (SLAs) across the core.
- **Advanced threat prevention**—You can secure your network with Juniper ATP Cloud integrated with the SRX4700. Juniper ATP Cloud provides advanced threat mitigation and detection capabilities, which help protect your network against potential vulnerabilities such as zero-day attacks and other unknown threats.
- **Easy management and scalability**—The SRX4700 provides centralized management using Juniper's unified management experience, including zero-touch provisioning (ZTP), unbroken visibility, intelligent rule placement, and simplified policy configuration and automation. Supports Network Address Translation (NAT) and automated IPsec VPN deployments via wizards.

SRX4700 Chassis

IN THIS SECTION

The SRX4700 Firewall chassis is a rigid sheet metal structure that houses all the other hardware components.

Chassis Physical Specifications for SRX4700

The SRX4700 Firewall has a 1-U form factor and can be installed in a standard 19-inch rack.

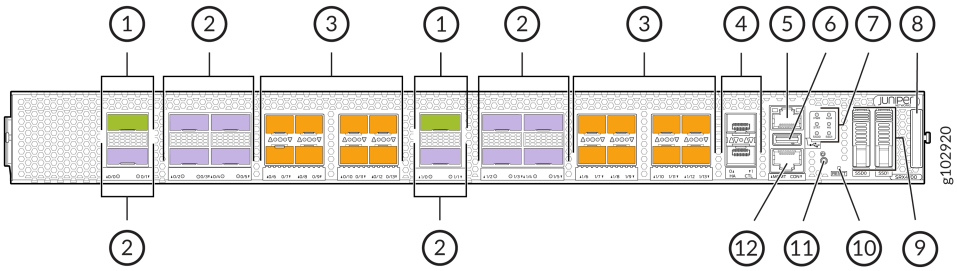
Table 5: Physical Specifications of SRX4700

Model	Height	Width	Depth	Weight
SRX4700 chassis	1.72 in. (4.37 cm)	17.28 in. (43.9 cm)	26.89 in. (68.31 cm)	32.85 lb (14.9 kg)
SRX4700 chassis with AC PSUs			27.29 in (69.32 cm)	40 lb (18.2 kg)
SRX4700 chassis with DC PSUs			29.20 in (74.17 cm)	42 lb (19.1 kg)

Chassis Front Panel

IN THIS SECTION

Figure 1: Front Panel Components of an SRX4700

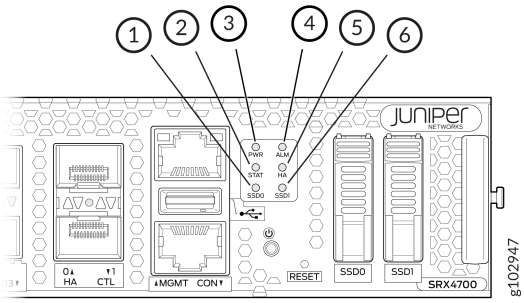


Callout	Component (Label on the Chassis)	Description
1	QSFP56-DD ports	Two 400-Gigabit Ethernet (400 GbE) QSFP56-DD MACsec ports for network traffic
2	QSFP28 ports	Ten 100 GbE QSFP28 MACsec ports for network traffic
3	SFP56 ports	Sixteen 50 GbE SFP56 MACsec ports for network traffic
4	**HA** ports	Two 1 GbE SFP high availability **CTL** ports with MACsec support
5	Management port (**MGMT**)	1-Gigabit Ethernet RJ-45 port
6	USB port	One USB 3.0 Type A port that accepts a USB storage device
7	Chassis LEDs	Indicate component and system status and troubleshoot information at a glance
8	Pull-out information tab	Contains the serial number
9	**SSD0**	1-TB SSD
	SSD1	2-TB SSD

(Continued)

Callout	Component (Label on the Chassis)	Description
10	**RESET**	Reset button. To reset the firewall, press and hold the **RESET** button for around 250 ms
11	Power button	Power button To power on the firewall press and hold the button for 250ms To power off the firewall press and hold the button for 4 seconds
12	Console port (**CON**)	You can connect a laptop to the SRX4700 for CLI management. The port uses an RJ-45 serial connection and supports the RS-232 (EIA-232) standard

Chassis Status LEDs

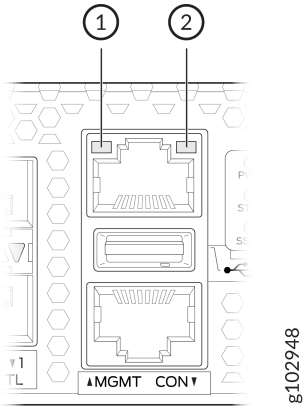


Callout	LED	Description
1	SSD0	• Blinking green—The device is transferring data to or from the SSD storage device. • Solid red—The SSD storage device has failed. • Off—SSD storage device is not present on the device.
2	STAT	• Solid green—The device is operating normally. • Blinking green— The device is powered on and is in the bootup phase before OS initialization • Solid red—A hardware component has failure. • Off—The device is powered off.
3	PWR	• Solid green—The device is powered on. • Blinking green—The device is powered on and is in the bootup phase before OS initialization. • Red—System power failure. • Off—The device is powered off.
4	ALM	• Solid red—Critical alarm • Solid yellow—Non-critical alarm • Off—No alarms

(Continued)

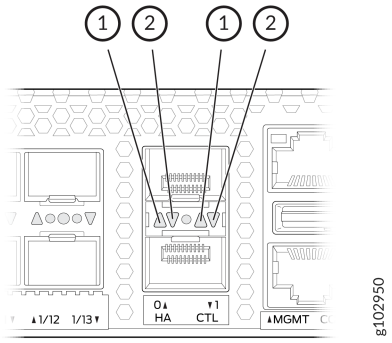
Callout	LED	Description
5	HA	• Solid green—All HA links are available. • Solid yellow—Some HA links are unavailable. • Red—Device is inoperable due to a monitor failure. • Off—HA is disabled.
6	SSD1	• Blinking green—The device is transferring data to or from the SSD storage device. • Solid red—The SSD storage device has failed. • Off—SSD storage device is not present on the device.

Management Port LEDs



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

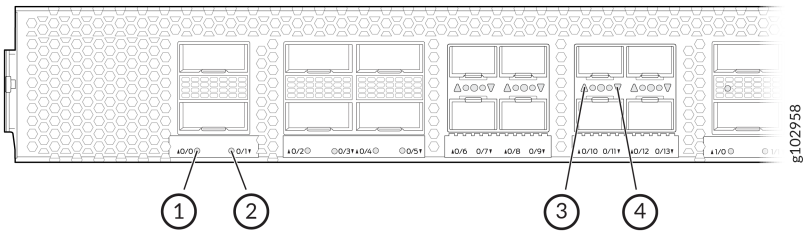
HA Port LEDs



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

Network Port LEDs

Each SRX4700 network port uses a single bicolored LED to indicate link status or a fault condition.



1. Link status LED of QSFP56-DD port 0/0
2. Link status LED of QSFP28 port 0/1
3. Link status LED of SFP56 port 0/10
4. Link status LED of SFP56 port 0/11

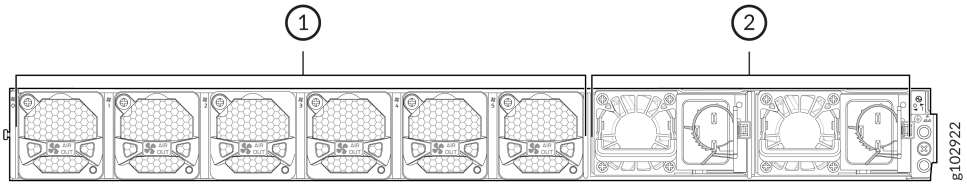
The number next to the LED indicates the port number to which the LED belongs. All network port LEDs behave the same. Table 6 on page 20 describes the network port LEDs on SRX4700 Firewall, their colors and states, and the status that they indicate.

Table 6: Network Port LEDs on SRX4700 Firewall

LED Color	LED State	Description
Unlit	Off	This indicates one of the following events: • Transceiver not present. • The port has been disabled by the administrator.
Green	On steadily	Link is established, and there is link activity.
Amber	On steadily	Port link is down or the port encountered errors such as loss of signal, local fault, or remote fault.
Red	On steadily	The link is down because the port/ transceiver has a hardware failure.

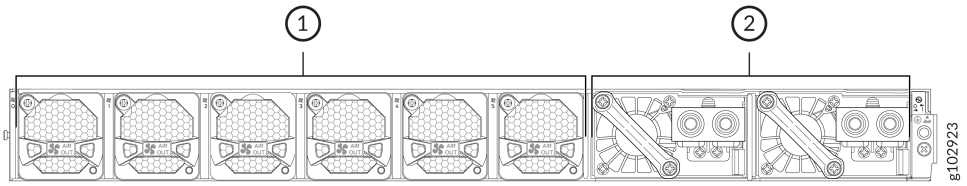
Chassis Rear Panel

Figure 2: Rear Panel Components of the AC Variant of SRX4700



Callout	Component	Description
1	Fan modules	Six airflow out (AFO) fan modules (5+1 redundancy). Five fan modules are required for proper airflow across the chassis internal components. The sixth fan module provides redundancy.
2	Power supply unit (PSU)	Two 2200 W AC PSUs provided with the SRX4700.

Figure 3: Rear Panel Components of the DC Variant of SRX4700



Callout	Component	Description
1	Fan modules	Six airflow out (AFO) fan modules (5+1 redundancy). Five fan modules are required for proper airflow across the chassis internal components. The sixth fan module provides redundancy.
2	Power supply unit (PSU)	Two 2200 W DC PSUs provided with the SRX4700.

Cooling System and Airflow in SRX4700 Firewalls

IN THIS SECTION

The cooling system in the SRX4700 firewalls consists of six fan modules. In addition to the fans, an internal fan in each PSU also cools the device components. We ship the SRX4700 is shipped with 5+1 redundant fan modules preinstalled in the rear panel.

Fan Modules

The six fan modules in SRX4700 firewalls are hot-insertable and hot-removable field-replaceable units (FRUs). You can remove and replace them without powering off the firewall or disrupting firewall functions. The fan modules are installed in the fan module slots on the rear panel of the firewall. The fan module slots are numbered 0 through 5 from left to right. Each fan module slot has a fan icon and a fan module status LED.

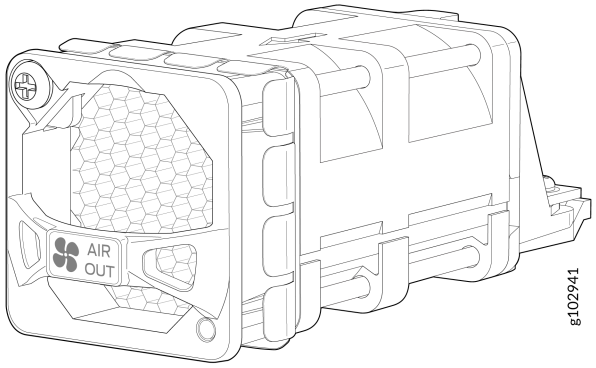


Table 7: Physical Specifications of the SRX4700 Fan Modules

Height	Width	Depth	Weight
1.63 in. (4.14 cm)	1.63 in. (4.14 cm)	4.58 in. (11.63 cm)	0.16 lb (73 g)

NOTE:

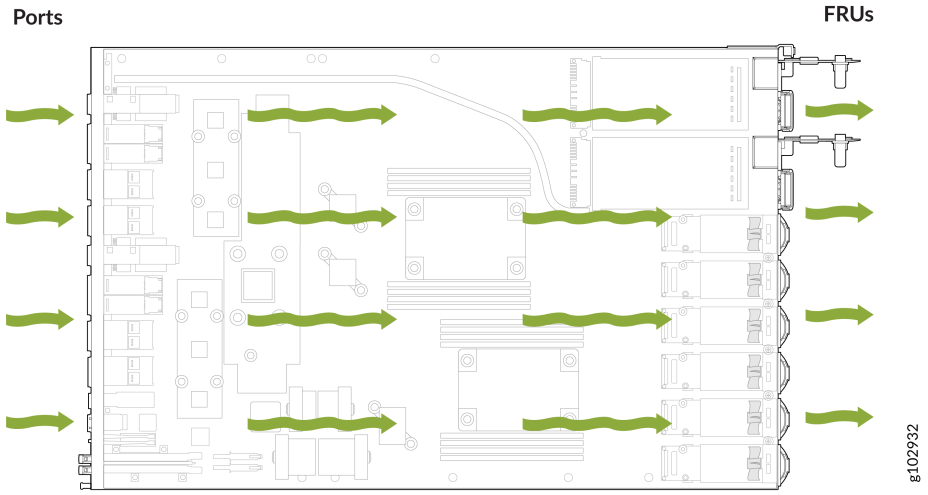
- You must install all the fan modules, and the fan modules must be operational for optimal functioning of the firewall.
- Under normal operating conditions, the fan modules operate at a moderate speed. Temperature sensors in the chassis monitor the temperature within the chassis.

  If a fan module fails or if the ambient temperature inside the chassis rises above the acceptable range, Junos OS raises an alarm. If the temperature inside the chassis rises above the threshold temperature, the system shuts down automatically.

Airflow

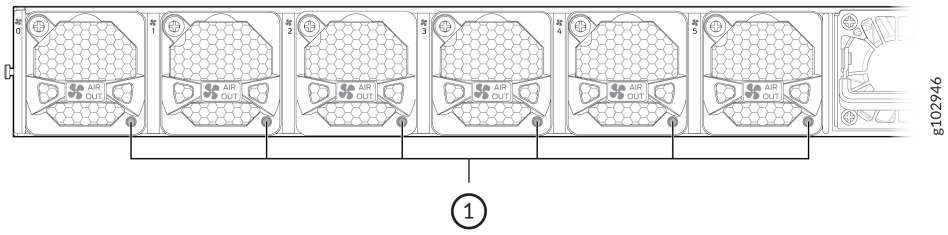
The SRX4700 firewall provides front-to-back airflow. The fan modules pull the air toward them through the front of the chassis and exhaust it out through the back of the chassis.

Figure 4: Airflow Through the SRX4700 Chassis



SRX4700 Fan Module LEDs

You can examine the LEDs on each fan module to check the status of the fans.



1. Fan Modules LEDs

Table 8: Fan Module LEDs

LED Color	LED State	Description
Green	On steadily	The fan module is operating normally. The system has verified that the module is engaged, that the airflow is in the correct direction, and that the fan is operating correctly.

Table 8: Fan Module LEDs *(Continued)*

LED Color	LED State	Description
Red	On steadily	The system has detected an error in the fan module. Replace the module immediately. Either the fan has failed, or it is seated incorrectly. To maintain proper airflow through the chassis, leave the fan module installed in the chassis until you are ready to replace it.

SRX4700 Power System

SUMMARY

The SRX4700 power system includes AC and DC power supply units (PSUs) and related power cords, cables, and cable lugs. The PSUs operate within specified ranges and are equipped with alarms and indicators.

IN THIS SECTION

The SRX4700 Firewall ships with two AC or two DC PSUs (1+1 redundancy) preinstalled in the rear panel of the chassis in slots labeled 0 and 1. These PSUs are hot-removable and hot-insertable field replaceable units (FRUs). You can install the PSUs without powering off the firewall or disrupting the firewall function.

The SRX4700 firewall supports the following AC and DC PSUs:

- JNP-PWR2200-AC
- JNP-PWR2200-DC

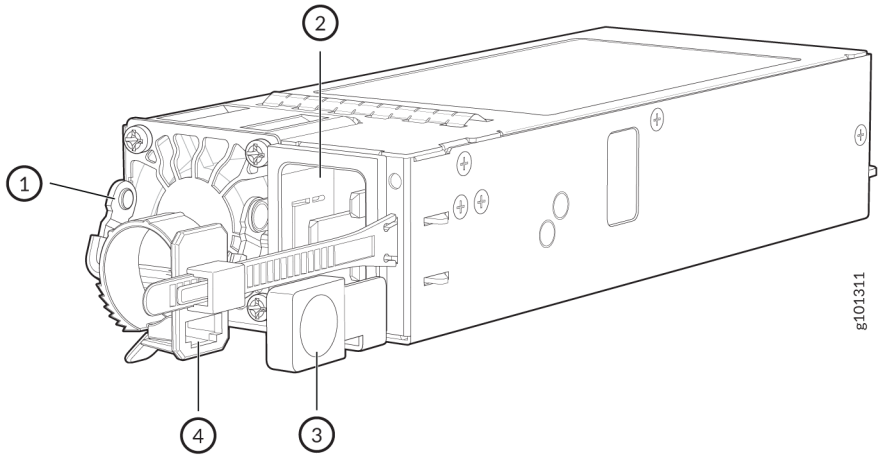
CAUTION: Do not mix AC and DC PSUs in the same chassis.

SRX4700 AC Power Supply Unit

IN THIS SECTION

The SRX4700 firewall supports 2200-W AC PSUs that you can monitor using an inter-integrated circuit (I^2C) bus from the boot complex programmable logic device (boot CPLD). The PSUs directly plug into the connectors provided on the CPU board. The 12 V outputs from both the PSUs are shorted on the main board and are used by on-board voltage regulators for generating downstream voltages.

Each AC PSU weighs approximately 2.42 lb (1.1 kg) and consists of a handle, an ejector lever, an AC appliance inlet, a fan, and a bicolor LED that helps monitor the status of the PSU. Each inlet requires a dedicated AC power feed and a dedicated customer-site circuit breaker. We recommend that you use a minimum 16 A customer-site circuit breaker, or as required by local code.



1. Handle
2. AC inlet plug
3. Ejector lever
4. Power cord retainer

Each AC PSU provides power to all components in the firewall. The two PSUs provide full power redundancy to the firewall. If one PSU fails or is removed, the second PSU balances the electrical load without interruption. The firewall reassesses the power required to support the firewall configuration and issues error messages if the available power is insufficient.

WARNING: The firewall is pluggable type A equipment installed in a restricted-access location. It has a separate protective earthing terminal provided on the chassis in addition to the grounding pin of the power supply cord. This separate protective earthing terminal must be permanently connected to earth ground.

AC Power Supply Unit Electrical Specifications

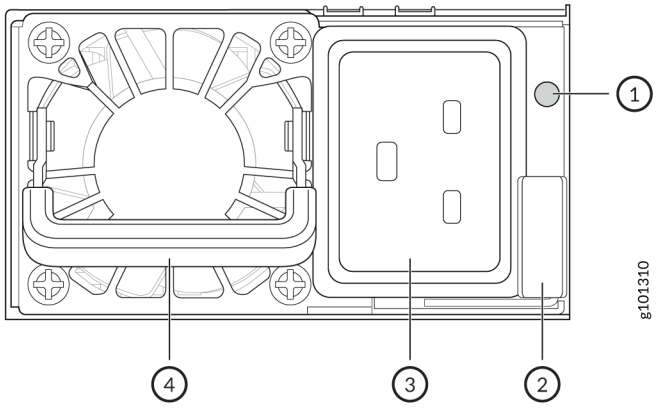
Table 9: AC Power Supply Unit Electrical Specifications

Item	Specification
Maximum output power	100 V—127 V: 1100 W 200 V—240 V: 2200 W
AC input nominal voltage	100 V—127 VAC 200 V—240 VAC
AC input voltage	Operating range: 90—264 VAC
AC input line frequency	47—63 Hz (nominal)
AC system current rating	13 A @100 VAC—240 VAC

AC Power Supply Unit LED

Figure 5 on page 28 shows the AC PSU components along with the location of one bicolor LED on the faceplate of the AC PSU. This LED displays information about the status of the PSU.

Figure 5: AC Power Supply Unit Components and LED



1– Status LED	3– AC inlet plug
2– Ejector lever	4– Handle

Table 10: AC Power Supply Unit LED

Label	Color	State	Description
STATUS	Green	Blinking (1Hz)	PSU is in standby state
		Blinking (2Hz)	PSU firmware is updating
		On steadily	The PSU is functioning normally
	Amber	On steadily	PSU is faulty and not functioning normally; failure, overcurrent, short circuit, over voltage, fan failure, or over temperature. AC cord is unplugged or AC power is lost
		Blinking (1Hz)	PSU warning events where the PSU continues to operate; high temperature or high power
	Off		No AC power to all the PSUs

Supported AC Power Cords

A detachable AC power cord is supplied with the AC PSUs. The coupler is type C19 as described by International Electrotechnical Commission (IEC) standard 60320. The plug end of the power cord fits into the power source outlet that is standard for your geographical location.

Table 11 on page 29 lists the default power cord that is provided for each country.

CAUTION: The AC power cord provided with each PSU is intended for use with that PSU only and not for any other use.

NOTE: In North America, AC power cords must not exceed 4.5 m in length, to comply with National Electrical Code (NEC) Sections 400-8 (NFPA 75, 5-2.2) and 210-52 and Canadian Electrical Code (CEC) Section 4-010(3). The cords supplied with the switch are in compliance.

Table 11: SRX4700 AC Power Cord Specifications

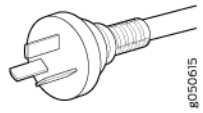
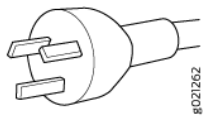
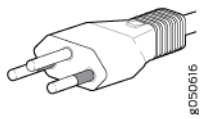
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number	Graphic
Argentina	250 VAC, 16 A, 50 Hz	IRAM 2073	CBL-EX-PWR-C19-AR	
Australia	250 VAC, 15 A, 50 Hz	AS/NZS 3112	CBL-EX-PWR-C19-AU	
Brazil	250 VAC, 16 A, 50 Hz	NBR 14136	CBL-EX-PWR-C19-BR	

Table 11: SRX4700 AC Power Cord Specifications *(Continued)*

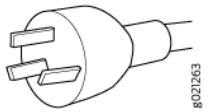
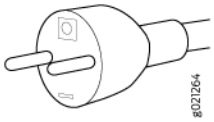
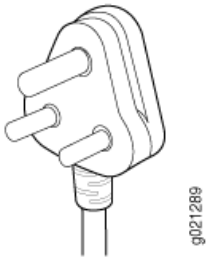
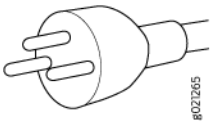
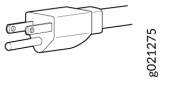
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number	Graphic
China	250 VAC, 16 A, 50 Hz	GB 2099	CBL-EX-PWR-C19-CH	
Europe (except Italy, Switzerland, and United Kingdom)	250 VAC, 16 A, 50 Hz	CEE (7) 7	CBL-EX-PWR-C19-EU	
India	250 AC, 16 A, 50 Hz	IS 1293 and IS694	CBL-SRX-PWR-C19-IN	
Israel	250 AC, 16 A, 50 Hz	SI 32	CBL-EX-PWR-C19-IL	
Italy	250 VAC, 16 A, 50 Hz	CEI 23-16	CBL-EX-PWR-C19-IT	
Japan	125 VAC, 15 A, 50 Hz or 60 Hz	NEMA5-15Type N5/15	CBL-EX-PWR-C19-JP110V	

Table 11: SRX4700 AC Power Cord Specifications *(Continued)*

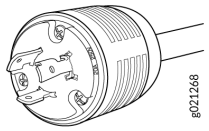
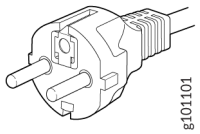
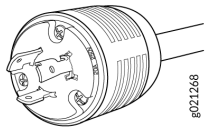
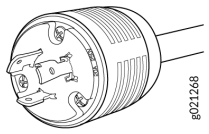
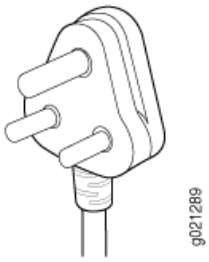
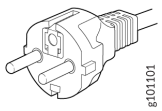
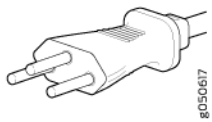
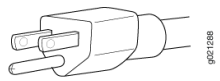
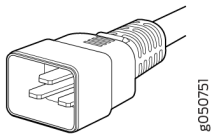
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number	Graphic
	250 VAC, 15 A, 50 Hz or 60 Hz	NEMA L6-20	CBL-PWR-C19-HT-JP	
Korea	250 VAC, 16 A, 50 Hz	KC 8305	CBL-EX-PWR-C19-KR	
North America	250 VAC, 20 A 50 Hz or 60 Hz	NemaNEMA 6-20	CBL2-PTX-SP-US-N	
	250 VAC, 20 A 50 or 60 Hz	NEMA L6-20P	CBL2-PTX-SP-US-L	
South Africa	250 VAC, 16 A, 50 Hz	SABS 164-1	CBL-EX-PWR-C19-SA	
South Korea	250 VAC, 16 A, 50 Hz	C19 to CEE (7) VII	CBL-SRX-PWR-C19-SK	

Table 11: SRX4700 AC Power Cord Specifications *(Continued)*

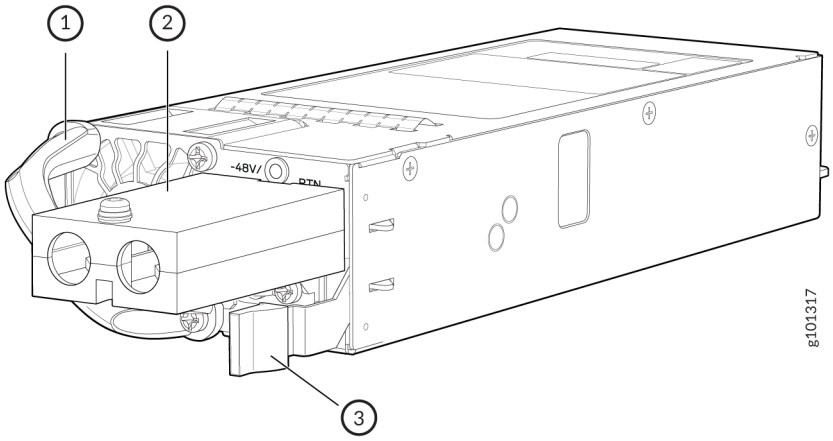
Country/Region	Electrical Specifications	Plug Standards	Juniper Model Number	Graphic
Switzerland	250 VAC, 16 A, 50 Hz	SEV 5934/2 (Type 23 16A plug)	CBL-EX-PWR-C19-SZ	
Taiwan	250 VAC, 15 A, 50 Hz	C19 to CNS 690	CBL-SRX-PWR-C19-TW	
United Kingdom	250 VAC, 13 A, 50 Hz	BS 1363(A)	CBL-EX-PWR-C19-UK	
Worldwide (except Japan)	250 VAC, 16 A, 50 Hz	EN 60320-2-2/1	CBL-EX-PWR-C19-C20	

SRX4700 DC Power Supply Unit

IN THIS SECTION

The DC PSU is a hot-removable and hot-insertable field-replaceable unit (FRU). You can install it without powering off the firewall or disrupting the firewall function.

Each DC PSU weighs approximately 2.42 lb (1.1 kg) and consists of a handle, an ejector lever, a bi-color status LED, and a terminal block that provides a single DC input (–48/–60 VDC and return). The DC PSU requires a dedicated customer-site circuit breaker. We recommend that you use a dedicated customer-site circuit breaker rated for 60 A (80 VDC), or as required by local code.



1– Handle	3– Ejector lever
2– DC inlet cable lug point	

Each DC PSU provides power to all components in the firewall. The two PSUs provide full power redundancy to the firewall. If one PSU fails or is removed, the second PSU balances the electrical load without interruption. The firewall reassesses the power required to support the firewall configuration and issues error messages if the available power is insufficient.

DC Power Supply Unit Electrical Specifications

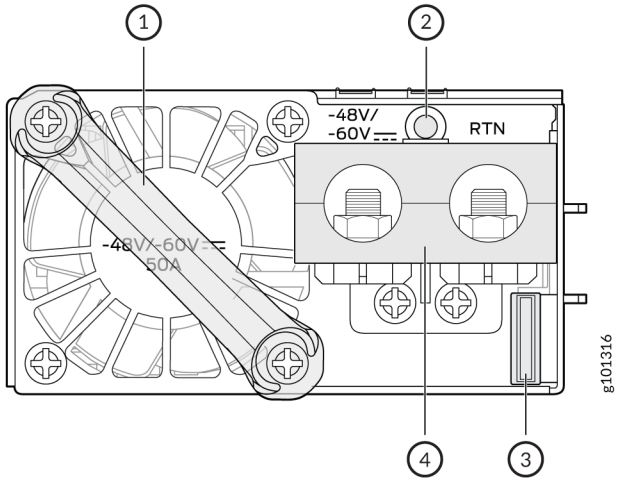
Table 12: DC Power Supply Unit Electrical Specifications

Item	Specification
Maximum output power	2200 W
DC input voltage	Minimum: –40 VDC Nominal: –48 VDC through –60 VDC Operating range: –40 through –72 VDC
DC input current rating	50 A maximum

DC Power Supply Unit LEDs

Figure 6 on page 34 shows the DC PSU components along with the location of one bicolor LED on the faceplate of the DC PSU. This LED displays information about the status of the PSU.

Figure 6: DC Power Supply Unit Components and LED



1– Handle	3– Ejector lever
2– Status LED	4– DC inlet cable lug point

Table 13: DC Power Supply Unit LED

Label	Color	State	Description
STATUS	Green	Blinking (1 Hz)	PSU is in standby state.
		Blinking (2 Hz)	PSU firmware is updating.
		On steadily	The PSU is functioning normally

Table 13: DC Power Supply Unit LED *(Continued)*

Label	Color	State	Description
	Amber	On steadily	PSU is faulty and not functioning normally; failure, overcurrent, short circuit, over voltage, fan failure, or over temperature. DC cord is unplugged or DC power is lost.
		Blinking (1 Hz)	PSU warning events where the PSU continues to operate; high temperature or high power.
	Off		No DC power to both the PSUs.

DC Power Circuit Breaker Requirements for the SRX4700 Firewall

Each DC PSU has a single DC input (–48 VDC and return) that requires a dedicated circuit breaker. We recommend that you use a dedicated customer-site circuit breaker rated for 60 A (80 VDC), or as required by local code. Doing so enables you to operate the firewall in any configuration without upgrading the power infrastructure.

DC Power Cable Specifications

IN THIS SECTION

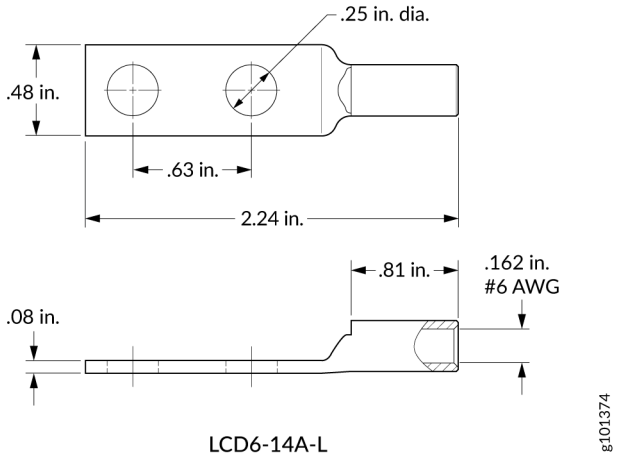
DC Power Cable Lug Specifications

The DC power lug LCD-14A-L accommodates 6 AWG (13 mm^2) stranded wire. The grounding cable that you provide for the chassis must be the same size as or heavier than the input wire of each PSU. Minimum recommendations are 6 AWG (13 mm^2) stranded wire, minimum 60 °C wire, or as permitted by local code.

DC power cords and lugs are not supplied with the DC PSUs.

Install heat-shrink tubing insulation around the power cables at the connection point of the DC power supply terminal.

Figure 7: DC Power Cable Lug



CAUTION: Before you install the firewall, 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 firewall.

DC Power Cable Specifications

You must supply four DC power cables that meet the following specifications: 6 AWG (13 mm^2) stranded wire, minimum 60 °C wire, or as permitted by local code.

NOTE: Install heat-shrink tubing insulation around the power cables at the connection point of the DC PSU terminal.

CHAPTER 3

Site Planning, Preparation, and Specifications

IN THIS CHAPTER

Site Guidelines and Requirements for SRX4700

SUMMARY

The proper function of the SRX4700 depends on your meeting certain environmental requirements, following site and wiring guidelines, and ensuring that your installation meets the grounding specifications and airflow clearance requirements that support SRX4700 .

IN THIS SECTION

Site Preparation Checklist for SRX4700

The checklist in Table 14 on page 38 summarizes the tasks you need to perform when preparing a site for SRX4700 installation.

Table 14: Site Preparation Checklist

Item or Task	For More Information	Performed by	Date
Environment			
Verify that environmental factors such as temperature and humidity do not exceed router tolerances.	"Environmental Requirements and Specifications for SRX4700" on page 40		
Power			

Table 14: Site Preparation Checklist *(Continued)*

Item or Task	For More Information	Performed by	Date
Measure the distance between the external power sources and the router installation site.	"Clearance Requirements for Airflow and Hardware Maintenance for SRX4700" on page 48		
Locate sites to connect system grounding.			
Rack or Cabinet			
Verify that the rack or cabinet meets the minimum requirements for installing the router.	• Rack Requirements • "Cabinet Requirements" on page 47		
Plan rack or cabinet location, including required space clearances.			
Secure the rack or cabinet to the floor and building structure.			
Cables			
Acquire the cables and connectors: • Determine the number of cables needed based on your planned configuration. • Review the maximum distance allowed for each cable. Choose the length of the cable based on the distance between the hardware components being connected.			

Table 14: Site Preparation Checklist *(Continued)*

Item or Task	For More Information	Performed by	Date
Plan the cable routing and management.			

Environmental Requirements and Specifications for SRX4700

You must install the router in a rack or cabinet. You must house the router in a dry, clean, well-ventilated, and temperature-controlled environment.

Follow these environmental guidelines:

- Keep the site as dust-free as possible, because dust can clog air intake vents and filters, reducing the efficiency of the router cooling system.
- Maintain ambient airflow for normal router operation. If the airflow is blocked or restricted, or if the intake air is too warm, the router might overheat, leading to the router temperature monitor shutting down the device to protect the hardware components.

Table 15 on page 40 provides the required environmental conditions for normal router operation.

Table 15: SRX4700 Environmental Tolerances

Altitude	Relative Humidity	Temperature	Seismic
6000 ft	Normal operation ensured in the relative humidity range of 5% through 85%, noncondensing.	• Normal operation ensured in the temperature range of 32 °F through 104 °F (0 °C through 40 °C). • Nonoperating storage temperature in shipping container: –40 °F through 158 °F (–40 °C through 70 °C).	Designed to comply with Zone 4 earthquake requirements per DC NEBS GR-3160.

NOTE: Install the firewall 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.

General Electrical Safety Guidelines and Warnings for SRX4700

WARNING: Certain ports on the device are designed for use as intrabuilding (within-the-building) interfaces only (Type 2 or Type 4 ports as described in *GR-1089-CORE*) and require isolation from the exposed outside plant (OSP) cabling. To comply with NEBS (Network Equipment-Building System) requirements and protect against lightning surges and commercial power disturbances, the intrabuilding ports *must not* be metallically connected to interfaces that connect to the OSP or its wiring. The intrabuilding ports on the device are suitable for connection to intrabuilding or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection for connecting these interfaces metallically to OSP wiring.

Avertissement Certains ports de l'appareil sont destinés à un usage en intérieur uniquement (ports Type 2 ou Type 4 tels que décrits dans le document *GR-1089-CORE*) et doivent être isolés du câblage de l'installation extérieure exposée. Pour respecter les exigences NEBS et assurer une protection contre la foudre et les perturbations de tension secteur, les ports pour intérieur *ne doivent pas* être raccordés physiquement aux interfaces prévues pour la connexion à l'installation extérieure ou à son câblage. Les ports pour intérieur de l'appareil sont réservés au raccordement de câbles pour intérieur ou non exposés uniquement. L'ajout de protections ne constitue pas une précaution suffisante pour raccorder physiquement ces interfaces au câblage de l'installation extérieure.

CAUTION: Before removing or installing components of a device, connect an electrostatic discharge (ESD) grounding strap to an ESD point and wrap and fasten the other end of the strap around your bare wrist. Failure to use an ESD grounding strap could result in damage to the device.

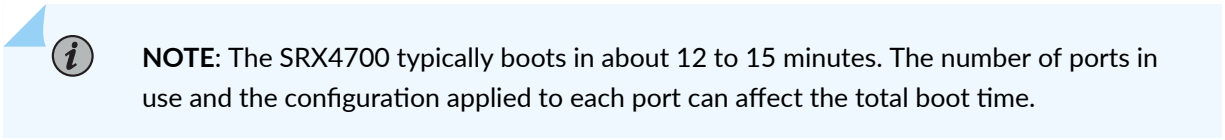
Attention Avant de retirer ou d'installer des composants d'un appareil, raccordez un bracelet antistatique à un point de décharge électrostatique et fixez le bracelet à votre poignet nu. L'absence de port d'un bracelet antistatique pourrait provoquer des dégâts sur l'appareil.

- Install the device in compliance with the following local, national, and international electrical codes:

  - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code.
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7.
  - Evaluated to the TN power system.
  - Canada—Canadian Electrical Code, Part 1, CSA C22.1.
  - Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

    Peut être installé dans des salles de matériel de traitement de l'information conformément à l'article 645 du National Electrical Code et à la NFPA 75.

- 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.
- Make sure that you clean grounding surface and give them a bright finish before making grounding connections.
- 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 device within marked electrical ratings and product usage instructions.
- To ensure that the device and peripheral equipment function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.



NOTE: The SRX4700 typically boots in about 12 to 15 minutes. The number of ports in use and the configuration applied to each port can affect the total boot time.

You can remove and replace many device components without powering off or disconnecting power to the device, as detailed elsewhere in the hardware documentation for this device. Never install equipment that appears to be damaged.

General Site Guidelines

Efficient device operation requires proper site planning. For the device to operate properly, you must ensure maintenance and proper layout of the equipment, rack or cabinet, and wiring closet.

To plan and create an acceptable operating environment for your device and prevent environmentally caused equipment failures:

- Keep the area around the chassis free from dust and conductive material, such as metal flakes.
- Follow the prescribed airflow guidelines to ensure that the cooling system functions properly. Ensure that the exhaust from other equipment does not blow into the intake vents of the device.
- Follow the prescribed electrostatic discharge (ESD) prevention procedures to prevent damaging the equipment. Static discharge can cause components to fail completely or intermittently over time.
- Install the device in a secure area, so that only authorized personnel can access the device.

Site Electrical Wiring Guidelines

Table 16 on page 44 describes the factors you must consider while planning the electrical wiring at your site.

WARNING: You must provide a properly grounded and shielded environment and use electrical surge-suppression devices.

Avertissement Vous devez établir un environnement protégé et convenablement mis à la terre et utiliser des dispositifs de parasurtension.

Table 16: Site Electrical Wiring Guidelines

Site Wiring Factor	Guidelines
Signaling limitations	If your site experiences any of the following problems, consult experts in electrical surge suppression and shielding: • Radio frequency interference (RFI) because of improperly installed wires. • Damage from lightning strikes occurring when wires exceed recommended distances or pass between buildings. • Damage to unshielded conductors and electronic devices as a result of electromagnetic pulses (EMPs) caused by lightning.
Radio frequency interference	To reduce or eliminate RFI from your site wiring, do the following: • Use a twisted-pair cable with a good distribution of grounding conductors. • If you need to exceed the recommended distances, use a high-quality twisted-pair cable with one ground conductor for each data signal, when applicable.
Electromagnetic compatibility	If your site is susceptible to problems with electromagnetic compatibility (EMC), particularly from lightning or radio transmitters, seek expert advice. Strong sources of electromagnetic interference (EMI) can cause: • Destruction of the signal drivers and receivers in the device. • Electrical hazards as a result of power surges conducted over the lines into the equipment.

Rack Requirements for SRX4700

You can mount the SRX4700 on four-post racks. The rack mounting kit (JNP-4P-TL-1RU-RMK) is shipped with the firewall. Table 17 on page 45 provides the rack requirements and specifications for SRX4700.

Table 17: Rack Requirements and Specifications

Rack Requirement	Guidelines
Rack type	Use a four-post rack with bracket holes or hole patterns spaced at 1 U increments (1.75 in. or 4.45 cm). Ensure that the rack meets the size and strength requirements to support the weight. A U is the standard rack unit as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310–D) published by the Electronics Industry Association.
Mounting bracket hole spacing	Ensure that the holes in the mounting brackets are spaced at 1U (1.75 in. or 4.45 cm) increments so that the device can be mounted in any rack that provides holes that are spaced at that distance. The front rack opening between the flanges must be 450 mm wide + 2 mm (17.75 in. + 0.08 in.).

Table 17: Rack Requirements and Specifications *(Continued)*

Rack Requirement	Guidelines
Rack size and strength	• Ensure that the rack complies with the standards for a 19 in. rack as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310–D) published by the Electronics Industry Association. Use an 800 mm rack as defined in the four-part Equipment Engineering (EE) European telecommunications standard for equipment practice (document numbers ETS 300 119-1 through 119-4) published by the European Telecommunications Standards Institute (http://www.etsi.org). • The horizontal spacing between the rails in a rack compliant with this standard is usually wider than the device's mounting brackets. The mounting brackets measure 19 in. (48.26 cm) from outer edge to outer edge. Use approved wing devices to narrow the opening between the rails as required. • Ensure that the rack rails are spaced widely enough to accommodate the external dimensions of the device chassis. The outer edges of the front-mounting brackets extend the width to 19 in. (48.26 cm). • Ensure that for four-post installations, the front and rear rack rails are spaced between 23.6 in. (60 cm) and 36 in. (91.4 cm) front-to-back. • Ensure that the rack is strong enough to support the weight of the device. A fully-configured SRX4700 with 2 PSUs weighs about 42 lb (19.1 kg). • Ensure that the spacing of rails and adjacent racks allows for proper clearance around the device and rack.

Table 17: Rack Requirements and Specifications *(Continued)*

Rack Requirement	Guidelines
Rack connection to building structure	• Secure the rack to the building structure. • If earthquakes occur in your geographical area, secure the rack to the floor. • Secure the rack to the ceiling brackets and to wall or floor brackets for maximum stability.

Cabinet Requirements

You can mount the device in a cabinet that contains a 19-in. rack.

Table 18: Cabinet Requirements and Specifications

Cabinet Requirement	Guidelines
Cabinet size and clearance	• The minimum cabinet size is 27.7 in. (70.35 cm) between cabinet front door and cabinet rear wall. It is recommended to have minimum of 6 in. clearance from the cabinet front door and switch front panel minimum of 6 in. clearance from the cabinet rear wall and switch rear panel. Large cabinets improve airflow and reduce chances of overheating. • The outer edges of the front mounting brackets extend the width of the chassis to 19 in. (48.2 cm).

Table 18: Cabinet Requirements and Specifications *(Continued)*

Cabinet Requirement	Guidelines
Cabinet airflow requirements	When you mount the device in a cabinet: • Ensure that ventilation through the cabinet is sufficient to prevent overheating. • Ensure that there is adequate cool air supply to dissipate the thermal output of the device or devices. • Ensure that the hot air exhaust of the chassis exits the cabinet without recirculating into the device. An open cabinet (without a top or doors) that employs hot air exhaust extraction from the top ensures the best airflow through the chassis. If the cabinet contains a top or doors, perforations in these elements assist with removing the hot air exhaust. • Install the device in the cabinet in a way that maximizes the open space on the side of the chassis that has the hot air exhaust. • Route and secure all cables to minimize the blockage of airflow to and from the chassis. • Ensure that the spacing of rails and adjacent cabinets is such that proper clearance exists around the device and cabinet. • A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

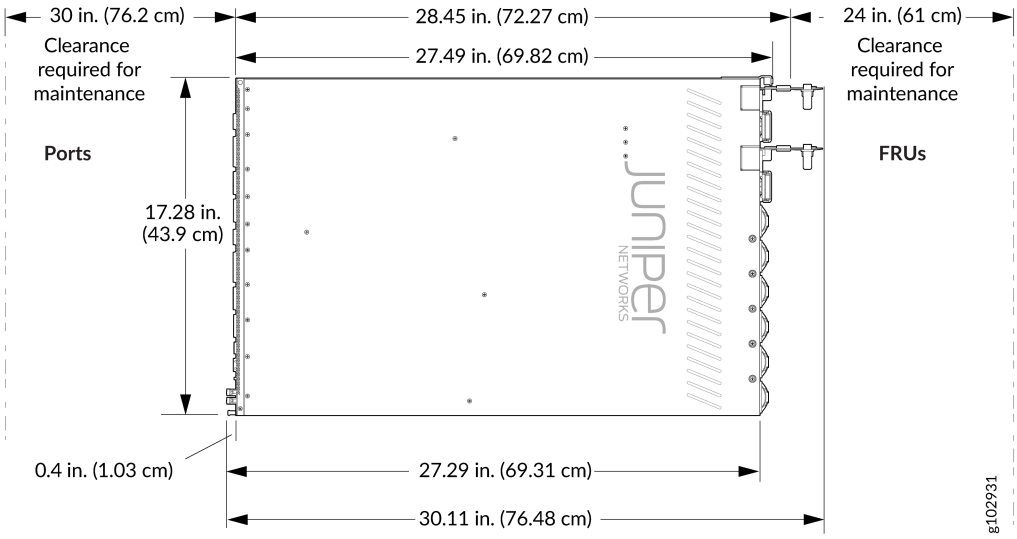
Clearance Requirements for Airflow and Hardware Maintenance for SRX4700

When planning the site for installing a SRX4700, follow these clearance requirements (see Figure 8 on page 49):

- For the cooling system to function properly, ensure that the airflow around the chassis is unrestricted.
- If you are mounting the router on a rack or cabinet along with other equipment, ensure that the hot air exhaust from other equipment does not blow into the cold air intake vents of the chassis.

- DC NEBS GR-3160 recommends that you allow at least 30 in. (76.2 cm) in front of the rack or cabinet for chassis replacement and 24 in. (61 cm) in rear for component replacement.

Figure 8: Clearance Requirements for Airflow and Hardware Maintenance for SRX4700



SRX4700 Management Cable Specifications and Pinouts

IN THIS SECTION

SRX4700 Cable Specifications for Console and Management Connections

Table 19: Specifications of the Cables for Console and Management Connections

Port on the Firewall	Cable Specification	Maximum Length	Device Receptacle
Console (**CON**) port	RS-232 (EIA-232) serial cable	2.13 m	RJ-45
Management (**MGMT**) port	Category 5 cable or equivalent suitable for 1000 BASE-T operation	100 m	RJ-45

NOTE: We no longer include the RJ-45 console cable with the DB-9 adapter 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 the X64 (64-Bit) Virtual COM port (VCP) driver installed on your PC. See https://ftdichip.com/drivers/vcp-drivers/ to download the driver.

SRX4700 Management Port Connector Pinouts

You must use an RJ-45 connector to connect the 10/100/1000BASE-T management port (labeled **MGMT**) to a management device for out-of-band management.

Table 20: Pinouts of the RJ-45 Management Port Connector on the SRX4700

Pin	Signal	Description
1	TRP1+	Transmit/receive data pair 1

Table 20: Pinouts of the RJ-45 Management Port Connector on the SRX4700 *(Continued)*

Pin	Signal	Description
2	TRP1–	Transmit/receive data pair 1
3	TRP2+	Transmit/receive data pair 2
4	TRP3+	Transmit/receive data pair 3
5	TRP3–	Transmit/receive data pair 3
6	TRP2–	Transmit/receive data pair 2
7	TRP4+	Transmit/receive data pair 4
8	TRP4–	Transmit/receive data pair 4

SRX4700 Console Port Connector Pinouts

The console port (labeled **CON**) is an RS-232 serial interface. You must use an RJ-45 connector to connect to a console management device. The default baud rate for the console port is 9600 baud.

NOTE: If your laptop or PC does not have a DB-9 plug connector pin and you want to connect your laptop or PC directly to the router, use a combination of the RJ-45 cable and RJ-45 to DB-9 adapter and a USB to DB-9 plug adapter. You must provide the USB to DB-9 plug adapter.

Table 21: Pinouts of the Console Port Connector on the SRX4700

Pin	Signal	Description
1	RTS Output	Request to send

Table 21: Pinouts of the Console Port Connector on the SRX4700 *(Continued)*

Pin	Signal	Description
2	DTR Output	Data terminal ready
3	TxD Output (Serial Output)	Transmit data
4	Signal Ground	Signal ground
5	Signal Ground	Signal ground
6	RxD Input (Serial Input)	Receive data
7	DSR/DCD Input	Data carrier detect
8	CTS Input	Clear to send

SRX4700 Network Cable and Transceiver Planning

IN THIS SECTION

Pluggable Transceivers and Cables Supported on SRX4700 Firewall

You can find the list of transceivers and cables supported on SRX4700 routers and information about those transceivers and cables at the Hardware Compatibility Tool page for SRX4700.

NOTE: We recommend that you use only optical transceivers, optical connectors, and cables purchased from Juniper Networks with your Juniper Networks device.

CAUTION: The Juniper Networks Technical Assistance Center (JTAC) provides complete support for Juniper-supplied optical modules and cables. However, JTAC does not provide support for third-party optical modules and cables that are not qualified or supplied by Juniper Networks. If you face a problem running a Juniper device that uses third-party optical modules or cables, JTAC may help you diagnose host-related issues if the observed issue is not, in the opinion of JTAC, related to the use of the third-party optical modules or cables. Your JTAC engineer will likely request that you check the third-party optical module or cable and, if required, replace it with an equivalent Juniper-qualified component.

Use of third-party optical modules with high-power consumption (for example, coherent ZR or ZR+) can potentially cause thermal damage to or reduce the lifespan of the host equipment. Any damage to the host equipment due to the use of third-party optical modules or cables is the users' responsibility. Juniper Networks will accept no liability for any damage caused due to such use.

Fiber-Optic Cable Signal Loss, Attenuation, and Dispersion

IN THIS SECTION

Signal Loss in Multimode and Single-Mode Fiber-Optic Cable

Multimode fiber is large enough in diameter to allow rays of light to reflect internally (bounce off the walls of the fiber). Interfaces with multimode optics typically use LEDs as light sources. However, LEDs are not coherent sources. They spray varying wavelengths of light into the multimode fiber, which reflects the light at different angles. Light rays travel in jagged lines through a multimode fiber, causing signal dispersion. When light traveling in the fiber core radiates into the fiber cladding, higher-order mode loss results. Together these factors limit the transmission distance of multimode fiber compared with single-mode fiber.

Single-mode fiber is so small in diameter that rays of light can reflect internally through one layer only. Interfaces with single-mode optics use lasers as light sources. Lasers generate a single wavelength of light, which travels in a straight line through the single-mode fiber. Compared with multimode fiber, single-mode fiber has a higher bandwidth and can carry signals for longer distances.

Exceeding the maximum transmission distances can result in significant signal loss, which causes unreliable transmission.

Attenuation and Dispersion in Fiber-Optic Cable

Correct functioning of an optical data link depends on modulated light reaching the receiver with enough power to be demodulated correctly. *Attenuation* is the reduction in power of the light signal as it is transmitted. Attenuation is caused by passive media components such as cables, cable splices, and connectors. Although attenuation is significantly lower for optical fiber than for other media, it still occurs in both multimode and single-mode transmission. An efficient optical data link must have enough light available to overcome attenuation.

Dispersion is the spreading of the signal over time. The following two types of dispersion can affect an optical data link:

- Chromatic dispersion—Spreading of the signal over time, resulting from the different speeds of light rays.
- Modal dispersion—Spreading of the signal over time, resulting from the different propagation modes in the fiber.

For multimode transmission, modal dispersion—rather than chromatic dispersion or attenuation—usually limits the maximum bit rate and link length. For single-mode transmission, modal dispersion is not a factor. However, at higher bit rates and over longer distances, chromatic dispersion rather than modal dispersion limits maximum link length.

An efficient optical data link must have enough light to exceed the minimum power that the receiver requires to operate within its specifications. In addition, the total dispersion must be less than the limits specified for the type of link in Telcordia Technologies document GR-253-CORE (Section 4.3) and International Telecommunications Union (ITU) document G.957.

When chromatic dispersion is at the maximum allowed, its effect can be considered as a power penalty in the power budget. The optical power budget must allow for the sum of component attenuation, power penalties (including those from dispersion), and a safety margin for unexpected losses.

Calculate Power Budget and Power Margin for Fiber-Optic Cables

IN THIS SECTION

Use the information in this topic and the specifications for your optical interface to calculate the power budget and power margin for fiber-optic cables.

TIP: You can use the Hardware Compatibility Tool page to find information about the pluggable transceivers supported on your Juniper Networks device.

To calculate the power budget and power margin, perform the following tasks:

Calculate Power Budget for Fiber-Optic Cables

To ensure that fiber-optic connections have sufficient power for correct operation, you need to calculate the link's power budget (P_B), which is the maximum amount of power it can transmit. When you calculate the power budget, you use a worst-case analysis to provide a margin of error, even though all the parts of an actual system do not operate at the worst-case levels. To calculate the worst-case estimate of P_B, you assume minimum transmitter power (P_T) and minimum receiver sensitivity (P_R):

$$P_B = P_T - P_R$$

The following hypothetical power budget equation uses values measured in decibels (dB) and decibels referred to one milliwatt (dBm):

$$P_B = P_T - P_R$$

$$P_B = -15 \text{ dBm} - (-28 \text{ dBm})$$

$$P_B = 13 \text{ dB}$$

How to Calculate Power Margin for Fiber-Optic Cables

After calculating a link's P_B, you can calculate the power margin (P_M), which represents the amount of power available after subtracting attenuation or link loss (LL) from the P_B. A worst-case estimate of P_M assumes maximum LL:

$P_M = P_B - LL$

P_M greater than zero indicates that the power budget is sufficient to operate the receiver.

Factors that can cause link loss include higher-order mode losses, modal and chromatic dispersion, connectors, splices, and fiber attenuation. Table 22 on page 56 lists an estimated amount of loss for the factors used in the following sample calculations. For information about the actual amount of signal loss caused by equipment and other factors, refer to vendor documentation.

Table 22: Estimated Values for Factors Causing Link Loss

Link-Loss Factor	Estimated Link-Loss Value
Higher-order mode losses	Single mode—None Multimode—0.5 dB
Modal and chromatic dispersion	Single mode—None Multimode—None, if product of bandwidth and distance is less than 500 MHz-km
Faulty connector	0.5 dB
Splice	0.5 dB
Fiber attenuation	Single mode—0.5 dB/km Multimode—1 dB/km

The following sample calculation for a 2-km-long multimode link with a P_B of 13 dB uses the estimated values from Table 22 on page 56. This example calculates LL as the sum of fiber attenuation (2 km @ 1 dB/km, or 2 dB) and loss for five connectors (0.5 dB per connector, or 2.5 dB) and two splices (0.5 dB per splice, or 1 dB) as well as higher-order mode losses (0.5 dB). The P_M is calculated as follows:

$P_M = P_B - LL$

$P_M = 13 \text{ dB} - 2 \text{ km } (1 \text{ dB/km}) - 5 \ (0.5 \text{ dB}) - 2 \ (0.5 \text{ dB}) - 0.5 \text{ dB}$

$P_M = 13 \text{ dB} - 2 \text{ dB} - 2.5 \text{ dB} - 1 \text{ dB} - 0.5 \text{ dB}$

$P_M = 7 \text{ dB}$

The following sample calculation for an 8-km-long single-mode link with a P_B of 13 dB uses the estimated values from Table 22 on page 56. This example calculates LL as the sum of fiber attenuation (8 km @ 0.5 dB/km, or 4 dB) and loss for seven connectors (0.5 dB per connector, or 3.5 dB). The P_M is calculated as follows:

$P_M = P_B - LL$

$P_M = 13\ dB - 8\ km\ (0.5\ dB/km) - 7(0.5\ dB)$

$P_M = 13\ dB - 4\ dB - 3.5\ dB$

$P_M = 5.5\ dB$

In both the examples, the calculated P_M is greater than zero, indicating that the link has sufficient power for transmission and does not exceed the maximum receiver input power.

4

CHAPTER

Initial Installation and Configuration

IN THIS CHAPTER

SRX4700 Firewall Installation Overview

To install and configure your device:

1. Follow instructions in "Unpack the SRX4700" on page 59.
2. Install the firewall as described in "Install the SRX4700 in a Rack" on page 61.
3. Connect cables to external devices as described in "Connect SRX4700 to External Devices" on page 71.
4. Connect the grounding cable and power supplies as described in "Connect SRX4700 to Power" on page 73. Power on the device.
5. Perform initial configuration by following the instructions in "Configure Junos OS on the SRX4700" on page 83.

Unpack the SRX4700

SUMMARY

Unpack the firewall using the recommended tools and following the recommended procedure.

IN THIS SECTION

Tools and Parts Required to Unpack the SRX4700 Firewall

To unpack the SRX4700 and prepare for installation, you need the following tools:

- Phillips (+) screwdriver, number 2
- A box cutter or packing knife to slice open the tape that seals the boxes

Unpack an SRX4700

We ship the SRX4700 in a cardboard carton and secure it with foam packing material.

> **NOTE**: The SRX4700 has maximum protection inside the cardboard carton. Do not unpack it until you are ready to begin installation.

To unpack the SRX4700:

1. Move the cardboard carton to a staging area as close to the installation site as possible. Make sure that 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 SRX4700.
5. Verify the parts received against the list in Table 23 on page 60.
6. Store the brackets and bolts inside the accessory box.
7. Save the shipping carton and packing materials in case you need to move or ship the firewall at a later time.

Verify Parts Received with the SRX4700

The shipment includes a packing list. Check the parts you receive in the shipping carton against the items on the packing list. We ship the parts as per the configuration you order.

If any part on the packing list is missing, contact your customer service representative or contact Juniper customer care from within the U.S. or Canada by telephone at 1-888-314-5822. For international-dial or direct-dial options in countries without toll-free numbers, see https://www.juniper.net/support/requesting-support.html.

Table 23: Parts List for the SRX4700

Component	Quality
SRX4700 chassis Part number: SRX4700-CHAS	1
Power supply unit (PSU)	2 AC or 2 DC

Table 23: Parts List for the SRX4700 *(Continued)*

Component	Quality
Fan	6
Power cord that is appropriate for your geographical location	2 AC (only for AC models)
Rack mount kit	1
Documentation Roadmap	1

Install the SRX4700 in a Rack

SUMMARY

Mount the SRX4700 on a rack by following the recommended procedures that are appropriate for your site.

IN THIS SECTION

You can mount the SRX4700 on a four-post rack or in a cabinet. Use the toolless rack mount kit shipped with the device.

Complete these prerequisites before you mount the device:

- Prepare the site for installation as described in "Site Guidelines and Requirements for SRX4700" on page 38.
- Be sure the site has adequate clearance for both airflow and hardware maintenance, as described in "Clearance Requirements for Airflow and Hardware Maintenance for SRX4700" on page 48.
- Unpack the device as described in "Unpack the SRX4700" on page 59.

NOTE: Ensure that you support the rear of the chassis throughout the process of mounting the appliance on the rack.

CAUTION: A qualified technician must verify that the rack or cabinet is strong enough to support the device's weight before mounting the device. Have the technician verify also that the rack or cabinet has adequate support at the installation site.

CAUTION: If you are installing more than one device on a rack or in a cabinet, install the first device at the bottom of the rack.

Mount your Device by Using the JNP-4P-TL-1RU-RMK Rack Mount Kit on a Square Hole 4-Post Rack

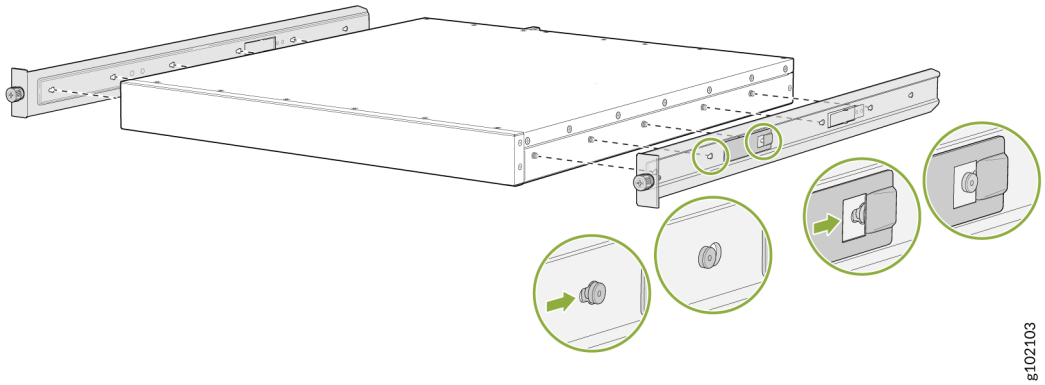
Ensure that you have the following tools and parts available:

- An ESD grounding strap—not provided.
- A pair of side mounting brackets that attach to the chassis—provided with the rack mount kit.
- A pair of front and rear mounting rails that attach to the rack posts—provided with the rack mount kit.

To mount the device on a four-post rack:

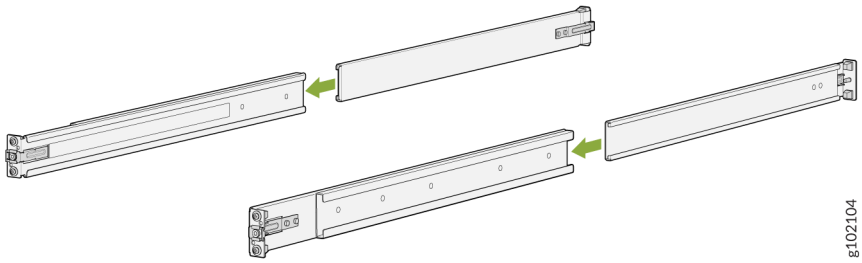
1. Review the General Safety Guidelines and Warnings.
2. Wrap and fasten one end of the electrostatic discharge (ESD) cable grounding strap around your bare wrist, and connect the other end to a site ESD point.
3. To attach the side mounting brackets to the chassis, align the keyholes on the mounting brackets over the shoulder screws on the chassis. Slide the mounting brackets toward the rear of the chassis so that the shoulder screws get locked in place.

Figure 9: Attach the Side Mounting Brackets



4. Assemble the mounting rails by sliding the rear mounting rails into the front rails.

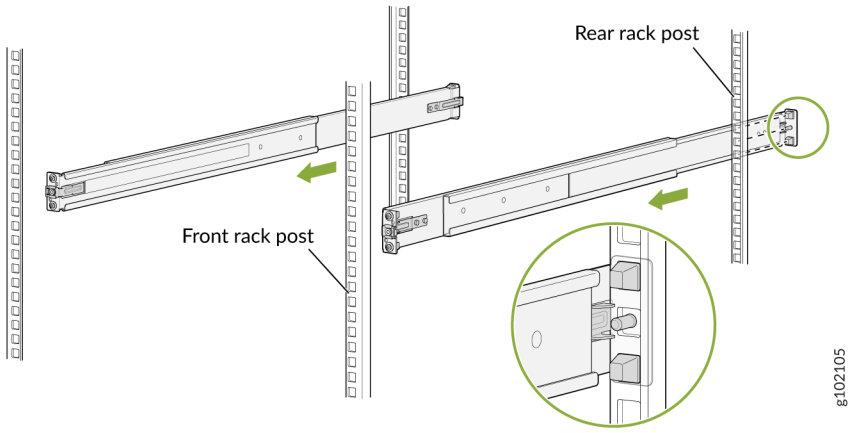
Figure 10: Assemble the Mounting Rails



5. Install the mounting rails on the rack:

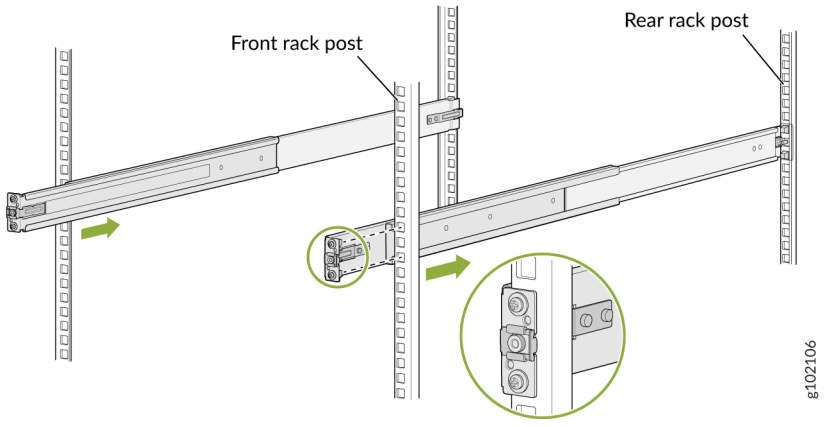
   a. Align the guide blocks of the rear mounting rails with the rear-post holes. Pull the rear mounting rails toward the front of the rack to lock the rails in place. You will hear a distinct click sound when the latch locks into the corresponding rack holes.

Figure 11: Install the Rear Mounting Rails



b. Align the guide blocks of the front mounting rails with the front-post holes. Push the front mounting rails toward the rear of the rack to lock the rails in place. You will hear a distinct click sound when the latch locks into the corresponding rack holes.

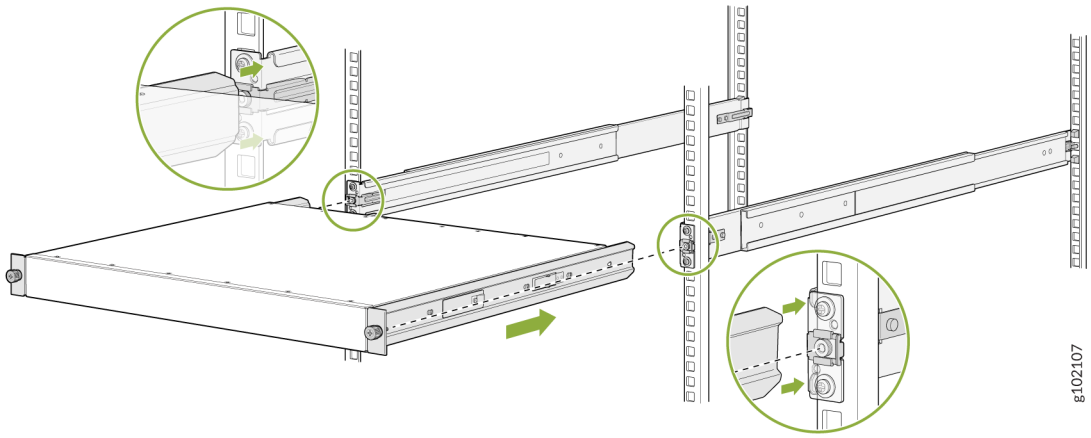
Figure 12: Install the Front Mounting Rails



c. Visually ensure that the front and rear latches are locked into place on the mounting rails. The mounting rails should be securely installed on the rack.

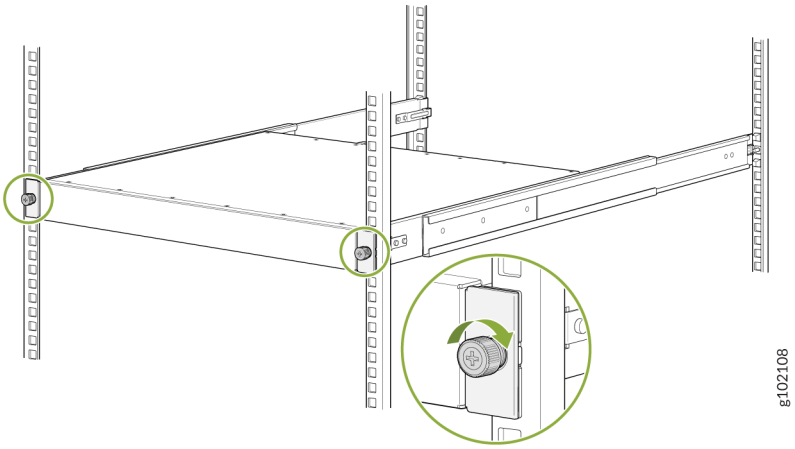
6. Lift the device and position it in the rack, aligning the side mounting brackets with the mounting rails. Slide the device into the channels of the rack mounting rails.

Figure 13: Slide the Device into the Rack



7. Tighten the two thumbscrews to secure the device.

Figure 14: Tighten the Thumbscrews



Mount your Device by Using the JNP-4P-TL-1RU-RMK Rack Mount Kit on a Threaded-Hole 4-Post Rack

Ensure that you have the following tools and parts available:

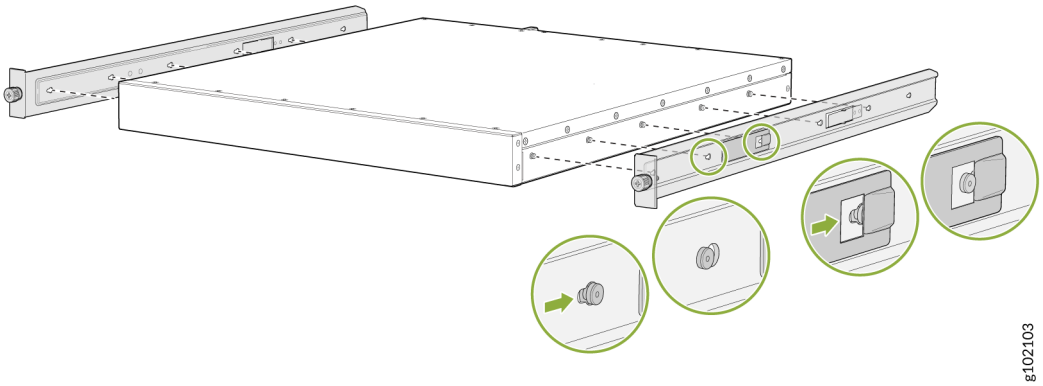
- An ESD grounding strap—not provided.
- A Phillips (+) screwdriver, number 2—not provided.

- Eight screws to attach the mounting rails to the rack posts—not provided.
- A pair of side mounting brackets that attach to the chassis—provided with the rack mount kit.
- A pair of mounting front and rear rails that attach to the rack posts—provided with the rack mount kit.

To mount the device on a four-post rack with threaded holes:

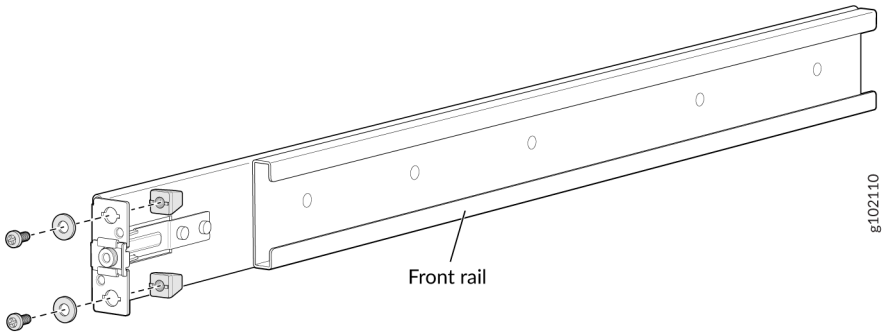
1. Review the General Safety Guidelines and Warnings.
2. Wrap and fasten one end of the electrostatic discharge (ESD) cable grounding strap around your bare wrist, and connect the other end to a site ESD point.
3. To attach the side mounting brackets to the chassis, align the keyholes on the mounting brackets over the shoulder screws on the chassis. Slide the mounting brackets toward the rear of the chassis so that the shoulder screws get locked in place.

Figure 15: Attach the Side Mounting Brackets



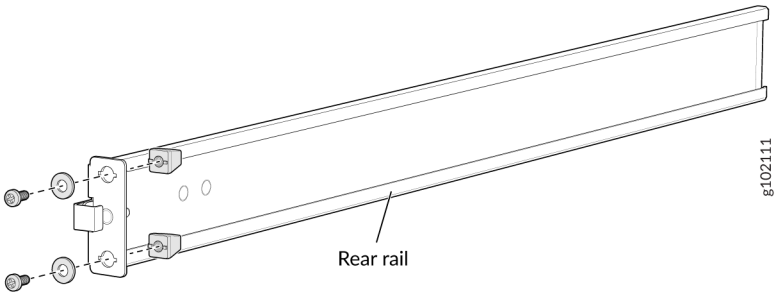
4. Assemble the mounting rails:
   a. Remove the guide blocks from the front mounting rails by loosening the screws and washers.

Figure 16: Removing the Guide Blocks from the Front Mounting Rail



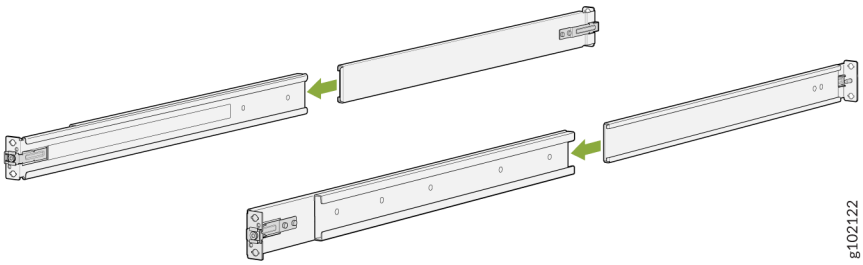
b. Remove the guide blocks from the rear mounting rail by loosening the screws and washers.

Figure 17: Removing the Guide Blocks from the Rear Mounting Rail



c. Slide the rear mounting rails into the front rails.

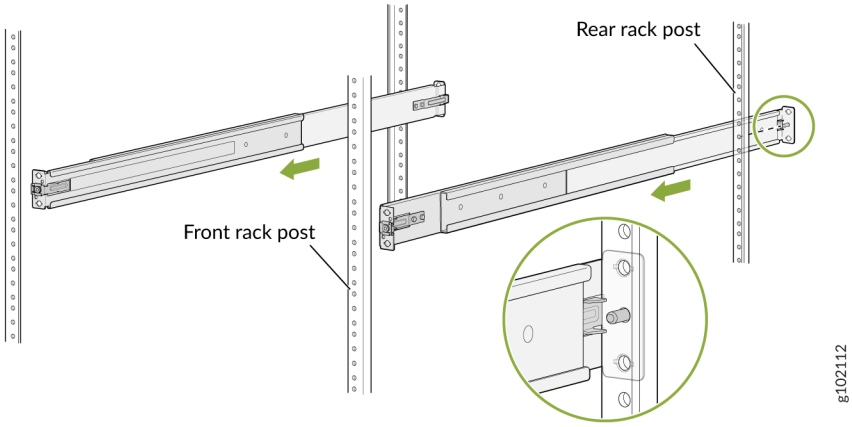
Figure 18: Assemble the Mounting Rails



5. Install the mounting rails on the rack:

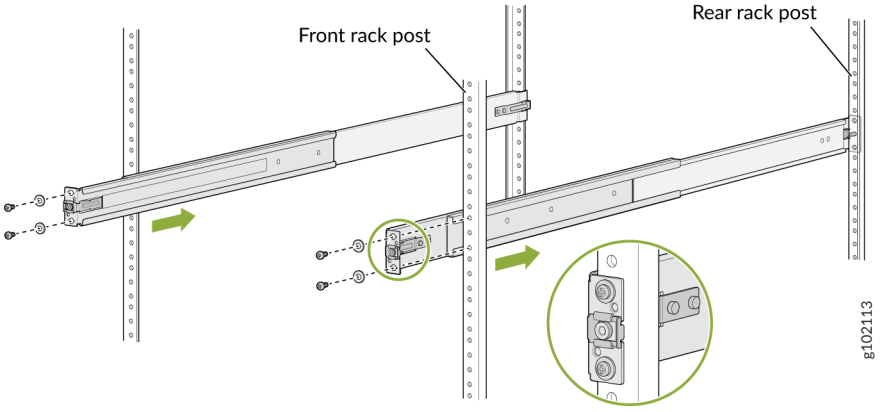
a. Insert the guide pin of the rear mounting rails into the rear-post holes. Pull the rear mounting rails toward the front of the rack to lock the rails in place. You will hear a distinct click sound when the latch locks into place.

Figure 19: Install the Rear Mounting Rails



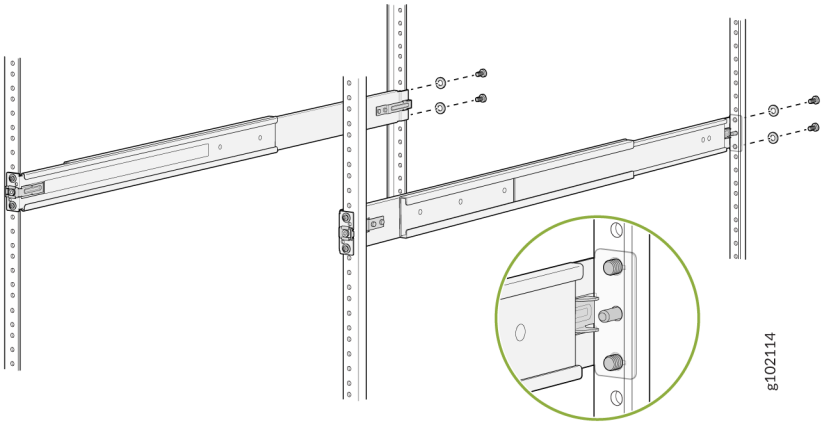
b. Insert the guide pin of the front mounting rails into the front-post holes. Push the front mounting rails toward the rear of the rack to lock the rails in place. You will hear a distinct click sound when the latch locks into place. Secure the front mounting rails to the front rack post by using screws appropriate for your rack threaded size (not provided).

Figure 20: Install and Secure the Front Mounting Rails



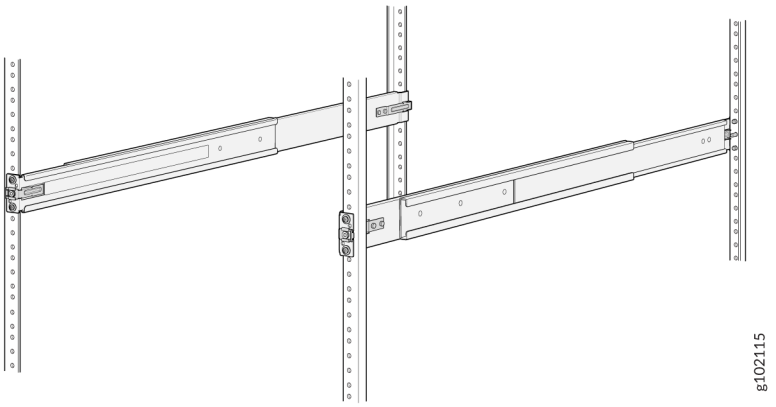
c. Secure the rear mounting rails to the rear rack post by using screws appropriate for your rack threaded size (not provided).

Figure 21: Secure the Rear Mounting Brackets



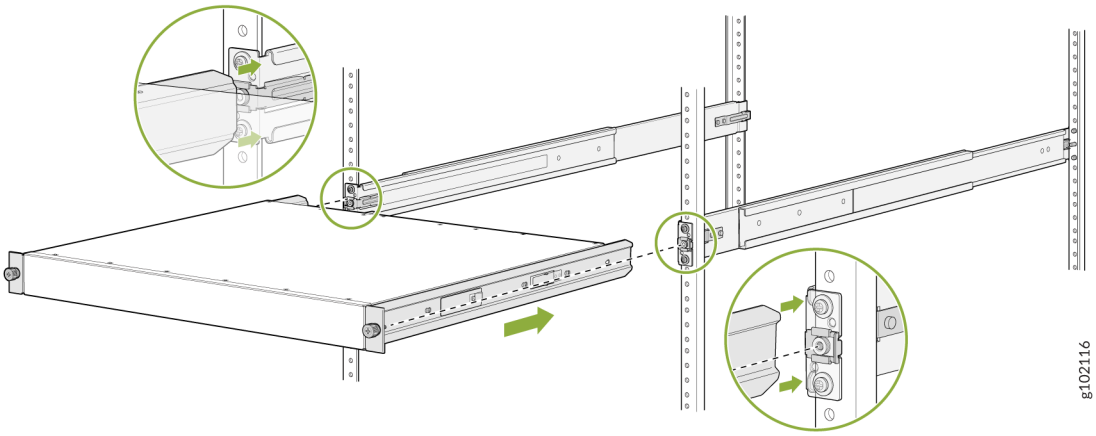
d. Visually ensure that the front and rear latches are locked into place on the mounting rails. The mounting rails should be securely installed on the rack.

Figure 22: Mounting Rails Installed and Secured



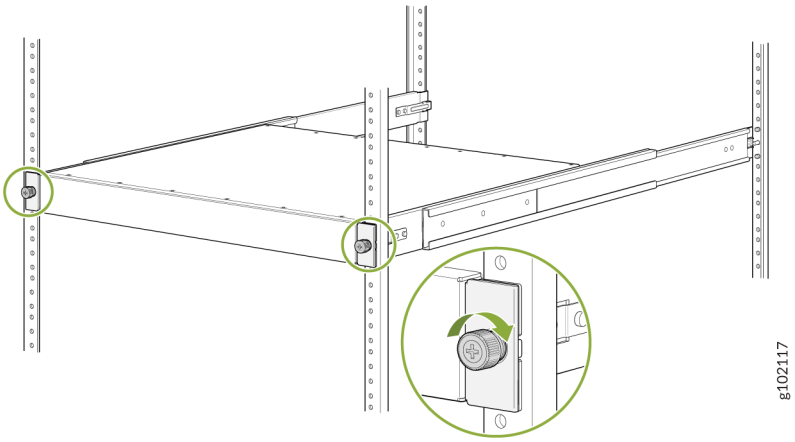
6. Lift the device and position it in the rack, aligning the side mounting brackets with the mounting rails. Slide the device into the channels of the rack mounting rails.

Figure 23: Slide the Device into the Rack



7. Tighten the two thumbscrews to secure the device.

Figure 24: Tighten the Thumbscrews



Connect SRX4700 to External Devices

IN THIS SECTION

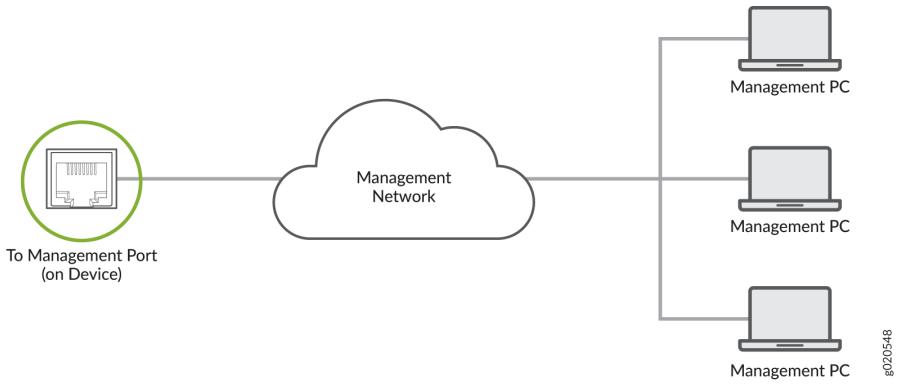
Connect the SRX4700 to a Network for Out-of-Band Management

Ensure that you have an Ethernet cable that has an RJ-45 connector at each end.

To connect a device to a network for out-of-band management:

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

Figure 25: Connecting Your Device to a Network for Out-of-Band Management



Connect the SRX4700 to a Management Console Using an RJ-45 Connector

Ensure that you have an Ethernet cable that has an RJ-45 connector at either end. You will also need the appropriate adapter (not provided) depending upon your console server or management console.

You can order the following separately from Juniper:

- 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)

NOTE: If you want to use the 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.

To connect the device to a management console:

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. Connect one end of the Ethernet cable to the console port on the device.
3. Connect the other end of the cable to the console server.

Figure 26: Connecting Your Device to a Management Console through a Console Server

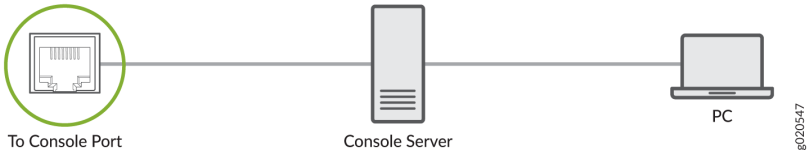


Figure 27: Connecting the Your Device directly to a Management Console

Connect SRX4700 to Power

SUMMARY

This section takes you through numerous steps and safety precautions to be followed while connecting power to the SRX4700, to prevent equipment damage and personal injury.

IN THIS SECTION

NOTE: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the SRX4700 to an earth ground before you connect it to power.

Tools and Parts Required to Ground and Connect the SRX4700 to Power

To ground and to provide power to the firewall, you need the following tools and parts:

- Phillips (+) screwdrivers, Number 1 and Number 2
- A socket nutdriver
- A 2.5-mm flat-blade (–) screwdriver

- A torque-controlled driver, with a maximum torque capacity of 23 lbf-in. (2.6 Nm) to 25 lbf-in. (2.8 Nm) for tightening screws to terminals on each power supply unit (PSU) on a DC-powered firewall.

  CAUTION: The maximum torque rating of the terminal screws on the DC power supply is 23 lbf-in. (2.6 Nm) through 25 lbf-in. (2.8 Nm). If you apply excessive torque, you might damage the terminal screws. Use only a torque-controlled driver to tighten screws on the DC power supply terminals. Use an appropriately sized driver, with a maximum torque capacity of 6 lb-in. (0.6 Nm) or less. Ensure that the driver is undamaged and properly calibrated and that you have been trained in its use. You might want to use a driver that is designed to prevent overtorque when the preset torque level is achieved.

- Electrostatic discharge (ESD) grounding wrist strap.

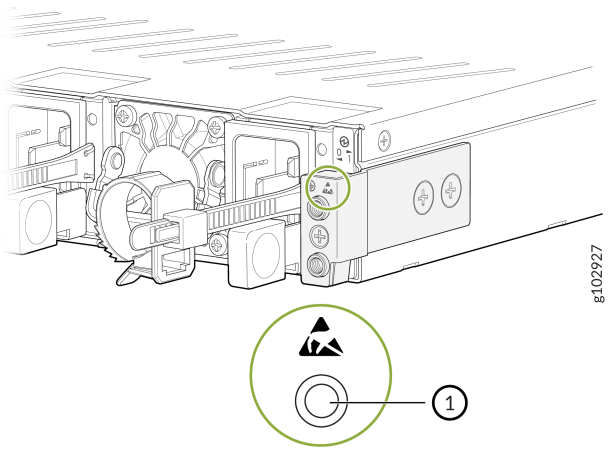
Connect Earth Ground to the SRX4700

To ground the SRX4700 Firewall:

Ensure that you have the following parts and tools available:

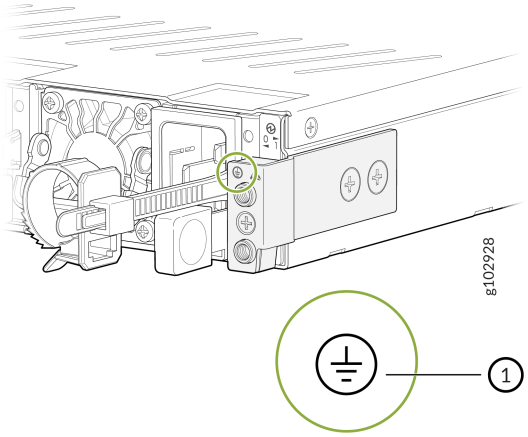
- Grounding cable for your firewall (not provided)—The grounding cable must be 6 AWG (13 mm^2), minimum 90° C wire, or as permitted by the local code.
- Grounding lug for your grounding cable (not provided)—The grounding lug required is a Panduit LCD6-14AF-L or equivalent.
- Two pan head M5 x10 mm screws with integrated split washers (not provided)—The screws and washers are used to secure the grounding lug to the protective earthing terminal.

1. Wrap and fasten one end of the electrostatic discharge (ESD) cable grounding strap around your bare wrist, and connect the other end to a site ESD point or to the ESD point on your firewall.



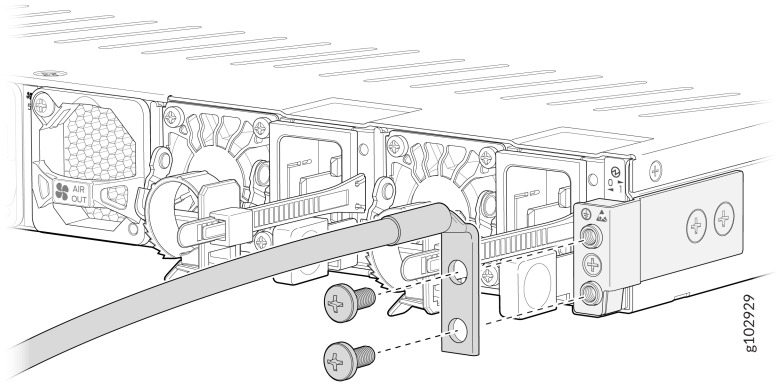
1	Chassis ESD Point

2. Connect the grounding cable to a proper earth ground, such as the rack in which you will mount the firewall.
3. Place the grounding cable terminal attached to the grounding cable over the grounding point.



1	Chassis grounding point

4. Secure the grounding cable terminal to the grounding point using the M5 screws.



5. Dress the grounding cable. Ensure that the cable doesn't block access to or come in contact with other firewall components, and that it doesn't drape where people could trip over it.

Connect AC Power to the SRX4700

The AC PSUs in an SRX4700 are hot-removable and hot-insertable field-replaceable units (FRUs). You can remove and replace the AC PSUs without powering off the firewall or disrupting its functions.

CAUTION: You must not mix AC and DC PSUs in the same chassis.

Before you begin to connect AC power to the firewall:

- Ensure that you have connected the chassis to an earth ground.

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

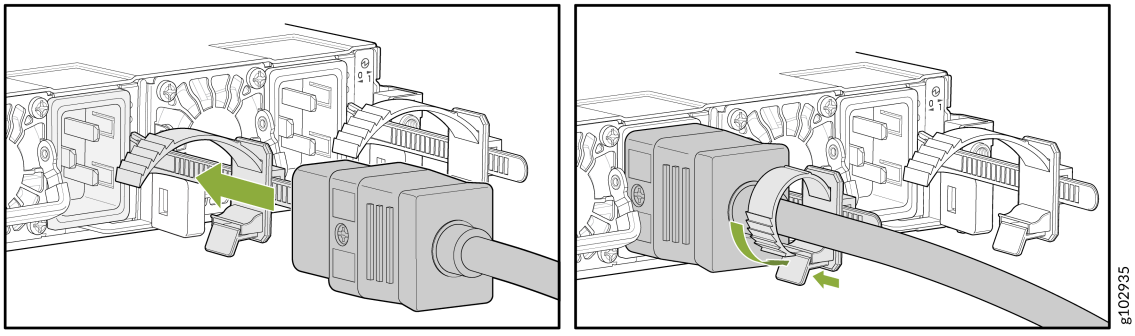
  To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the chassis to an earth ground before you connect it to power. For installations that require a separate grounding conductor to the chassis, use the protective earthing terminal on the firewall chassis to connect to the earth ground. The firewall gains additional grounding when you plug the PSU in the firewall to a grounded AC power outlet. Use the AC power cord appropriate for your geographical location.

- Ensure that you have a power cord appropriate for your geographical location available to connect AC power to the firewall.

- Read AC Power Electrical Safety Guidelines and Action to Take After an Electrical Accident.
- Ensure that you have taken the necessary precautions to prevent electrostatic discharge (ESD) damage.
- Ensure that you have an ESD grounding strap.
- If not already installed, install the PSUs in the firewall.

To connect AC power to an SRX4700:

1. Wrap and fasten one end of the ESD wrist strap around your bare wrist, and connect the other end of the strap to the ESD point on the firewall.
2. Locate the AC power cords shipped with the SRX4700; the cords have plugs appropriate for your geographical location. See "Supported AC Power Cords" on page 29.
3. Insert the coupler end of the power cord into the AC power cord inlet on the AC power supply faceplate.
4. Push the retainer clip through the loop and tighten it until it fits snug around the power cord.



5. Repeat step 3 and step 4 to insert the second power cord.
6. If the AC power source outlet has a power switch, set it to the off (O) position.
7. Insert the power cord plug into an AC power source outlet.

NOTE: Each PSU must be connected to a dedicated AC power feed and a dedicated customer-site circuit breaker. We recommend that you use a dedicated customer-site circuit breaker rated for 16 A (250 VAC) minimum, or as required by local code.

WARNING: The firewall is a pluggable type A equipment installed in a restricted-access location. It has a separate protective earthing terminal (sized for M6 hex screws) provided on the chassis in addition to the grounding pin of the power supply cord. This separate protective earthing terminal must be permanently connected to earth.

8. Route the power cord appropriately. Verify that the power cord does not block the air exhaust and access to firewall components or drape where people could trip on it.
9. If the AC power source outlet has a power switch, set it to the on (|) position.

Connect DC Power to the SRX4700

The DC power supply units (PSUs) in an SRX4700 are hot-removable and hot-insertable field-replaceable units (FRUs). You can remove and replace the DC PSUs without powering off the firewall or disrupting its functions.

CAUTION: You must not mix AC and DC PSUs in the same chassis.

Before you begin to connect DC power to the firewall:

- Ensure that you have connected the chassis to an earth ground.
- Ensure that you have the DC power cables and lugs to connect DC power to the firewall.
- Read Action to Take After an Electrical Accident.
- Ensure that you have taken the necessary precautions to prevent electrostatic discharge (ESD) damage.
- Ensure that you have an ESD grounding strap.
- If not already installed, install the power supplies in the firewall.

You connect DC power to the firewall by attaching power cables from the external DC power sources to the terminal studs on the power supply faceplates. You must provide the power cables and cable lugs (not supplied with the firewall). For power cable specifications, see "DC Power Cable Specifications" on page 35.

WARNING: Before you connect power to the firewall, a licensed electrician must attach appropriate cable terminals to the grounding and power cables that you use. A cable with an incorrectly attached terminal can damage the firewall (for example, by causing a short circuit).

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the chassis before connecting power. See "Connect Earth Ground to the SRX4700" on page 74 for instructions.

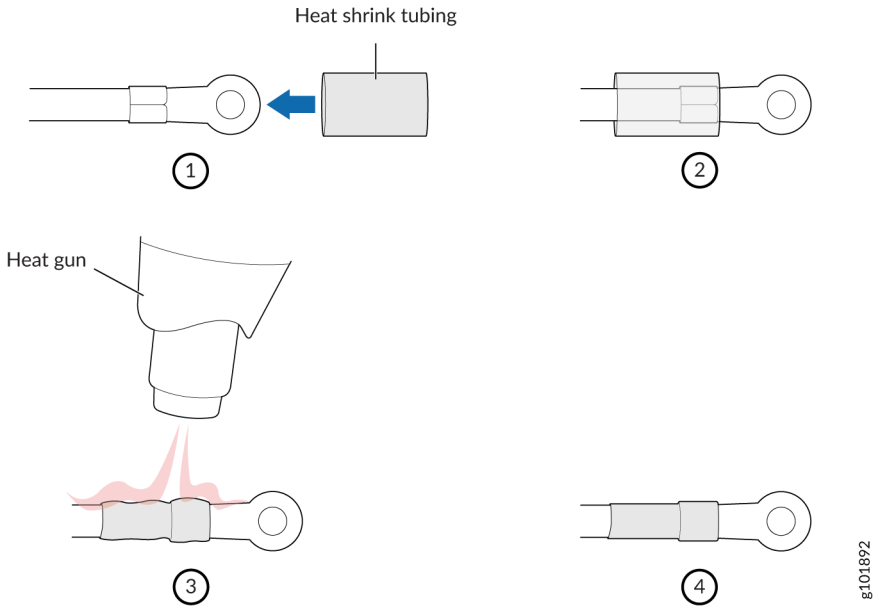
WARNING: Before performing the following procedure, ensure that you remove the power from the DC circuit. To ensure that all power is off, locate the circuit breaker on the panel board that services the DC circuit. Switch the circuit breaker to the OFF position (0), and tape the switch handle of the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

To connect the DC source power cables to the firewall for each PSU:

1. Switch off the dedicated facility circuit breakers. Ensure that the voltage across the DC power source cable leads is 0 V. You must ensure that the cable leads do not become active during installation.
2. Attach an ESD grounding strap to your bare wrist, and connect the other end of the strap to an ESD grounding point.
3. 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 terminal barrel. Ensure that the tubing covers the end of the wire and the barrel of the terminal 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: Make sure that you do not overheat the tubing.

Figure 28: Install Heat-Shrink Tubing

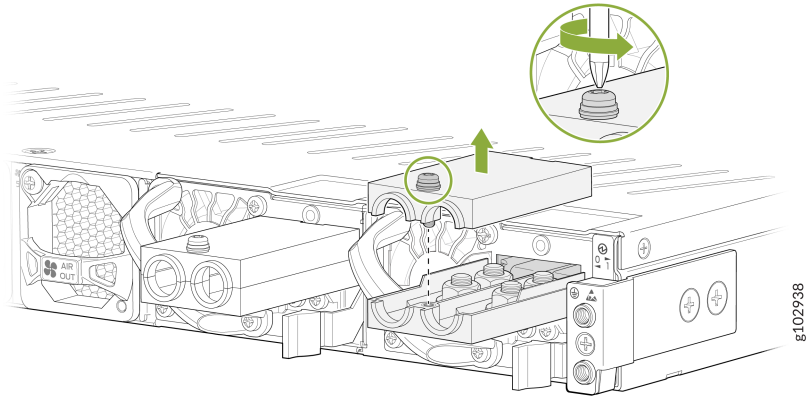


4. Verify that you have correctly labeled the DC power cables before making connections to the power supply.

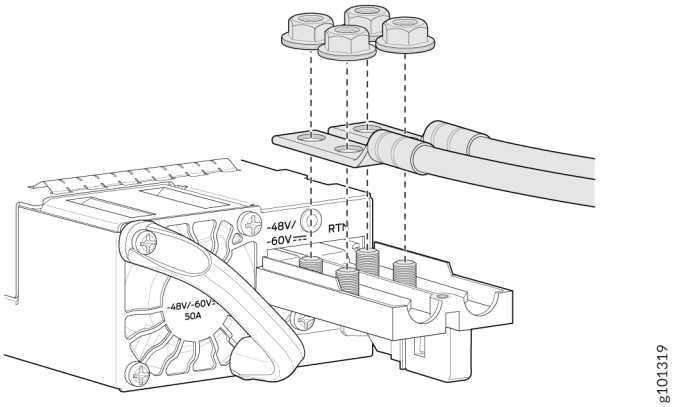
   In a typical power distribution scheme where the return is connected to chassis ground at the battery plant, you can use a multimeter to verify the ohm output of the —48 V and return (RTN) DC cables to chassis ground. The cable with very large resistance (indicating an open circuit) to chassis ground will be —48 V. 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. The DC power supply has two terminals labeled **—48 V/—60 V** (negative) and **RTN** (positive) for connecting the DC power cables labeled positive (+) and negative (—). The terminals are covered by a cover on the terminal block.
6. Using a screwdriver (anticlockwise), unscrew the nut on top of the terminal block.



7. Remove the nuts from the four terminals.
8. Secure each power cable lug to the terminals with the nuts. Tighten the nuts on the power supply terminals until snug by using the screwdriver. Apply between 23 lbf-in. (2.6 Nm) to and 25 lbf-in. (2.8 Nm) of torque to the nuts. Do not apply vertical force while tightening the screws. Do not overtighten the nuts. (Use a socket nutdriver.)



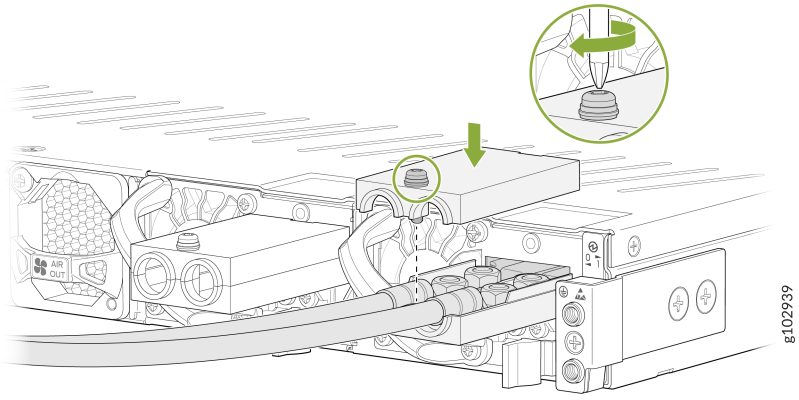
a. Secure the positive (+) DC source power cable lug to the **RTN** (return) terminal.

b. Secure the negative (–) DC source power cable lug to the **–48 V/–60 V** (input) terminal.

> **CAUTION**: Ensure that each power cable lug seats flush against the surface of the terminal block as you are tightening the nuts. Ensure that each nut is properly threaded into the terminal. Applying installation torque to the nuts when improperly threaded can result in damage to the terminal.

> **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.

9. Place the terminal block cover on and tighten the screw.



10. Verify that the power cables are connected correctly, that they do not touch or block access to firewall components, and that they do not drape where people could trip on them.
11. Switch the circuit breaker on the panel board that services the DC circuit to the ON (|) position.
12. Connect the power cables to the external DC power source. If the external DC power source has a switch, set it to the ON (|) position.

Power Off the SRX4700

For a graceful shutdown, press and hold the power button for atleast 4 seconds. The firewall begins gracefully shutting down the operating system (OS) and then powers itself off.

> **CAUTION**: Use the graceful shutdown method to power off or reboot the firewall.

To remove power completely from the firewall, unplug the AC power cord or DC power supply cable.

After powering off the device, wait at least 60 seconds before turning it back on. After powering on the device, wait at least 10 seconds before turning it off.

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

> **NOTE**: The fans in the PSU continue to rotate even after you power off the SRX4700 Firewall. To stop the fans, remove the power cord from the PSU. The fans will stop in a few seconds.

After turning on the power supply, it can take up to 60 seconds for status indicators—such as the **PWR** LED 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.

Configure Junos OS on the SRX4700

IN THIS SECTION

We ship the SRX4700 Firewall with preinstalled Junos OS, which is ready to be configured when you power on the device. You can use the J-Web GUI, Juniper® Mist, Juniper® Security Director (on-prem), Juniper® Security Director Cloud, Secure ZTP, or CLI to perform the initial configuration.

Configure the SRX4700 Using J-Web

The J-Web interface is a Web-based graphical interface that allows you to operate a firewall without commands.

Follow the instructions in Access the J-Web User Interface to how to start and access the J-Web user interface and The J-Web Setup Wizard to configure your device.

Configure the SRX4700 using Juniper Mist

You can configure and manage your device using the Mist cloud portal. If you have a Mist WAN Assurance license, follow the instructions in the Cloud-Ready SRX Series Firewalls with Mist.

If you don't have a license, use the CLI to configure your system.

Configure the SRX4700 using Juniper® Security Director Cloud

Juniper® Security Director Cloud is a cloud-based software-as-a-solution (SaaS) portal that helps you securely migrate your network to a Secure Access Service Edge (SASE) architecture.

Follow the instructions in the Juniper Security Director Cloud Quick Start guide to configure your device.

Configure the SRX4700 using Secure ZTP

Secure ZTP is highly automated, you can conveniently and securely set up and configure your device in your network with little manual work.

Follow the instructions in the Secure ZTP guide to configure your device.

Access the CLI on the SRX4700

To access the CLI on your device:

1. Connect the management device to the serial console port as described in "Connect the SRX4700 to a Management Console Using an RJ-45 Connector" on page 72.

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

> **NOTE**: After you have completed the initial configuration, you can connect your device to a network for out-of-band management as described in "Connect the SRX4700 to a Network for Out-of-Band Management" on page 71.

Configure Root Authentication and the Management Interface from the CLI

You must perform the initial configuration of the device through the console port.

Gather the following information before configuring the device:

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

To configure root authentication and the management interface:

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

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

3. Set the root authentication password. You can enter 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
```

Factory-Default Configuration of the SRX4700

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

- Two security zones are created: trust and untrust.
- 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.

View the Factory-Default Configuration of the SRX4700

To view the factory-default configuration of the firewall using the CLI:

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

```
root@srx4700>file list /etc/config
```

3. View the required default configuration file.

```
root@srx4700>file show /etc/config/config-file-name
```

5

CHAPTER

Maintain Components

IN THIS CHAPTER

Routine Maintenance Procedures for the SRX4700 Firewall

IN THIS SECTION

Purpose

For optimum firewall performance, perform preventive maintenance procedures regularly.

Action

- Inspect the installation site for moisture, loose wires or cables, and excessive dust.
- Make sure that airflow is unobstructed around the device and into the air intake vents.
- Check the status-reporting components on the front panel of the device—system alarms and LEDs.
- Periodically inspect the site to ensure that the grounding and power cables connected to the firewall are securely in place.

SRX4700 Cooling System Maintenance

SUMMARY

Maintaining the SRX4700 includes removing and installing the fan modules.

IN THIS SECTION

The SRX4700 has six independent, hot-removable and hot-insertable field-replaceable fan modules at the rear of the chassis.

For optimum cooling, verify the condition of the fan modules.

- Monitor the status of the fan modules. All the fan modules work in unison to cool the firewall. If one fan module fails, the redundant fan module acts as a backup. A major alarm is triggered when a fan fails, and a minor alarm and major alarm is triggered when a fan module is removed. We recommend that you replace the fan module immediately to maintain proper cooling.
- To display the status of the cooling system, issue the `show chassis environment` command.

You can remove and replace the fan modules without powering off the firewall or disrupting firewall functions.

Before you replace a fan module:

- Ensure that you understand how to prevent electrostatic discharge (ESD) damage.
- Ensure that you have the following parts and tools:
  - An ESD grounding strap
  - An antistatic bag or an antistatic mat
  - A replacement fan module
  - (Optional) A Phillips (+) screwdriver, Number 1 or Number 2, for loosening or tightening the screws.

You must replace the Fan modules within the duration mentioned in Table 24 on page 91.

Table 24: Replacement Duration for the Fan Module

Chassis Ambient Temperature	Duration
27 °C	5 minutes
35 °C	3 minutes
40 °C	2 minutes

Remove the Fan Module from the SRX4700

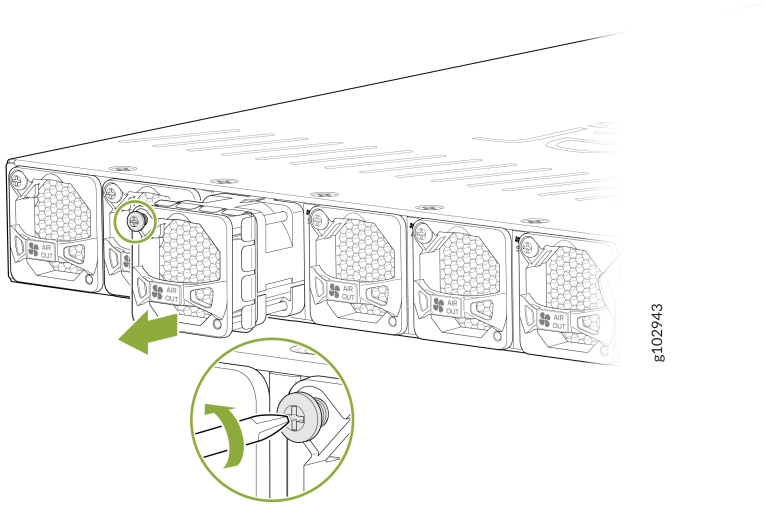
CAUTION: Do not remove a fan unless a replacement fan is available.

To remove a fan module:

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. Place the antistatic bag or the antistatic mat on a flat, stable surface.
3. Loosen the screw on the front faceplate of the fan module by using the screwdriver.

   WARNING: To prevent injury, do not touch the fan module with your hands or any tools when you slide the fan module out of the chassis—the fan module might still be running.

4. Grasp the handle on the fan module and pull it firmly to slide the it out of the chassis.

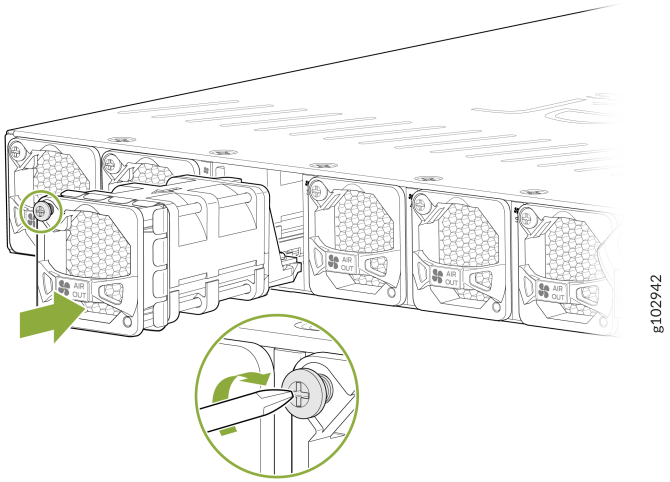


5. Place the fan module in the antistatic bag or on the antistatic mat.

Install the Fan Module in the SRX4700

To install a fan module:

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. Remove the fan module from its bag.
3. Hold the handle of the fan module with one hand and support the weight of the module with the other hand. Place the fan module in the fan module slot on the rear panel of the firewall and slide the module in until it is fully seated.
4. Tighten the screw on the faceplate of the fan module by using screw driver.



SRX4700 Power Supply Maintenance

SUMMARY

Maintaining an SRX4700 includes removing a failed power supply unit (PSU) and installing a functional PSU.

IN THIS SECTION

Maintain the Power Supplies

IN THIS SECTION

Purpose

For optimum firewall performance, verify the condition of the power supplies.

Action

On a regular basis check the power supply status:

- Issue the `show chassis power` CLI command.
- Arrange the power and grounding cables in a way so that they do not obstruct access to other firewall components.
- Routinely check the status LEDs on the power supply faceplates and the chassis LEDs to determine whether if the PSUs are functioning normally.
- Check the red and yellow alarm LEDs on the chassis LEDs. If a PSU fails or you remove a PSU, it triggers an alarm that causes one or both LEDs to light. To find out the associated error messages, issue the following command:

```
user@host> show chassis alarms
```

- Periodically inspect the site to ensure that the grounding and power cables connected to the firewall are securely in place and that there's no moisture accumulating near the firewall.

CAUTION: Do not mix AC and DC PSUs in the same chassis.

Replace an AC PSU on the SRX4700

IN THIS SECTION

The SRX4700 rear panel has two AC PSUs, which are hot-removable and hot-insertable field-replaceable units (FRUs). You can remove and replace the PSUs without powering off the SRX4700 or disrupting the firewall functions.

Ensure that you have the following parts and tools:

- An electrostatic discharge (ESD) grounding strap
- An antistatic bag or an antistatic mat
- A replacement AC PSU
- A blank cover panel (in case you're not replacing the component)

Remove an AC PSU from the SRX4700

Before you remove a PSU, be aware of the following:

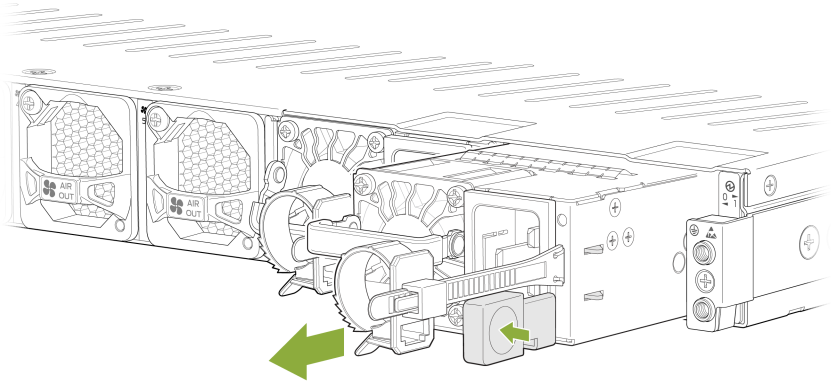
CAUTION: Avoid leaving the PSU slot empty for more than 30 minutes when the device is operational. For proper airflow, you must place the PSU in the chassis. Always cover the empty PSU slot with a blank panel.

NOTE: The minimum required number of PSUs must be present in the firewall at all times.

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

To remove an AC PSU:

1. Switch off the dedicated customer-site circuit breaker for the power supply, and remove the power cord from the AC power source. Follow the instructions for your site.
2. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
3. Loosen the retainer clip that is around the power cord.
4. Remove the power cord from the PSU.
5. Press the release latch on the right side of the AC PSU to disconnect the PSU from the chassis.

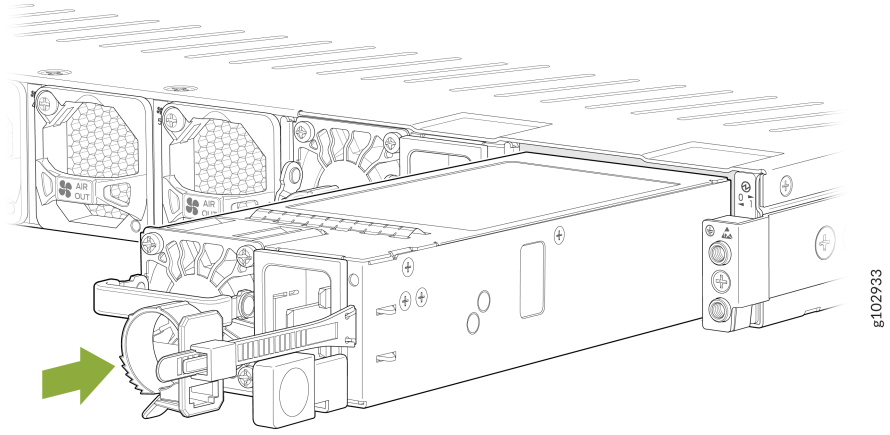


6. Pull the PSU straight out of the chassis.

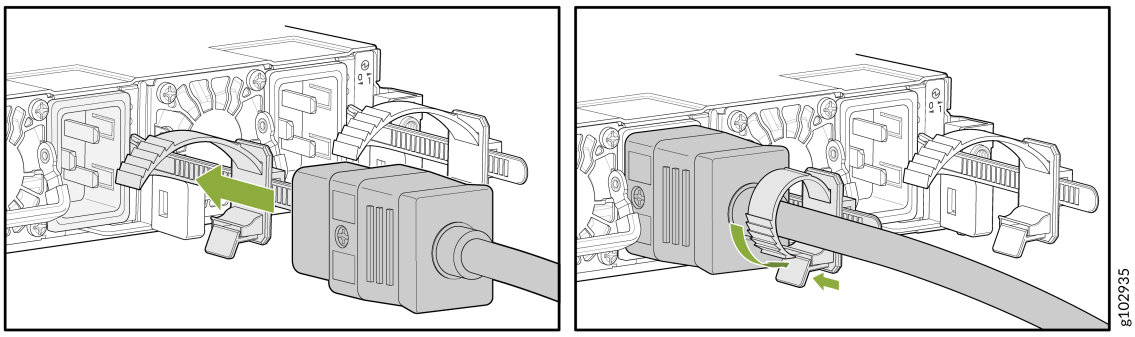
Install an AC PSU in the SRX4700

To install an AC PSU:

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. Using both hands, hold and slide the AC PSU straight into the chassis until the PSU is fully seated in the chassis slot.



3. Attach the power cord to the PSU.
4. Push the retainer clip through the loop and tighten it until it fits snug around the power cord.



5. Attach the power cord to the AC power source, and switch on the dedicated customer-site circuit breaker. Follow the instructions for your site.
6. Observe the status LED on the PSU faceplate. If the PSU is correctly installed and functioning normally, the status LED lights green steadily.

Replace a DC PSU on the SRX4700

IN THIS SECTION

The rear panel of the SRX4700 has two DC PSUs, which are hot-removable and hot-insertable field-replaceable units (FRUs). You can remove and replace the PSUs without powering off the SRX4700 or disrupting the firewall functions.

Ensure that you the following parts and tools are available:

- An ESD grounding strap
- Phillips (+) screwdriver, Number 1 and Number 2
- An antistatic bag or an antistatic mat
- A replacement DC PSU
- A blank cover panel (in case you're not replacing the component)

Remove a DC PSU from the SRX4700

Before you remove a PSU, be aware of the following:

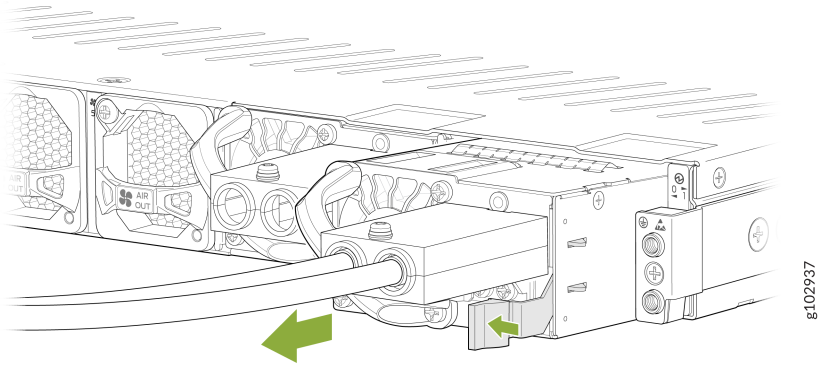
CAUTION: Avoid leaving the PSU slot empty for more than 30 minutes when the device is operational. For proper airflow, you must place the PSU in the chassis. Always cover the empty PSU slot with a blank panel.

NOTE: The minimum required number of PSUs must be present in the firewall at all times.

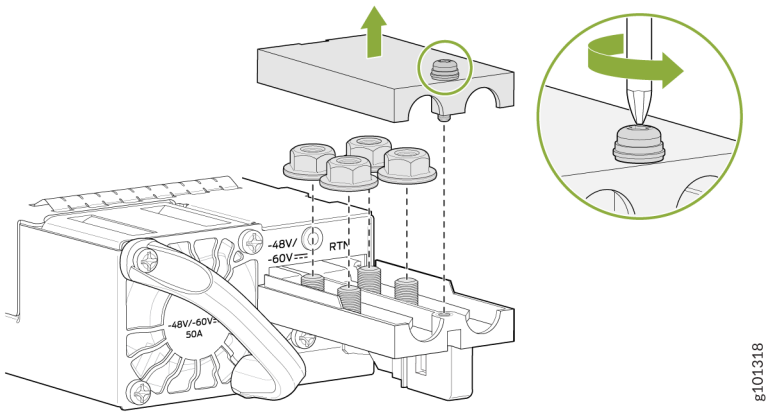
NOTE: After powering off a PSU, wait at least 60 seconds before turning it back on.

To remove a DC PSU from the firewall:

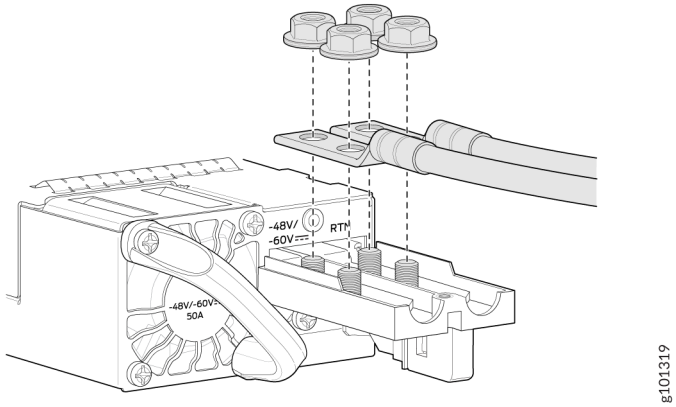
1. Switch off the dedicated customer-site circuit breaker for the PSU being removed. Follow your site's procedures for ESD.
2. Make sure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cables might become active during the removal process.
3. Verify that the status LED on the PSU is not lit.
4. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
5. Press the latch located on the right side of the DC PSU, to release it from the chassis.
6. Pull the PSU straight out of the chassis.



7. Using a screwdriver (anticlockwise), unscrew the nut on top of the terminal block and remove the terminal block cover.



8. Remove the nuts and cables from the four terminals.



9. Carefully move the power cables out of the way.
10. Place the terminal block cover on and tighten the screw.

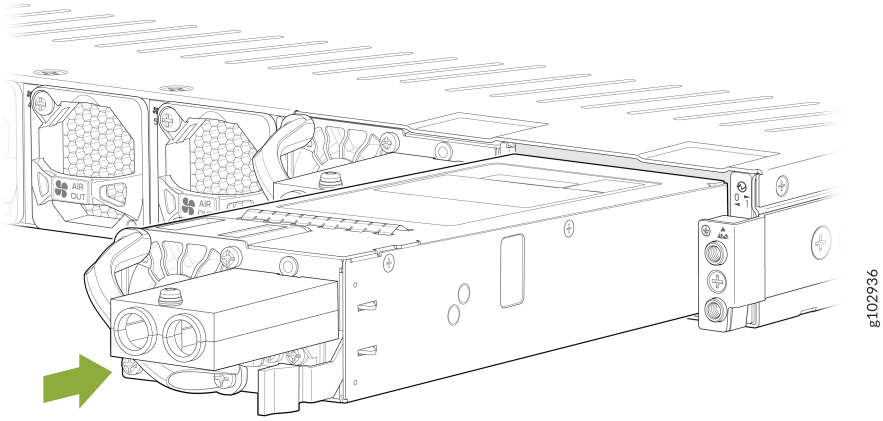
Install a DC PSU in the SRX4700

WARNING: Before you perform DC power procedures, ensure there is no power to 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.

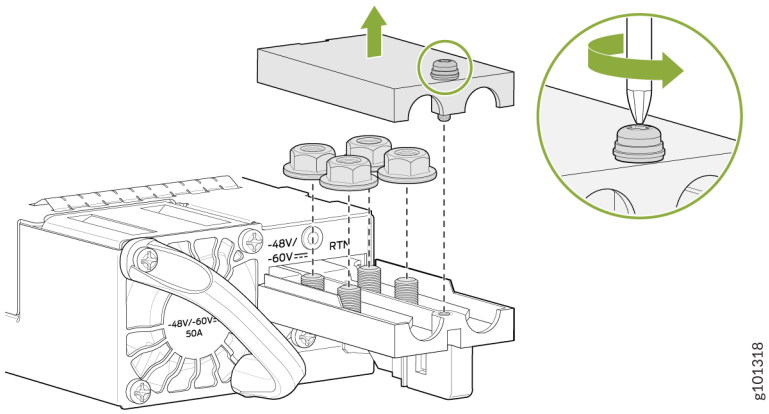
To install a DC PSU:

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.
2. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.

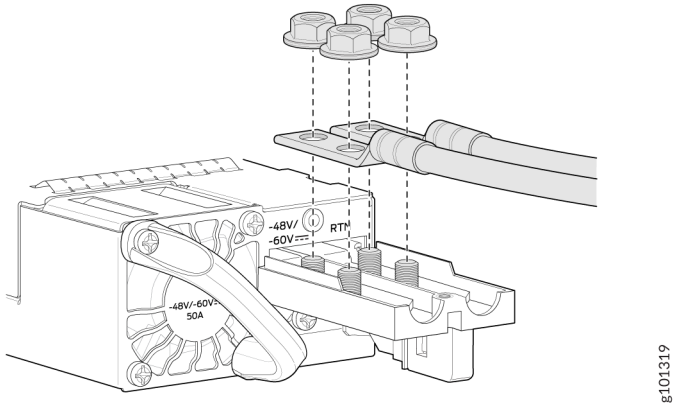
3. Using both hands, slide the DC PSU straight into the chassis until the PSU is fully seated in the chassis slot. The PSU faceplate must align with any adjacent PSU faceplate installed in the PSU slot.



4. Using a screwdriver (anticlockwise), unscrew the nut on top of the terminal block and remove the terminal block cover.
5. Remove the nuts from the four terminals.



6. Secure each power cable lug to the terminal with the nuts. Use the screwdriver to tighten the nuts on the PSU terminals until snug. Apply between 23 lbf-in. (2.6 Nm) to 25 lbf-in. (2.8 Nm) of torque to the nuts. Use a socket nutdriver to ensure you don't overtighten the nuts.



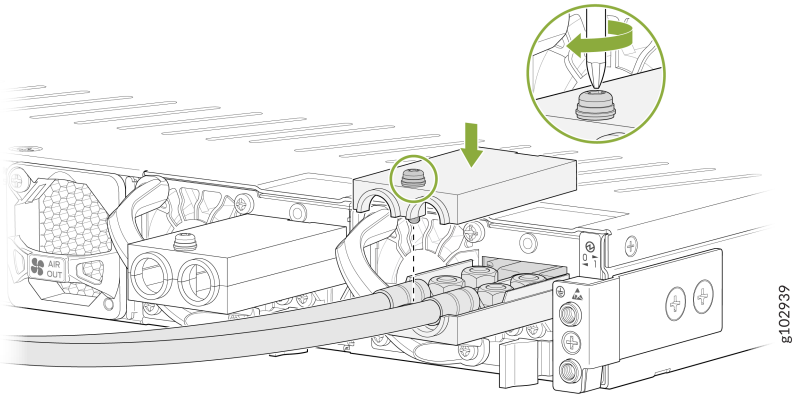
a. Secure the positive (+) DC source power cable lug to the **RTN** (return) terminal.

b. Secure the negative (–) DC source power cable lug to the **–48V/-60V** (input) terminal.

> **CAUTION**: Ensure that each power cable lug seats flush against the surface of the terminal block as you are tightening the nuts. Ensure that each nut is properly threaded into the terminal. Applying installation torque to the nuts when improperly threaded can result in damage to the terminal.

> **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.

7. Place the terminal block cover on and tighten the screw.



8. Verify that the power cables are connected correctly, that they are not touching or blocking access to firewall components, and that they do not drape where people could trip on them.
9. Close the input circuit breaker.
10. Connect the PSU to the power source.

SRX4700 SSD Maintenance

SUMMARY

This topic explains how to replace a solid state-drive (SSD) on your SRX4700 Firewall.

IN THIS SECTION

Replace an SRX4700 Firewall SSD

IN THIS SECTION

The two SSDs installed in the SRX4700 Firewall are field-replaceable units (FRUs). SSDs are not hot-swappable, so you need to power off the firewall to replace an SSD.

NOTE: You must install the **1T** SSD in slot **SSD0** (primary slot) and the **2T** SSD in slot **SSD1** (secondary slot).

Ensure that you have the following equipment available:

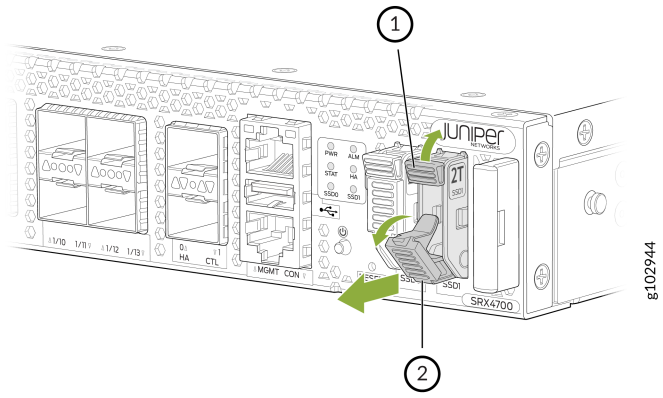
- Electrostatic discharge (ESD) grounding strap

- An antistatic bag or an antistatic mat
- SSD to replace

Remove an SSD from the SRX4700 Firewall

You need to power off the SRX4700 Firewall to remove an SSD.

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. Place the antistatic bag or the antistatic mat on a flat, stable surface.
3. Place your finger on the SSD front locker and press the front locker to unlock the SSD front stopper.



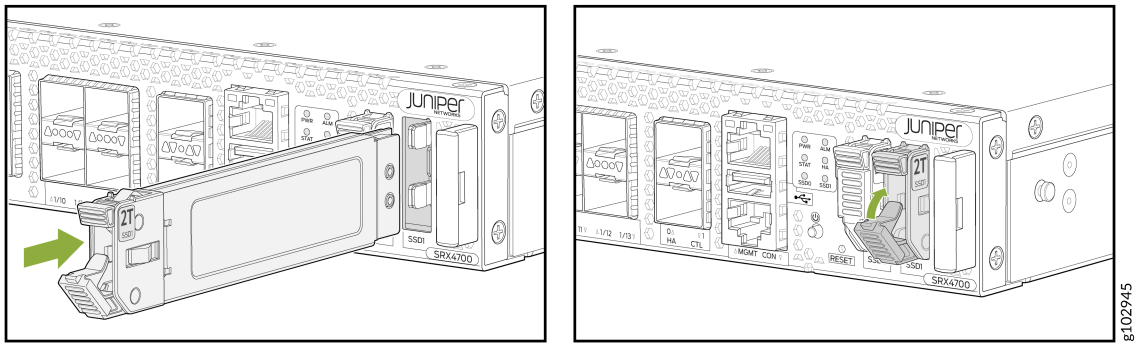
Callout	Component
1	SSD front locker
2	SSD front stopper

4. Pull the SSD firmly to slide it out of its slot.
5. Place the SSD in the antistatic bag or on the antistatic mat placed on a flat, stable surface.

Install an SSD in the SRX4700 Firewall

You need to power off the SRX4700 Firewall to install a SSD.

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. Slide the SSD gently into its slot until it is fully seated. Press the SSD front stopper to lock the SSD into its slot.



Replace the 1T SSD in the SRX4700 Firewall

You need to power off the SRX4700 Firewall to replace the **1T** SSD (primary SSD).

NOTE: **1T** SSD must be installed only in slot **SSD0**.

If **1T** SSD goes faulty or if the software image on it is corrupted, the firewall will boot from **2T** SSD (secondary SSD).

1. Issue the `request vmhost power-off` operational mode CLI command. This command shuts down the firewall gracefully. You can manually power off the firewall using the power button located on the front panel of the firewall.
2. Remove the **1T** SSD from slot **SSD0**. See, "Remove an SSD from the SRX4700 Firewall" on page 103.
3. Install the replacement **1T** SSD in slot **SSD0**. See, "Install an SSD in the SRX4700 Firewall" on page 103.
4. Power on the firewall using the power button located on the front panel of the firewall. Firewall will boot from **1T** SSD with the factory-default image and configuration installed on it.
5. **(Optional):** To synchronize the image and configuration from the **2T** SSD to the **1T** SSD:
   a. Issue the `request vmhost reboot disk2` CLI command. This command reboots the firewall from the **2T** SSD.
   b. Issue the `request vmhost snapshot recovery` CLI command. This command takes a snapshot from the **2T** SSD to the **1T** SSD.
   c. Issue the `request vmhost reboot disk1` CLI command. This command reboots the firewall from the **1T** SSD.
6. Issue the `show vmhost hardware` CLI command to verify the details of the SSDs.

Replace the 2T SSD in the SRX4700 Firewall

You need to power off the SRX4700 Firewall to replace the **2T** SSD (secondary SSD).

NOTE: **2T** SSD must be installed only in slot **SSD1**.

1. Issue the `request vmhost power-off` operational mode CLI command. This command shuts down the firewall gracefully. You can manually power off the firewall using the power button located on the front panel of the firewall.
2. Remove the **2T** SSD from the slot **SSD1**. See, "Remove an SSD from the SRX4700 Firewall" on page 103.
3. Install the replacement **2T** SSD in slot the **SSD1**. See, "Install an SSD in the SRX4700 Firewall" on page 103.
4. Power on the firewall using the power button located on the front panel of the firewall. Firewall boots from the **1T** SSD.
5. To synchronize the image and configuration from the **1T** SSD to the **2T** SSD, issue the `request vmhost snapshot` CLI command. This command takes a snapshot from the **1T** SSD to the **2T** SSD.
6. Issue the `show vmhost hardware` CLI command to verify the details of the SSDs.

Replace the 1T and 2T SSDs from the SRX4700 Firewall

You need to power off the SRX4700 Firewall to replace the SSDs.

NOTE: **1T** SSD must be installed only in slot **SSD0** and **2T** SSD only in slot **SSD1**.

1. Issue the `request vmhost power-off` operational mode CLI command. This command shuts down the firewall gracefully. You can manually power off the firewall using the power button located on the front panel of the firewall.
2. Remove the **1T** SSD from the slot **SSD0** and **2T** SSD from the slot **SSD1**. See, "Remove an SSD from the SRX4700 Firewall" on page 103.
3. Install the replacement **1T** SSD in slot **SSD0** and **2T** SSD in slot **SSD1**. See, "Install an SSD in the SRX4700 Firewall" on page 103.
4. Power on the firewall using the power button located on the front panel of the firewall. Firewall boots from **1T** SSD with factory default settings and configurations.
5. Issue the `show vmhost hardware` CLI command to verify the details of the SSDs.
6. If needed, upgrade your firewall with the desired Junos OS software. After the upgrade is complete and the firewall is up and running with the upgraded Junos OS software image and configurations, issue the `request vmhost snapshot` CLI command to take a snapshot from the **1T** SSD to the **2T** SSD.

CHAPTER 6

Troubleshoot Hardware

IN THIS CHAPTER

Troubleshoot the SRX4700

SUMMARY

Troubleshooting SRX4700 Firewalls includes recognizing alarm types and alarm severity classes and resolving the error conditions that trigger alarms.

IN THIS SECTION

SRX4700 Firewall Troubleshooting Resources

To troubleshoot a firewall, use the Junos OS CLI and LEDs on the chassis:

- LEDs—When the firewall detects an alarm condition, the status LED on the front panel glows red.
- 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.

Chassis Component Alarm Conditions on an SRX4700 Firewall

You can monitor chassis alarms through the **ALM** LED. When the firewall detects an alarm condition, the **ALM** LED on the front panel glows and the level of severity can be either major (steady red), minor

(yellow), or both major and minor (blinking red). To view a more detailed description of the alarm cause, issue the `show chassis alarms` and `show system alarm` commands.

Table 25: Alarms for Firewall Chassis Components

Component	Alarm Conditions	Action	Alarm Severity
Fan	At least one of the fans has failed.	• Check and adjust the room temperature, if possible. • Check the airflow and ensure that the airflow through the firewall is unobstructed. • Replace the failed fan module to avoid failure of the other fan modules. • Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Steady red (major)
	The firewall chassis temperature is too warm.	• Check the room temperature. • Check the airflow. • Run all fans at full speed. • Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Yellow (minor)/Red (major)

Table 25: Alarms for Firewall Chassis Components *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	Missing fan module	Install the missing fan module.	Red (major)
	Fan overspeeding	• Check whether the fan is spinning at a speed higher than the configured speed. • Replace the fan module as it is likely to fail.	Yellow (minor)
	Fan spinning below its speed	• Check whether the fan is spinning at a speed lower than the configured speed. • Replace the fan module as it is likely to fail.	Yellow (minor)
	Impeding fan failure	Replace the fan module.	Yellow (minor)
Power supply unit (PSU)	A PSU has failed.	Replace the PSU.	Steady red (major)
	A PSU is not present.	Install a PSU in the empty slot. The firewall requires two PSUs to be installed.	
	Power cord is not connected.	Verify and ensure that the power cord is connected properly.	
	PSU fan failure.	As this is a non-recoverable fault, replace the PSU.	Yellow (minor)

Table 25: Alarms for Firewall Chassis Components *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	Input voltage failure on the PSU	• Check whether the voltage of the power source is in the operating range. • Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Red (major)
	PSU drawing more current than it should	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Yellow (minor)
	Unrecognized PSU	Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Red (major)
	PSU not powered on.	Connect the PSU to the power source.	Red (major)

Table 25: Alarms for Firewall Chassis Components *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	PSU internal devices failure.	• Replace the PSU. • Open a support case using the Case Manager link at https://www.juniper.net/support/ or call 1-888-314-5822 (toll-free within the United States and Canada) or 1-408-745-9500 (from outside the United States).	Red (major)
	Mix of AC and DC PSUs installed.	Check whether all the PSUs installed are of the same type.	Yellow (minor)
SSD	SSD detection failure	• Check whether the SSD slot is receiving power. • Check whether the SSD initialization in BIOS is failing. • Replace the faulty SSD.	Yellow (minor)
	SSD runtime read/write fault	• Check whether there is any issue with the PCIe. • Check whether the SSD initialization is failing. • Faulty SSD. • Replace the faulty SSD.	Yellow (minor)

Table 25: Alarms for Firewall Chassis Components *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
	SSD file system corrupted	• Check whether there is any issue with the SSD subsystem. • Check whether power to the firewall was abruptly removed. • Check whether the firewall experienced non-graceful shutdown or reset.. • Recover or reimage the SSD.	Yellow (minor)
USB	USB device not detected	• Check whether the USB slot is receiving power. • Check for the port-level failures. • Check whether the USB is faulty, and replace it if it is faulty.	Yellow (minor)

Troubleshoot the SRX4700 Firewall Cooling System

IN THIS SECTION

Problem

Description

A single fan module or fan modules are not functioning normally.

Solution

Follow these guidelines to troubleshoot the fan modules:

- Check the LEDs on the fan module and alarm LEDs on the front panel of the firewall.
- If the alarm LED on the front panel of the firewall is lit, use the following CLI command to get information about the source of an alarm condition:
  `user@host> show chassis alarms`.

  If the CLI output lists only one fan failure, and the other fans are functioning normally, the fan is most likely faulty and you must replace the fan tray.

  If the fan tray is removed, a minor alarm or a major alarm is raised.
- Place your hand near the near the fan modules to determine whether the fans are pushing air out of the chassis.
- The following conditions automatically cause the fans to run at full speed and also trigger the indicated alarm:
  - A fan fails (major alarm).
  - The firewall temperature exceeds the “temperature warm” threshold (minor alarm).
  - The temperature of the firewall exceeds the maximum (“temperature hot”) threshold (major alarm and automatic shutdown of the power supplies).

Troubleshoot the SRX4700 Firewall Power System

IN THIS SECTION

Problem

Description

The power system is not functioning normally.

Solution

- Check the LEDs on each power supply unit (PSU) faceplate. If an AC PSU or a DC PSU is correctly installed and functioning normally, then the LEDs glow steadily.

  For more information about PSU LEDs, see "SRX4700 Power System" on page 25.

- Use the CLI **show chassis environment pem** command to check the status of the installed PSUs.

If a PSU is not functioning normally, perform the following tasks to diagnose and correct the problem:

- If a red-alarm condition occurs, use the **show chassis alarms** command to determine the source of the problem.

  NOTE: If the system temperature exceeds the red-alarm threshold, Junos OS shuts down all the PSUs so that no status is displayed.

  Junos OS also can shut down one of the PSUs for other reasons. In this case, the remaining PSUs provide power to the firewall, and you can still view the system status through the CLI or J-Web interface.

  NOTE: The firewall shuts down automatically if the device temperature exceeds the red-alarm threshold.

- Check that the AC input switch (—) or DC circuit breaker (|) is in the on position and that the PSU is receiving power.

- Verify that the source circuit breaker has the proper current rating. Each PSU must be connected to a separate source circuit breaker.

- Verify that the AC power cord or DC power cables from the power source to the firewall are not damaged. If the insulation is cracked or broken, immediately replace the cord or cable.

- Connect the PSU to a different power source with a new power cord or power cables. If the PSU status LEDs indicate that the PSU is not functioning normally, then the PSU is the source of the

problem. Replace the PSU with a spare, as described in "SRX4700 Power Supply Maintenance" on page 93.

- Verify that the PSU is functioning properly by checking the status of PSU LED. For more information, see "SRX4700 Power System" on page 25.
- If you cannot determine the cause of the problem or need additional assistance while troubleshooting a firewall, 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.

Reboot the Firewall Using the RESET Button

To troubleshoot the firewall, you might need to reboot it. To reboot the SRX4700 Firewall, press and hold the **RESET** button for less than 5 seconds.

CAUTION: Do not press and hold the **RESET** button for more than 5 seconds.

CHAPTER 7

Contact Customer Support and Return the Chassis or Components

IN THIS CHAPTER

Return an SRX4700 Chassis or a Component

IN THIS SECTION

How to Return a SRX4700 Chassis or a Component for Repair or Replacement

If you need to return a firewall or hardware component to Juniper Networks for repair or replacement, follow this procedure:

1. Determine the serial number of the chassis if you need to return the firewall. If you need to return one or more components, determine the serial number for each component. For instructions, see "Locate the Serial Number on a SRX4700 Chassis or Component" on page 118.
2. Obtain a Return Material Authorization (RMA) number from Juniper Networks Technical Assistance Center (JTAC) as described in "Contact Customer Support to Obtain a Return Material Authorization" on page 121.

   NOTE: Do not return 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 through collect freight.

3. Pack the firewall or component for shipping as described in "Pack an SRX4700 Firewall or Component for Shipping" on page 122.

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

Locate the Serial Number on a SRX4700 Chassis or Component

IN THIS SECTION

If you are returning a firewall or hardware component to Juniper Networks for repair or replacement, you must locate the serial number of the firewall or component. You must provide the serial number to the JTAC when you contact them to obtain the RMA.

If the firewall is operational and you can access the CLI, you can list serial numbers of the firewall and for some components with a CLI command. If you do not have access to the CLI or if the serial number for the component does not appear in the command output, you can locate the serial number ID label on the physical firewall or component.

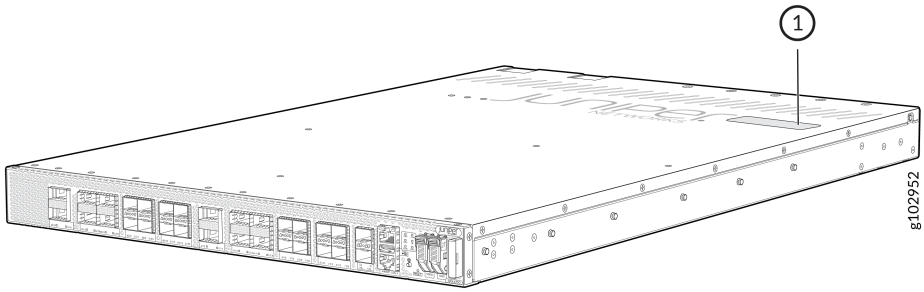
NOTE: If you want to find the serial number on the physical firewall component, you will need to remove the component from the firewall chassis, for which you must have the required parts and tools available.

List the SRX4700 Firewall and Components Details using the CLI

To list the firewall and firewall components and their serial numbers, enter the CLI command `show chassis hardware extensive`.

Locate the Chassis Serial Number ID Label on an SRX4700 Firewall

The serial number ID label is located on the top cover of the chassis on SRX4700 firewalls.

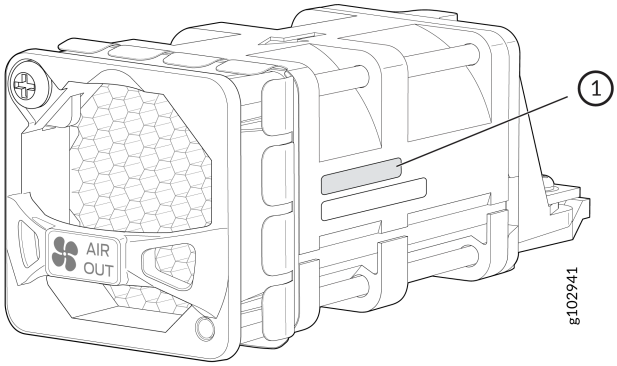


1. Serial ID Label

Locate the Serial Number ID Labels on FRUs in an SRX4700

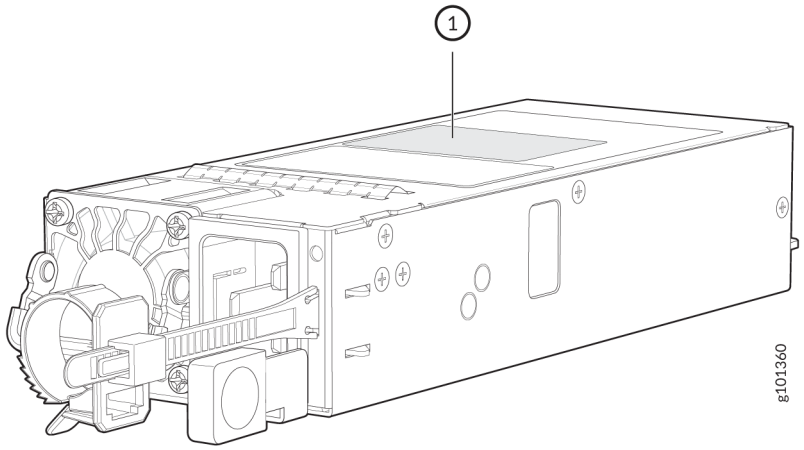
The fan modules and power supply units (PSUs) installed in SRX4700 firewalls are field-replaceable units (FRUs). You must remove the FRU from the firewall chassis to see its serial number ID label.

- Fan module—The serial number ID label is on the side of the fan module.



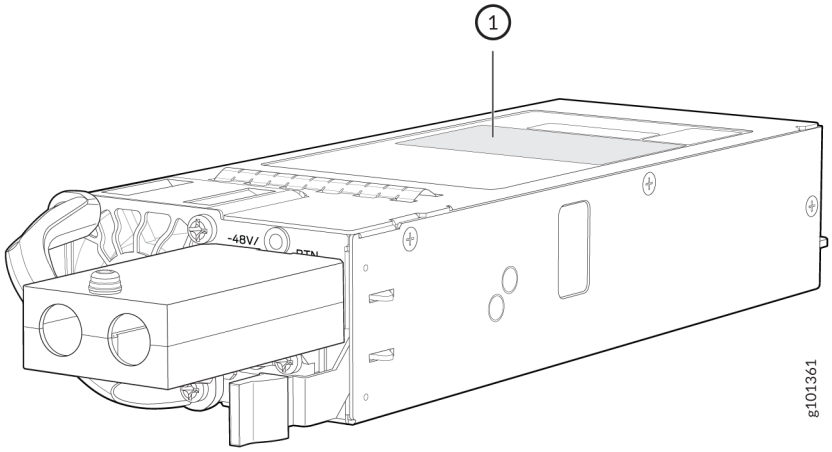
1. Serial number ID label

- PSU—The PSUs installed in an SRX4700 are FRUs. You must remove each FRU from the firewall chassis to see the FRU serial number ID label.
  - AC PSU—The serial number ID label is on the top of the AC PSU.



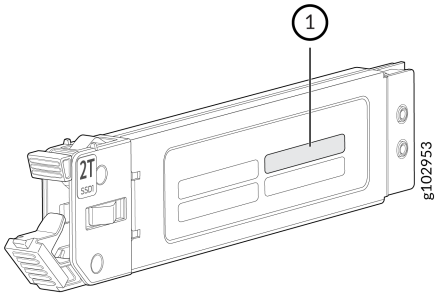
1. Serial number ID label

- DC PSU—The serial number ID label is on the top of the DC PSU.



1. Serial number ID label

- SSD—The serial number ID label is on the side of the SSD.



1. Serial number ID label

Contact Customer Support to Obtain a Return Material Authorization

If you need to return a device or hardware component to Juniper Networks for repair or replacement, obtain an RMA number from JTAC. You must obtain an RMA number before you attempt to return the component.

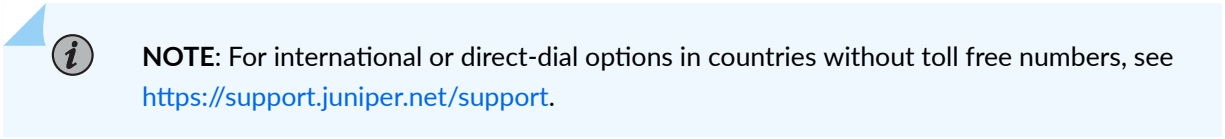
After locating the serial number of the device or hardware component you want to return, open a service request with the JTAC on the Web or by telephone.

Before you request an RMA number from JTAC, be prepared to provide the following information:

- Your existing service request number, if you have one
- Serial number of the component
- Your name, organization name, telephone number, fax number, and shipping address
- Details of the failure or problem
- Type of activity being performed on the device when the problem occurred
- Configuration data displayed by one or more `show` commands

You can contact JTAC 24 hours a day, seven days a week, on the Web or by telephone:

- Service Request Manager: https://support.juniper.net/support
- Telephone: +1-888-314-JTAC (+1-888-314-5822), toll free in U.S., Canada, and Mexico



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

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

The support representative validates your request and issues an RMA number for return of the component.

Pack an SRX4700 Firewall or Component for Shipping

IN THIS SECTION

If you are returning an SRX4700 firewall or component to Juniper Networks for repair or replacement, pack the item as described in this topic.

Before you pack the firewall or component, ensure that you have:

- Followed all the steps listed in "Contact Customer Support to Obtain a Return Material Authorization" on page 121.
- Retrieved the original shipping carton and packing materials. Contact your JTAC representative if you do not have these materials, to learn about approved packing materials (see "Contact Customer Support to Obtain a Return Material Authorization" on page 121).
- Ensure that you understand how to prevent electrostatic discharge (ESD) damage.
- An electrostatic discharge (ESD) grounding strap—not provided

Pack the Firewall for Shipping

Before you pack the firewall:

1. Shut down the firewall.
2. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
3. Disconnect power from the firewall.
4. Remove the cables that connect the firewall to external devices.
5. Remove all optical transceivers installed in the firewall.
6. Remove the fan modules and PSUs from the firewall.

Ensure that you have the following parts and tools:

- A Phillips (+) screwdriver, Number 2 —not provided

- The original packing material (cardboard box, accessory box and its contents, and foam padding)
- An ESD grounding strap—not provided
- Antistatic bag—not provided

If you need to transport the firewall to another location or return the firewall to Juniper Networks, you need to pack the firewall securely in its original packaging to prevent damage during transportation.

CAUTION: Do not pack the firewall in anything except its original container, or the firewall might be damaged in transit.

To pack the firewall:

1. Wrap and fasten one end of the ESD grounding strap around your bare wrist, and connect the other end of the strap to one of the ESD points on the chassis.
2. If the firewall is installed in a rack or cabinet, have one person support the weight of the firewall while another person unscrews and removes the mounting screws.
3. Remove the firewall from the rack or cabinet and place the firewall on a flat, stable surface.
4. Use the screwdriver to remove the rack mounting brackets from the firewall chassis.
5. Place the firewall in an antistatic bag.
6. Place the bottom portion of the packaging foam in the shipping carton.
7. Place the firewall inside the cavity in the bottom packaging foam.
8. Place the top portion of the packaging foam on top of the firewall.
9. If you are returning accessories or field-replaceable units (FRUs) with the firewall, pack them as instructed in "Pack the Firewall Components for Shipping" on page 123.
10. Place the accessory box by the rear end of the chassis in the shipping carton.
11. Close the top of the cardboard shipping box and seal it with packing tape.
12. Write the RMA number on the exterior of the box to ensure proper tracking.

Pack the Firewall Components for Shipping

Ensure that you have the following parts and tools available:

- Antistatic bag, one for each component—not provided
- An ESD grounding strap—not provided

If you need to transport a firewall component to another location or return a component to Juniper Networks, you need to pack the component securely in its original packaging to prevent damage during transportation.

CAUTION: Do not stack firewall components. Return individual components in separate boxes if they do not fit together on one level in the shipping box.

To pack the firewall components:

- Place individual components in antistatic bags.
- Use the original packing materials if they are available. If the original packing materials are not available, ensure the component is adequately packed to prevent damage during transit. The packing material you use must be able to support the weight of the component.
- Ensure that the components are adequately protected by wrapping them well with packing materials. Pack the component in an oversized box (if the original box is not available) with extra packing material around the unit so that the component is prevented from moving around inside the box.
- Securely tape the box closed.
- Write the RMA number on the exterior of the box to ensure proper tracking.

8
CHAPTER

Safety and Compliance Information

IN THIS CHAPTER

Safety Information for SRX4700

The Juniper Networks Safety Guide provides general safety information and guidelines for all Juniper Networks products. Follow the guidelines provided in the guide to reduce the likelihood of personal injury, equipment damage, and damage to surrounding areas.

Along with the information provided in the Juniper Networks Safety Guide, you must read and understand the specific safety information for SRX4700 provided in this hardware guide.

Compliance Standards for SRX4700 Firewalls

IN THIS SECTION

The SRX4700 complies with the following standards:

- Safety
  - UL 60950-1:2007 R10.14 Information Technology Equipment
  - CAN/CSA-C22.2 No. 60950-1-07, AMD 1:2011, AMD 2:2014 Information Technology Equipment
  - IEC/EN 60825-1 Safety of Laser Products – Part 1: Equipment Classification
  - IEC 62368-1 2014 (2nd Edition) Audio/Video, Information and Communication Technology Equipment
  - IEC 62368-1 2018 (3rd Edition) Audio/Video, Information and Communication Technology Equipment
  - EN 62368-1:2014+A11:2017 Audio/Video, Information and Communication Technology Equipment
  - UL/CSA 62368-1 :2019 (3rd Edition) Audio/Video, Information and Communication Technology Equipment

- EMC
  - FCC 47 CFR Part 15
  - ICES-003 / ICES-GEN
  - BS EN 55032
  - BS EN 55035
  - EN 300 386 V1.6.1
  - EN 300 386 V2.2.1
  - BS EN 300 386
  - EN 55032
  - CISPR 32
  - EN 55035
  - CISPR 35
  - IEC/EN 61000-3-2
  - IEC/EN 61000-3-3
  - AS/NZS CISPR 32
  - VCCI-CISPR 32
  - BSMI CNS 13438
  - KS C 9835 Old KN 35
  - KS C 9832 Old KN 32
  - KS C 9610
  - NEBS GR-1089-CORE, Issue 8
- Energy Efficiency requirements
  - AT&T TEER (ATIS-06000015.03.2013)
  - ECR 3.0.1
  - ETSI ES 203 136 (2013-05)
  - Verizon TEEER (VZ.TPR.9205 Issue 6)

- Environmental
  - Operating temperature: 0° C to 40° C
  - Storage temperature: –40° C to 70° C
  - Relative humidity (operating): 5 to 90% non-condensing
  - DC NEBS (GR 3160)
  - ETSI EN 300 019: Environmental Conditions & Environmental Tests for Telecommunications Equipment (Specific test requirements in Tables 7 & 8)
  - ETSI EN 300 019-2-1 Storage (ETSI EN 300 019 -1-1 Class 1.2)
  - ETSI EN 300 019-2-2 Transportation (ETSI EN 300 019-1-2 Class 2.3)
  - ETSI EN 300 019-2-3 Stationary Use at Weather-protected Locations (ETSI EN 300 019-1-3 Class 3.2)

Compliance Statements for NEBS

- The equipment is suitable for installation as part of the Common Bonding Network (CBN).
- The equipment is suitable for installation in locations where the National Electrical Code (NEC) applies.
- The battery return connection is to be treated as an isolated DC return (i.e.DC-I), as defined in GR-1089-CORE.
- You must provision a readily accessible device outside of the equipment to disconnect power. The device must also be rated based on local electrical code practice.
- For Juniper Networks systems with AC power supplies, an external surge protective device (SPD) must be used at the AC power source.

Compliance Statements for EMC Requirements for SRX4700 Firewall

IN THIS SECTION

This topic describes the EMC requirements for these hardware devices.

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.

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational, and safety requirements. Industry Canada does not guarantee the equipment will operate to the users' satisfaction.

Before installing this equipment, users should ensure that it is permissible to connect the equipment to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the inside wiring associated with a single line individual service can be extended by means of a certified connector assembly. The customer should be

aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, might give the telecommunications company cause to request the user to disconnect the equipment.

CAUTION: Users should not attempt to make electrical ground connections by themselves, but should contact the appropriate inspection authority or an electrician, as appropriate.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution might be particularly important in rural areas.

Taiwan

此為甲類資訊技術設備。於一般家居環境使用時，本設備可能導致射頻干擾，用□請採取相應措施。

The preceding translates as follows:

This is a Class A device. In a domestic environment, this device might cause radio interference, in which case the user needs to take adequate measures.

European Community

This is a Class A device. In a domestic environment this device might cause radio interference, in which case the user needs to take adequate measures.

Israel

אזהרה

מוצר זה הוא מוצר Class A.
בסביבה ביתית,מוצר זה עלול לגרום הפרעות בתדר רדיו,ובמקרה זה ,המשתמש עשוי להידרש לנקוט אמצעים מתאימים.

The preceding translates as follows:

Warning: 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

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

The preceding translates as follows:

This is a Class A device. In a domestic environment this device might cause radio interference, in which case the user needs to take adequate measures.

VCCI-A

Korea

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Korean Class A Warning g040913

The preceding translates as follows:

This equipment is Industrial (Class A) electromagnetic wave suitability equipment and seller or user should take notice of it, and this equipment is to be used in the places except for home

United States

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

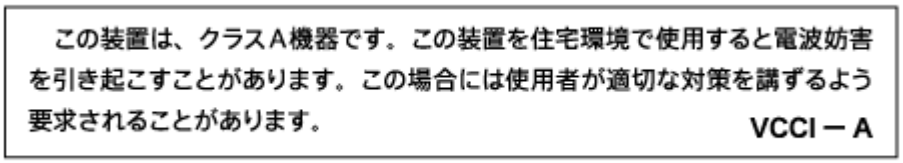
FCC Part 15 Statement

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, might cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

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

EMC Requirements for 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

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.