

SRX400 Firewall Hardware Guide

Published
2026-10-09

Copyright Information

© Copyright 2026 Hewlett Packard Enterprise Development LP

Open Source Code

This product includes code licensed under certain open source licenses which require source compliance. The corresponding source for these components is available upon request. This offer is valid to anyone in receipt of this information and shall expire three years following the date of the final distribution of this product version by Hewlett Packard Enterprise Company. To obtain such source code, please check if the code is available in the HPE Software Center at <https://myenterpriselicense.hpe.com/cwp-ui/software> but, if not, send a written request for specific software version and product for which you want the open source code. Along with the request, please send a check or money order in the amount of US \$10.00 to:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd, Spring, TX 77389
United States of America

Table of Contents

About This Guide | vi

1

Fast Track: Initial Installation

Fast Track to Rack Installation and Power | 2

Install the SRX400 Firewalls | **2**

Connect the SRX400 Firewalls to Power | **8**

Ground the SRX400 Firewalls | **8**

Connect the Power Cord and Power On the SRX400 | **10**

Power Off the SRX400 | **10**

Claim, Onboard, and Configure SRX400 Firewalls | 11

2

Overview

SRX400 Firewalls Overview | 14

3

Chassis

SRX400 Firewalls Chassis | 17

SRX400 Firewalls Chassis LEDs | 20

4

Power System

SRX400 Firewalls Power System | 25

Supported AC Power Cords | **26**

5

Installation and Setup

SRX400 Firewalls Installation Overview | 29

Unpack the SRX400 | 29

Unpack SRX400 Firewalls | **30**

Packing List for the SRX400 Firewalls | **30**

Install the SRX400 Firewalls | 31

Install the SRX400 Firewalls | **33**

Connect the SRX400 Firewalls to External Devices | 39

Connect Your Device to a Management Console Using a USB-C Connector | **39**

Connect the SRX400 Firewalls to Power | 41

Ground the SRX400 Firewalls | **41**

Connect the Power Cord and Power On the SRX400 | **42**

Power Off the SRX400 | **43**

Connect the SRX400 Firewalls to the Network | 43

Determine Transceiver Support for SRX400 Firewalls | **45**

Install a Transceiver | **45**

Connect a Fiber-Optic Cable | **47**

Perform Initial Software Configuration for SRX400 Firewall | 48

Configure the SRX400 Using J-Web | **48**

Configure the SRX400 Firewall Using Juniper® Security Director Cloud | **50**

Access the CLI on the SRX400 | **50**

Configure Root Authentication and Management Interface from CLI | **50**

Factory-Default Configuration of the SRX400 | **52**

View the SRX400 Factory-Default Configuration | **53**

6

Maintenance

Routine Maintenance Procedures for the SRX400 Firewalls | 55

7

Troubleshooting and Support

Troubleshoot the SRX400 Firewalls | 57

Troubleshooting Resources for SRX400 Firewalls | **57**

Use the RESET Button | **57**

Contact Customer Support and Return the Chassis or Components | 58

Contact Customer Support | **58**

Return a Hardware Component to Juniper Networks | **59**

Locate the Serial Number of the SRX400 Firewalls | **60**

Request a Return Material Authorization | **60**

Guidelines for Packing and Shipping Hardware Components | **61**

8

Safety and Compliance Information

Safety | 63

Agency Approvals for SRX400 Firewalls | 64

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX400 Firewalls.

After completing the installation and basic configuration procedures covered in this guide, refer to the [Junos OS Evolved](#) documentation for information about further software configuration.

1

CHAPTER

Fast Track: Initial Installation

IN THIS CHAPTER

- Fast Track to Rack Installation and Power | **2**
 - Claim, Onboard, and Configure SRX400 Firewalls | **11**
-

Fast Track to Rack Installation and Power

SUMMARY

This procedure guides you through the simplest steps to install the SRX400 Firewalls on a desk or other level surface. The procedure also includes the steps to mount each firewall in a two-post rack and connect it to power. Have more complex installation needs? See ["Install the SRX400 Firewalls"](#) on page 31.

IN THIS SECTION

- [Install the SRX400 Firewalls | 2](#)
- [Connect the SRX400 Firewalls to Power | 8](#)



Install the SRX400 Firewalls

IN THIS SECTION

- [Mount an SRX400 on a Desk or Other Level Surface | 3](#)
- [Mount an SRX400 on a Two-Post Rack | 4](#)

Before you install, review the following:

- [Site Guidelines and Requirements](#)
- [General Safety Guidelines and Warnings](#)
- ["Unpack the SRX400" on page 29](#)

You can mount SRX400 firewalls in the following ways:

1. On a desk or any other level surface using rubber feet.

2. In a two-post rack or cabinet using the SRX400-RMK rack-mount kit (ordered separately).

We'll walk you through the steps on how to mount the firewall on a desk, level surface, or two-post rack.

Mount an SRX400 on a Desk or Other Level Surface

Ensure that you have the following parts and tools available:

- Four rubber feet to stabilize the chassis on a desk or other level surface (provided)
- One AC power adapter.

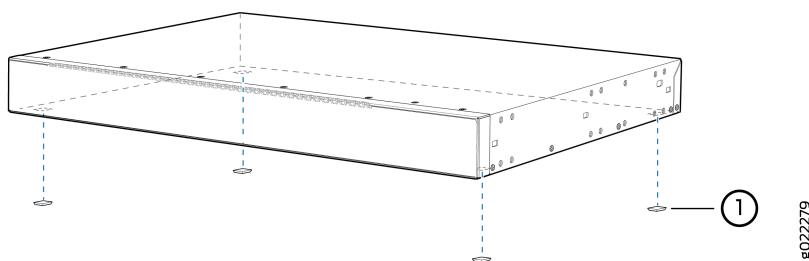
All the SRX400 models can be mounted on a desk or other level surface using the rubber feet.

To mount an SRX400 on a desk or other level surface:



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

1. Remove the firewall from the shipping carton—see ["Unpack the SRX400" on page 29.](#)
2. Turn the chassis upside down on the desk or the level surface where you intend to mount the firewall.
3. Attach the rubber feet to the bottom of the chassis.



Callout	Component
1	Rubber feet

4. Turn the chassis right side up and place it on the desk or the level surface.
5. Ensure the firewall rests firmly on the desk or level surface.

After you finish mounting the firewall on a desk or level surface, see "[Connect the SRX400 Firewalls to Power](#)" on page 41.

Mount an SRX400 on a Two-Post Rack

All the SRX400 models can be mounted on a two-post rack using the separately orderable SRX400-RMK rack-mount kit.

Ensure that you have the following parts and tools available:

- SRX400-RMK rack mount kit—separately orderable
 - Power adapter tray
 - Four cable ties
 - Four M4 screws
- One AC power adapter
- Phillips (+) screwdriver, number 2



NOTE: If you are mounting multiple SRX400 devices on a rack, mount the devices leaving 1-U space between the devices.

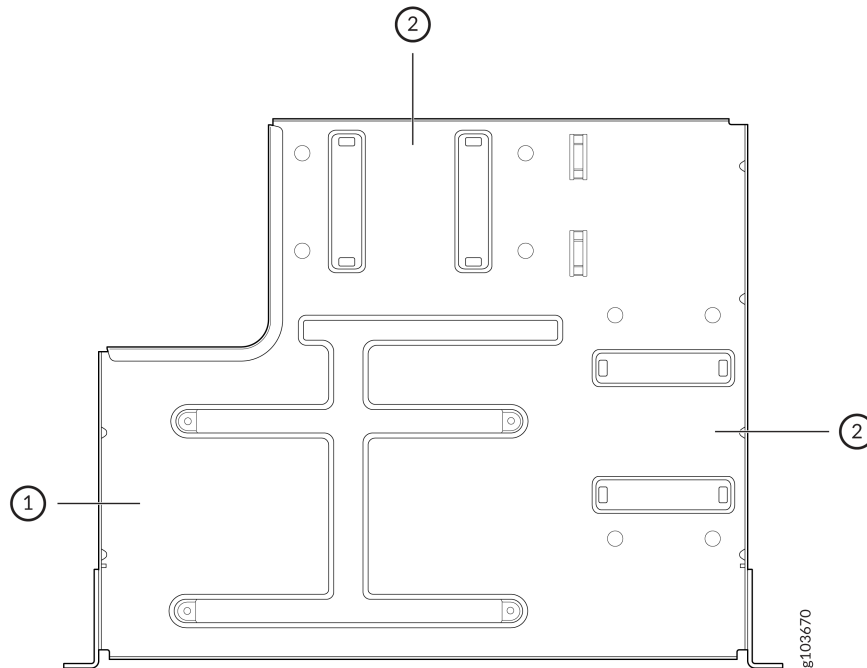


NOTE: If you are mounting multiple units on a rack, mount the units from the bottom to the top of the rack in decreasing order of weights. Therefore, you mount the heaviest unit right at the bottom and the lightest unit right at the top of the rack.

To mount an SRX400 firewall on a two-post rack:

1. Remove the firewall, power adapter tray, and AC power adapter from the shipping carton.

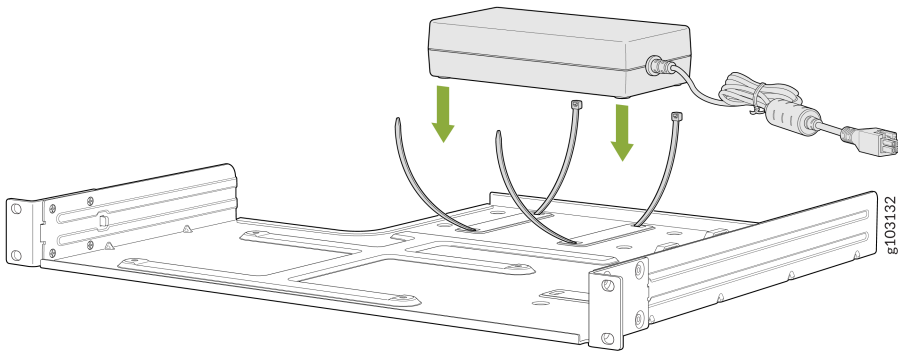
The power adapter tray will host the SRX400 firewall and an AC power adapter.



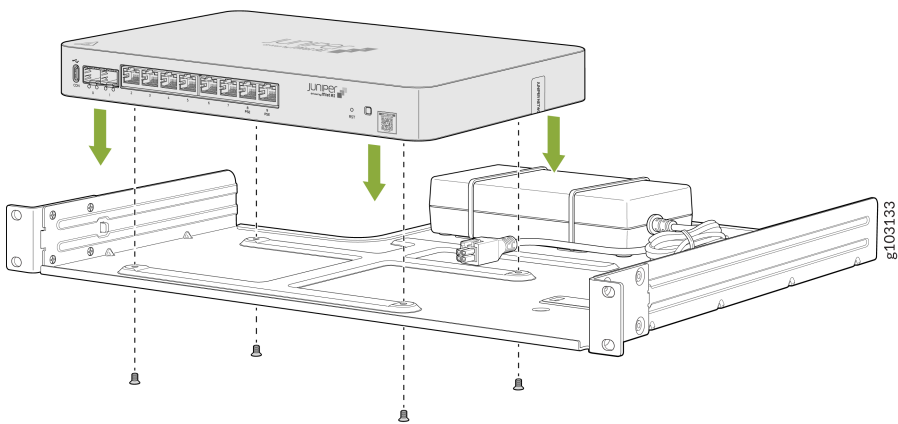
Callout	Component
1	SRX400 Chassis
2	Power Adapter

2. To install the power adapter on the tray, ensure you have the following parts available:

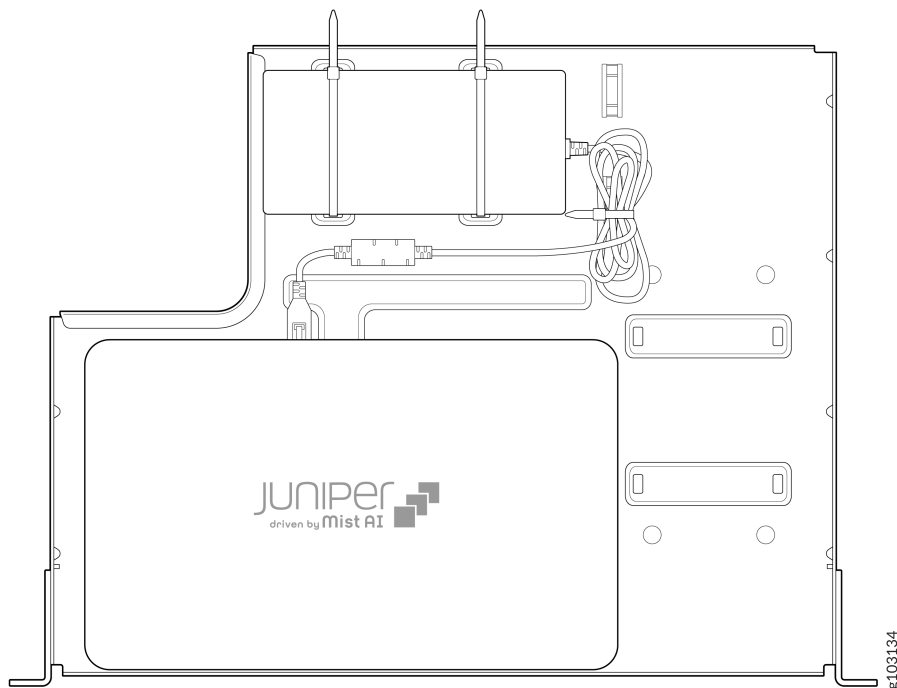
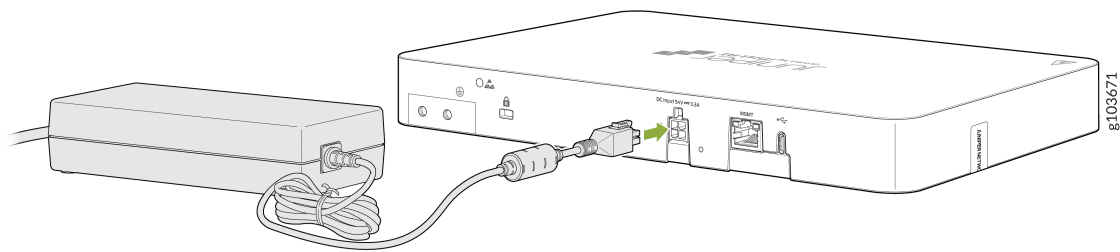
- An AC power adapter
 - Two cable ties
- a. Take a cable tie and insert the tail end of the cable tie through the two holes on the tray.
 - b. Repeat "2.a" on page 5 with the second cable tie.
 - c. Place the power adapter on the tray in between the cable ties.
 - d. Take the tailend of one cable tie, insert it through the square locking piece (other end of the cable tie), and pull the tie through the main head to set the length of excess material.
 - e. Repeat "2.d" on page 5 with the second cable tie.



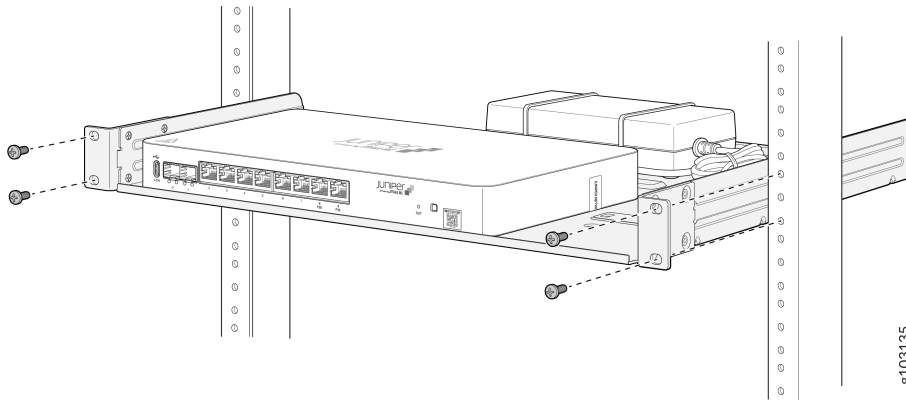
3. To install any one of the SRX400 chassis on the tray:
- Have one person grasp the sides of the tray and hold it.
 - Have a second person position the chassis on the tray and align the bottom holes of the chassis with the four holes on the tray.
 - Install the four M4 screws into each of these four holes on the tray. Use the Phillips (+) screwdriver, number 2 to tighten the four screws and secure the chassis to the tray.



4. Plug the DC connector end of the power cable into the power connector on the back of the firewall.



5. Have one person grasp the sides of the firewall, lift it, and position it in the rack.
6. Align each bottom hole of the power adapter tray with a hole in each rack rail, making sure the firewall is level.
7. Have a second person secure the firewall to the rack by using four mounting screws (not provided). Use the Phillips (+) screwdriver, number 2 to tighten the four screws and secure the power adapter tray to the rack. Tighten the screws with a torque of 18 Nm.



8. Ensure that the firewall is level by verifying that all the screws on one side of the rack are aligned with the screws on the other side.

Connect the SRX400 Firewalls to Power

SUMMARY

Connecting the SRX400 to power involves the following steps and safety precautions to prevent equipment damage and personal injury.

IN THIS SECTION

- [Ground the SRX400 Firewalls | 8](#)
- [Connect the Power Cord and Power On the SRX400 | 10](#)
- [Power Off the SRX400 | 10](#)

Ground the SRX400 Firewalls

Before connecting an SRX400 to an earth ground, ensure that you have the following parts and tools:

- An electrostatic discharge (ESD) grounding strap (not provided)
- Grounding cable for your firewall (not provided)—The grounding cable must be 14 AWG stranded wire and rated 90 °C or according to local electrical code.
- Grounding lug for your grounding cable (not provided)—This lug attaches to the chassis grounding point. The grounding lug required is a : Panduit LCD10-14AF-L or equivalent.
- Two M5 X 9.5 screws (not provided)

- A Phillips screwdriver to tighten the screws (not provided).

You must install heat-shrink tubing insulation around the crimped section of the power cables and lugs.



NOTE: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the SRX400 to an earth ground before you connect the firewall to power.

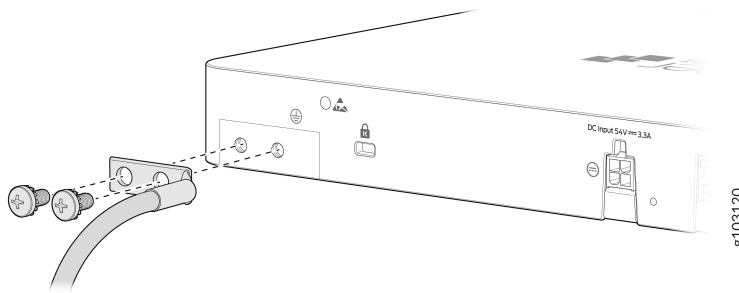
Before you connect an earth ground to the protective earthing terminal of the firewall, ensure that a licensed electrician attaches an appropriate grounding terminal to the grounding cable you supply. Using a grounding cable with an incorrectly attached terminal can damage the firewall.



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

To ground the SRX400:

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 the chassis.
2. Ensure that all grounding surfaces are clean and brought to a bright finish before making the grounding connections.
3. Connect the 14 AWG grounding cable to a proper earth ground, such as the rack in which you mount the firewall.
4. Place the grounding cable terminal over the grounding point (sized for M5 X 9.5 grounding screws) on the rear of the chassis.



5. Secure the grounding cable terminal to the grounding point with the two M5 X 9.5 screws. Apply between 2.5 Nm and 2.8 Nm of torque to the screw.
6. 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 SRX400

Ensure that you have a power cord appropriate for your geographical location.

For information about the supported AC power cord specifications for your firewall, see ["SRX400 Firewalls Power System" on page 25](#).

To connect the power cord:

1. Wrap and fasten one end of the electrostatic discharge (ESD) grounding strap around your bare wrist, and connect the other end to a site ESD point or to the ESD point on the chassis.
2. Locate the AC power cord shipped with the firewall; the cord has plug appropriate for your geographical location.
3. Insert the AC power cord coupler firmly into the power cord inlet on the AC power adapter.
4. If the AC power source outlet has a power switch, turn it off.
5. Plug the AC power cord into an AC power source outlet.
6. The SRX400 models do not have a power switch and each device powers on as soon as you plug it in.

Power Off the SRX400

You can power off the SRX400 in one of the following ways:

- Graceful shutdown—Using the CLI—Use the request `system power-off` command.

The device 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.

- Forced shutdown—Unplug the power cord or switch off the power source.



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

Use the forced shutdown method as a last resort to recover the firewall if the firewall OS is not responding to the graceful shutdown method.

Claim, Onboard, and Configure SRX400 Firewalls

SUMMARY

This topic provides you the pointers to onboard and configure the SRX400 Firewalls using Juniper® Mist, Juniper® Security Director, or configure the SRX400 Firewalls using J-Web or Junos OS Evolved CLI.

IN THIS SECTION

- [Claim, Onboard and Configure the SRX400 Firewalls using Mist | 11](#)
- [Onboard and Configure the SRX400 Firewalls using Security Director | 11](#)
- [Configure SRX400 Firewalls Using the Junos OS Evolved CLI | 12](#)

Claim, Onboard and Configure the SRX400 Firewalls using Mist

The SRX400 Firewall is a cloud-ready device, and you can manage with using the [Mist AI cloud portal](#). If you have a Mist WAN Assurance license, you can follow a few simple steps to get the SRX400 Firewalls up and running in the Mist AI cloud portal.

If you want to	Then
Perform configuration and deployment procedures	See Configuration Essentials: SRX400 Firewall Series
Claim and onboard to Mist	See Cloud-Ready SRX Series Firewalls with Mist .
Configure WAN Assurance	Mist WAN Assurance Configuration Guide .
See all available documentation for WAN Assurance	See WAN Assurance Documentation .

Onboard and Configure the SRX400 Firewalls using Security Director

If you have a Juniper Security Director license, you can follow a few simple steps to get the SRX400 Firewalls up and running on the Security Director Cloud portal. You can also manage the SRX400 Firewalls using Security Director On-Premise.

If you want to	Then
Claim and onboard to Security Director Cloud	See Onboard SRX Firewalls to Security Director Cloud .
See all available documentation for Security Director	See Juniper Security Director .
See all available documentation for Security Director Cloud	See Juniper Security Director Cloud .

Configure SRX400 Firewalls Using the Junos OS Evolved CLI

You can configure the SRX400 Firewalls using the Junos OS Evolved CLI.

If you want to	Then
Customize basic configuration	See "Perform Initial Software Configuration for SRX400 Firewall" on page 48
Explore software features supported on the SRX400 Firewalls	See Feature Explorer .
Configure Junos OS Evolved features on the SRX400 Firewalls	See User Guides .
Stay up-to-date about new and changed features, and known and resolved issues	See Junos OS Release Notes .

2

CHAPTER

Overview

IN THIS CHAPTER

- [SRX400 Firewalls Overview](#) | **14**
-

SRX400 Firewalls Overview

SUMMARY

Learn about the hardware features of the SRX400 Firewalls.

IN THIS SECTION

- [Meet the SRX400 Firewalls | 14](#)

Meet the SRX400 Firewalls

SRX400 Firewall is an Juniper Networks AI-native next-generation firewall (NGFW) that consolidates routing and software-defined WAN (SD-WAN) capabilities into a single, compact, fanless device. SRX400 firewall is designed to cater to your current network needs and is scalable to meet future demands.

SRX400 is ideal for small branches and retail locations.

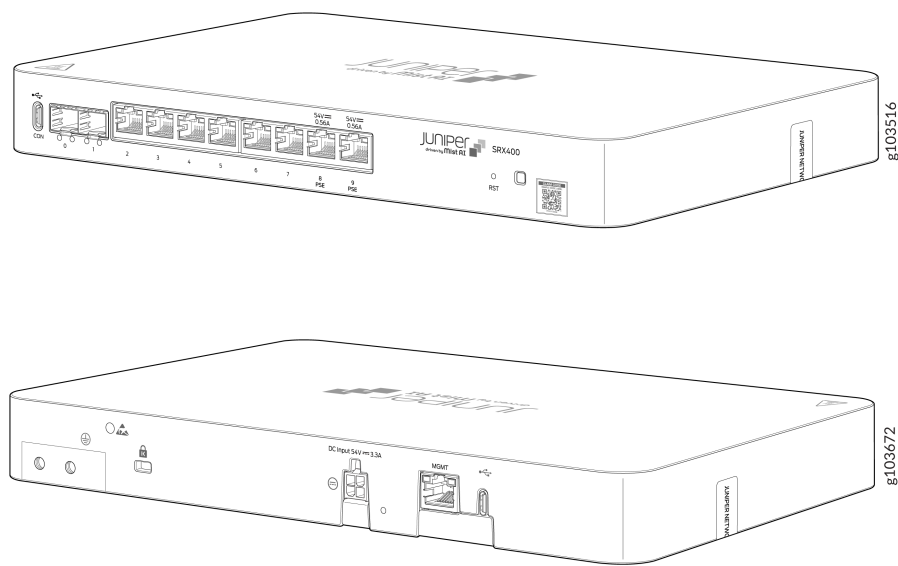


Table 1: SRX400 Firewalls Description

Form factor	1 U
Chassis type	Fixed configuration

Operating system	Junos OS Evolved
Power system	AC 180 W power supply adapter
Cooling system	Fanless
Port configuration	• Eight 10/100/1000BASE-T Gigabit Ethernet (GbE) RJ-45 ports Two ports (8 and 9) out of 8 x 10/100/1000 GbE BASE-T RJ-45 are PoE+ (30W/port) ports • Two 1GbE SFP ports (0 and 1) • One 1GbE BASE-T RJ45 management (MGMT) port • Console port - One USB 2.0 Type C • One USB 2.0 Type C port that accepts a USB storage device.
Memory	8 GB DDR4
Managed using	• Juniper® Mist • Juniper® Security Director Cloud • J-Web • Junos OS Evolved CLI

3

CHAPTER

Chassis

IN THIS CHAPTER

- SRX400 Firewalls Chassis | **17**
 - SRX400 Firewalls Chassis LEDs | **20**
-

SRX400 Firewalls Chassis

SUMMARY

Learn about the components in the SRX400 Firewalls chassis.

IN THIS SECTION

- [SRX400 Firewalls Specifications | 17](#)

The SRX400 Firewalls chassis is rigid sheet-metal structures that house all components of the device.

SRX400 Firewalls Specifications

Table 2: Physical Specifications

Specification	Value
Height	1.3 in. (3.3 cm)
Width	11.81 in. (29.9 cm)
Depth	7.52 in. (19.1 cm)
Weight	3.52 lb (1.6 kg)

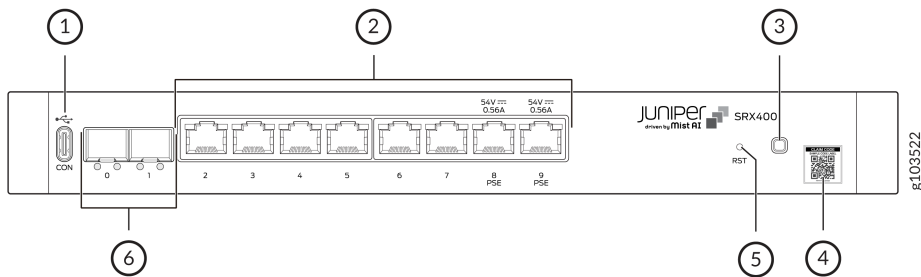
Table 3: Environmental Specifications

Specification	Value
Operating altitude	6561.68 ft (2000 m)
Operating temperature	32 °F to 122 °F (0 °C to 50 °C)
Storage temperature	-40 °F to 158 °F (-40 °C to 70 °C)
Relative humidity (operating) (noncondensing)	10% to 90%

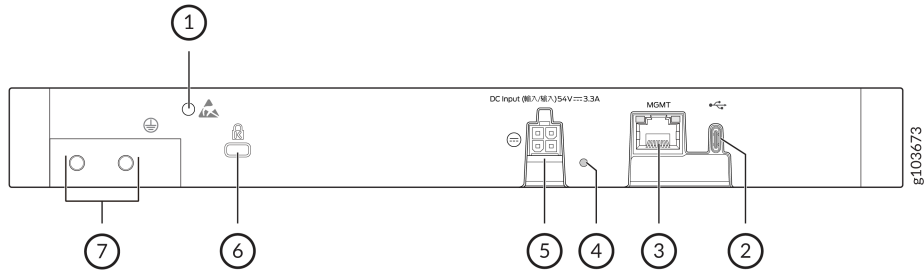
Table 3: Environmental Specifications (Continued)

Specification	Value
Relative humidity (nonoperating) (noncondensing)	5% to 95%
Seismic tolerance	Zone 4

Figure 1: SRX400 Front Panel



Callout	Item
1	Console port—USB Type C
2	Eight 10/100/1000BASE-T Gigabit Ethernet (GbE) RJ-45 network ports Ports 8 and 9 are PoE+ (30 W/port) ports
3	Multicolor system LED
4	QR code label (For quick onboarding of the device to Juniper Security Director Cloud)
5	RESET (RST) button
6	Two 1GbE SFP ports

Figure 2: SRX400 Rear Panel

Callout	Item
1	ESD point
2	USB 2.0 Type C port that accepts a USB storage device.
3	One 1GbE BASE-T RJ45 management MGMT port
4	Power supply adapter (PSA) LED
5	PSA point
6	Security slot to lock and secure the chassis
7	Ground terminal

SRX400 Firewalls Chassis LEDs

SUMMARY

This topic describes the status LEDs for the chassis and ports on the SRX400 Firewalls.

IN THIS SECTION

- [Chassis Status LED | 20](#)
- [SFP Network Port Status LEDs | 21](#)
- [RJ-45 Network Ports Status LEDs | 21](#)
- [MGMT Port Status LED | 22](#)
- [Power Supply Adapter LED | 23](#)

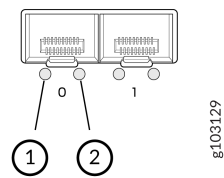
The LEDs on the SRX400 Firewalls indicate the status of the device and its components. You can also use the LEDs for troubleshooting.

Chassis Status LED

The System LED is a multi-color LED located on the front panel of the firewall. It provides a high level indicator of the firewall status.

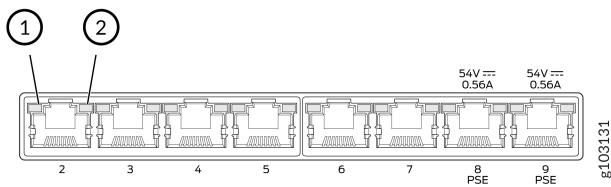
Component	LED	Color	Description
System LED	Status	Multicolor	Steady Green: Device is operating normally.
			Amber: Device is starting up.
			Purple: Minor alarms
			Red: Major alarms
			Off: Device has shut down.

SFP Network Port Status LEDs



Callout	LED	Color and State	Description
1	Link Activity	Blinking Green	The port and the link are active, and there is link activity.
		Glowing steadily	The port and the link are active, but there is no link activity.
		Unlit	The port is inactive.
2	Port speed	Blinking Green	1000 Mbps (1 blink per second)
		Unlit	The port is inactive.

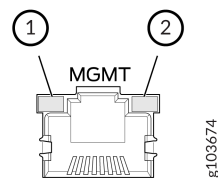
RJ-45 Network Ports Status LEDs



Callout	LED	Port Parameters	Color and State	Description
1	Link Activity	—	Blinking Green	The port and the link are active, and there is link activity.
			Glowing steadily	The port and the link are active, but there is no link activity.
			Unlit	The port is inactive.
2	Status	Speed (SPD)	Blinking Green	100 Mbps (1 blink per second)
			Glowing steadily	1000 Mbps
			Unlit	10 Mbps or the port is inactive

MGMT Port Status LED

The MGMT port is located on the rear of the chassis and the two LEDs link activity and port speed.



Callout	LED	Color and State	Description
1	Link Activity	Blinking Green	The port and the link are active, and there is link activity.
		Glowing steadily	The port and the link are active, but there is no link activity.
		Unlit	The port is inactive.
2	Status	Blinking Green	1000 Mbps (1 blink per second)
		Glowing steadily	10 Mbps or 100 Mbps
		Unlit	The link is down.

Power Supply Adapter LED

The Power Supply Adapter (PSA) LED is located on the rear of the chassis to indicate the status of the PSA.

LED	Color and State	Description
Status	Steady Green	Receiving power
	Unlit	Failure or no power

4

CHAPTER

Power System

IN THIS CHAPTER

- [SRX400 Firewalls Power System](#) | **25**
-

SRX400 Firewalls Power System

SUMMARY

The power system for the SRX400 Firewalls include an AC power supply adapter (PSA) and related power cords and cables. The AC power adapter operates within certain ranges and the chassis is equipped with a status indicator LED.

IN THIS SECTION

- [Supported AC Power Cords | 26](#)

The SRX400 Firewalls receive power from an external source. You must use an AC 180-W power supply adapter (PSA) provided by Juniper Networks to provide power to the appliances. The adapter provides an output of 54 volts direct current (VDC) at 3.3 amperes (A).

Table 4: Electrical Specifications of Power Supply Adapter

Specification	Value
Maximum power output	180 W
Input voltage	100–240 VAC
Input current rating	2.6 A at 100 VAC
Input line frequency	50-60 Hz

Table 5: System Power Consumption

Model	Maximum System Power Consumption	Typical System Power Consumption
SRX400	107 W	85 W

Supported AC Power Cords

A detachable AC power cord is supplied with the device. The coupler is type C13 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 6: Supported AC Power Cords

Locale	Cord Set Rating	Plug Standard
Argentina	250 VAC, 10 A, 50 Hz	IRAM 2073 Type RA/3
Australia	250 VAC, 10 A, 50 Hz	AS/NZS 3112 Type SAA/3
Brazil	250 VAC, 10 A, 50 Hz	NBR 14136 Type BR/3
China	250 VAC, 10 A, 50 Hz	GB 1002-1996 Type PRC/3
Continental Europe	250 VAC, 10 A, 50 Hz or 60 Hz	EN 60320/Type C13
India	250 VAC, 10 A, 50 Hz	IS 1293 Type IND/3
Israel	250 VAC, 10 A, 50 Hz	SI 32/1971 Type IL/3G
Italy	250 VAC, 10 A, 50 Hz	CEI 23-16 Type I/3G
Japan	125 VAC, 12 A, 50 Hz or 60 Hz	JIS C8303
Korea	250 VAC, 10 A, 50 Hz or 60 Hz	KSC8305
South Africa	250 VAC, 10 A, 50 Hz	SABS 164/1:1992 Type ZA/13
Switzerland	250 VAC, 10 A, 50 Hz	SEV 6534-2 Type 12G
Taiwan	125 VAC, 13 A, 60 Hz	NEMA 5-15 Type N5-15

Table 6: Supported AC Power Cords (*Continued*)

Locale	Cord Set Rating	Plug Standard
International (except India)	250 VAC, 10 A, 50 Hz	EN 60320/Type C13
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363/A Type BS89/13
USA	125 VAC, 13 A, 60 Hz	NEMA 5-15 Type N5-15

5

CHAPTER

Installation and Setup

IN THIS CHAPTER

- SRX400 Firewalls Installation Overview | **29**
 - Unpack the SRX400 | **29**
 - Install the SRX400 Firewalls | **31**
 - Connect the SRX400 Firewalls to External Devices | **39**
 - Connect the SRX400 Firewalls to Power | **41**
 - Connect the SRX400 Firewalls to the Network | **43**
 - Perform Initial Software Configuration for SRX400 Firewall | **48**
-

SRX400 Firewalls Installation Overview

SUMMARY

This topic lists the steps that you need to follow to get your SRX400 Firewalls up and running.



To install and configure the SRX400 Firewalls:

1. Unpack your device as described in ["Unpack the SRX400" on page 29](#).
2. Install the device as described in ["Install the SRX400 Firewalls" on page 31](#).
3. Connect cables to network device as described in ["Connect the SRX400 Firewalls to the Network" on page 43](#).
4. Connect cables to external devices as described in ["Connect the SRX400 Firewalls to External Devices" on page 39](#).
5. Connect the grounding cable and power on the firewall as described in ["Connect the SRX400 Firewalls to Power" on page 41](#).
6. Perform initial configuration by following the instructions in ["Perform Initial Software Configuration for SRX400 Firewall" on page 48](#).

Unpack the SRX400

SUMMARY

Unpack an SRX400 Firewall by following the recommended procedure and check that you have received all the components.

IN THIS SECTION

- [Unpack SRX400 Firewalls | 30](#)

- [Packing List for the SRX400 Firewalls](#) | 30

Unpack SRX400 Firewalls

We ship SRX400 Firewalls in a cardboard carton, secured with foam packing material.



CAUTION: SRX400 Firewalls have maximum protection inside the shipping carton. Do not unpack the device until you are ready to mount it.

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

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

To unpack the device:

1. Move the shipping carton to a staging area as close to the installation site as possible. Also ensure that this area provides you with enough room to remove the device and its components.
2. Position the carton so that the arrows marked on the carton are pointing up.
3. Open the top flaps on the shipping carton.
4. Pull out the packing material holding the device in place.
5. Verify the parts received against the packing list as mentioned in "[Packing List for the SRX400 Firewalls](#)" on page 30.
6. Save the shipping carton and packing materials in case you need to move or ship the device later.

Packing List for the SRX400 Firewalls

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 that 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 7: Parts List for the SRX400 Firewall

Component	Part Number	Quantity
Chassis	SRX400	1
Rubber feet	—	4
Power supply adapter (PSA) and power cord	SRX400-PSU-AC-EXT	1
Rack mount kit (separately orderable) • One power adaptor tray • Four cable ties • Four M4 screws	SRX400-RMK	1
Documentation roadmap	—	1

Install the SRX400 Firewalls

SUMMARY

This topic guides you through the steps to install an SRX400 firewall on a desk or other level surface or mount each firewall in a two-post rack.

IN THIS SECTION

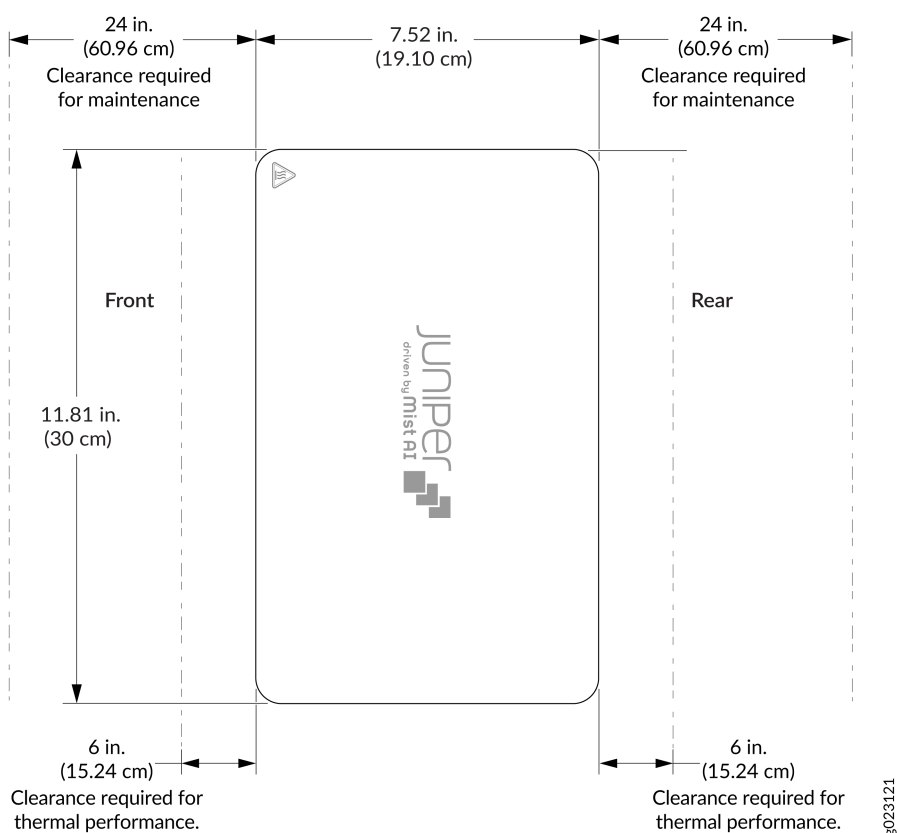
- [Install the SRX400 Firewalls | 33](#)

You can mount an SRX400 on a desk or other level surface. Alternatively, you can mount each of these firewalls in a two-post rack, using the separately orderable rack mount kit shipped with the firewall.

Complete these prerequisites before you mount the firewall:

- Prepare the site for installation as described in the [Site and Electrical Guidelines](#).
- Ensure that the site has adequate clearance for both airflow and hardware maintenance.

Figure 3: Clearance Requirements for the SRX400 Firewalls



- Unpack the device as described in "Unpack the SRX400" on page 29.



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 also verify that the rack or cabinet has adequate support at the installation site.

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.



NOTE: If you are mounting multiple SRX400 devices on a rack, mount the devices leaving 1RU space between the devices.

Install the SRX400 Firewalls

IN THIS SECTION

- [Mount an SRX400 on a Desk or Other Level Surface | 34](#)
- [Mount an SRX400 on a Two-Post Rack | 35](#)

Before you install, review the following:

- [Site Guidelines and Requirements](#)
- [General Safety Guidelines and Warnings](#)
- ["Unpack the SRX400" on page 29](#)

You can mount SRX400 firewalls in the following ways:

1. On a desk or any other level surface using rubber feet.
2. In a two-post rack or cabinet using the SRX400-RMK rack-mount kit (ordered separately).

We'll walk you through the steps on how to mount the firewall on a desk, level surface, or two-post rack.

Mount an SRX400 on a Desk or Other Level Surface

Ensure that you have the following parts and tools available:

- Four rubber feet to stabilize the chassis on a desk or other level surface (provided)
- One AC power adapter.

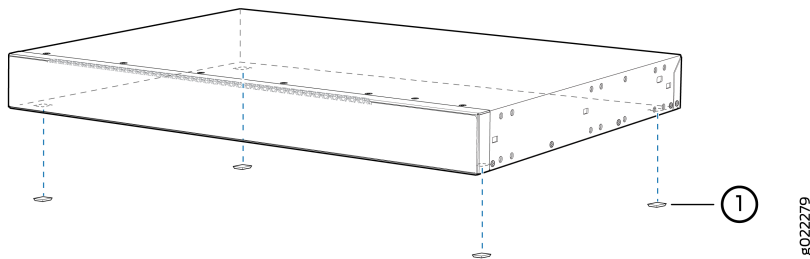
All the SRX400 models can be mounted on a desk or other level surface using the rubber feet.

To mount an SRX400 on a desk or other level surface:



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

1. Remove the firewall from the shipping carton—see ["Unpack the SRX400" on page 29](#).
2. Turn the chassis upside down on the desk or the level surface where you intend to mount the firewall.
3. Attach the rubber feet to the bottom of the chassis.



Callout	Component
1	Rubber feet

4. Turn the chassis right side up and place it on the desk or the level surface.
5. Ensure the firewall rests firmly on the desk or level surface.

After you finish mounting the firewall on a desk or level surface, see ["Connect the SRX400 Firewalls to Power" on page 41](#).

Mount an SRX400 on a Two-Post Rack

All the SRX400 models can be mounted on a two-post rack using the separately orderable SRX400-RMK rack-mount kit.

Ensure that you have the following parts and tools available:

- SRX400-RMK rack mount kit—separately orderable
 - Power adapter tray
 - Four cable ties
 - Four M4 screws
- One AC power adapter
- Phillips (+) screwdriver, number 2



NOTE: If you are mounting multiple SRX400 devices on a rack, mount the devices leaving 1-U space between the devices.

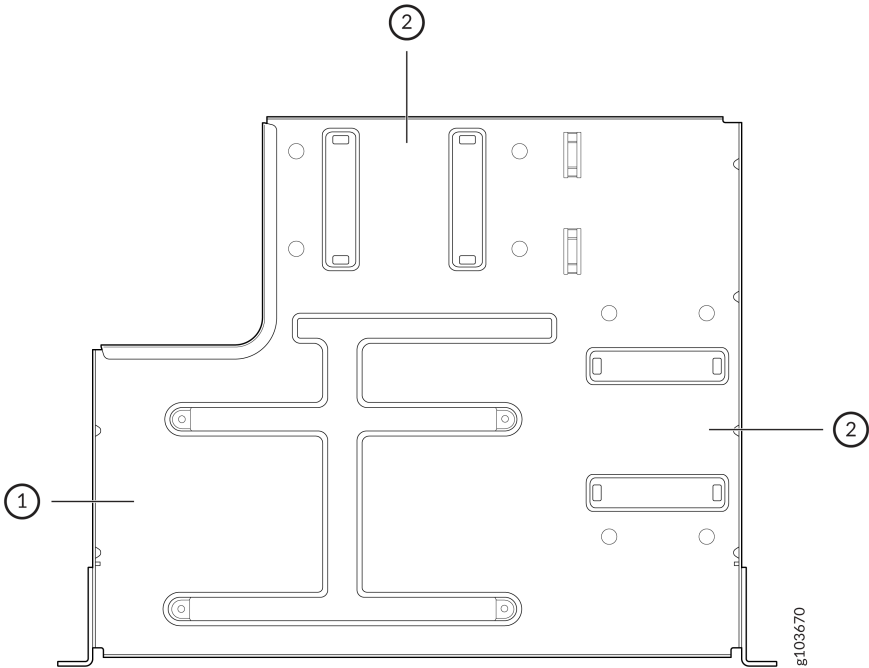


NOTE: If you are mounting multiple units on a rack, mount the units from the bottom to the top of the rack in decreasing order of weights. Therefore, you mount the heaviest unit right at the bottom and the lightest unit right at the top of the rack.

To mount an SRX400 firewall on a two-post rack:

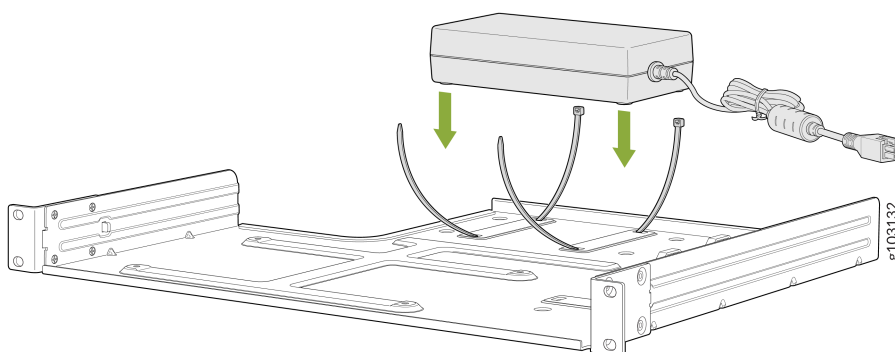
1. Remove the firewall, power adapter tray, and AC power adapter from the shipping carton.

The power adapter tray will host the SRX400 firewall and an AC power adapter.

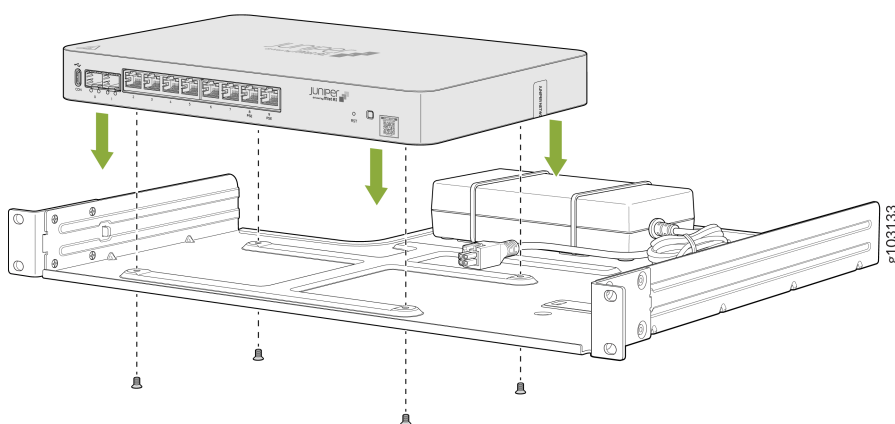


Callout	Component
1	SRX400 Chassis
2	Power Adapter

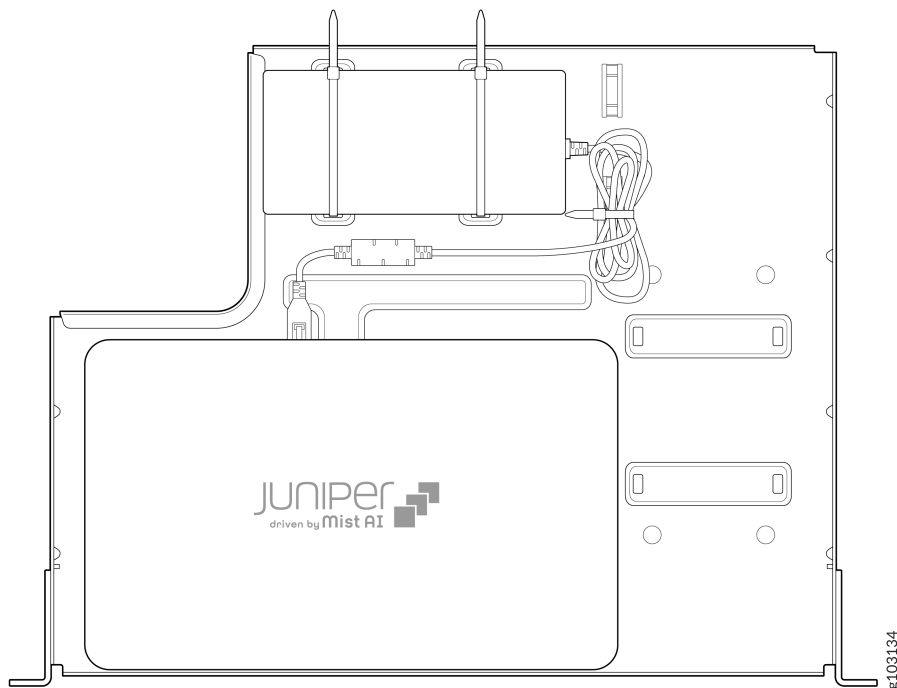
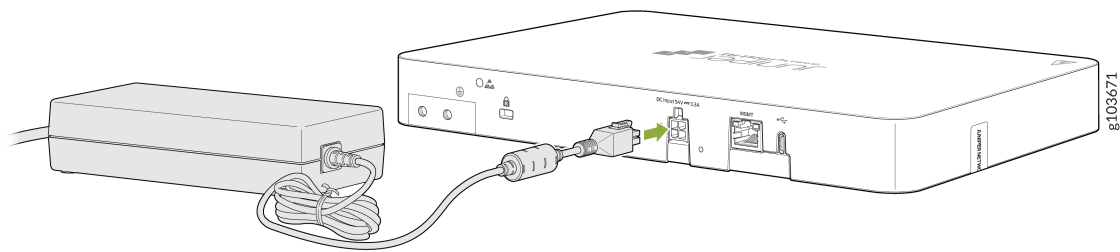
2. To install the power adapter on the tray, ensure you have the following parts available:
- An AC power adapter
 - Two cable ties
- a. Take a cable tie and insert the tail end of the cable tie through the two holes on the tray.
- b. Repeat "2.a" on page 36 with the second cable tie.
- c. Place the power adapter on the tray in between the cable ties.
- d. Take the tailend of one cable tie, insert it through the square locking piece (other end of the cable tie), and pull the tie through the main head to set the length of excess material.
- e. Repeat "2.d" on page 36 with the second cable tie.



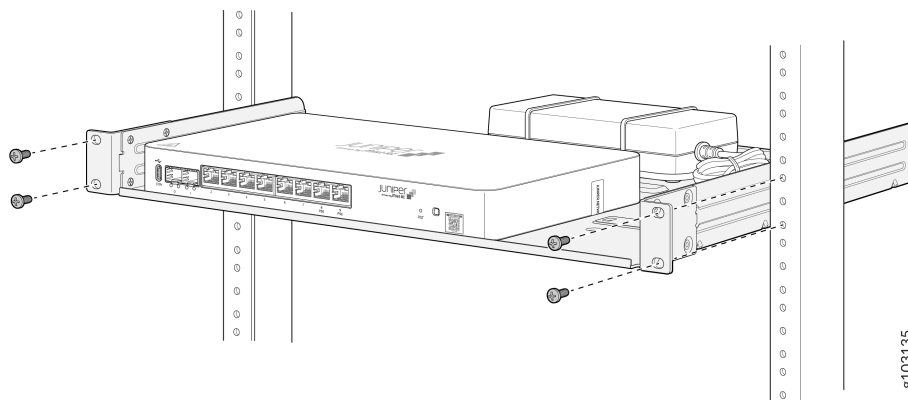
3. To install any one of the SRX400 chassis on the tray:
- Have one person grasp the sides of the tray and hold it.
 - Have a second person position the chassis on the tray and align the bottom holes of the chassis with the four holes on the tray.
 - Install the four M4 screws into each of these four holes on the tray. Use the Phillips (+) screwdriver, number 2 to tighten the four screws and secure the chassis to the tray.



4. Plug the DC connector end of the power cable into the power connector on the back of the firewall.



5. Have one person grasp the sides of the firewall, lift it, and position it in the rack.
6. Align each bottom hole of the power adapter tray with a hole in each rack rail, making sure the firewall is level.
7. Have a second person secure the firewall to the rack by using four mounting screws (not provided). Use the Phillips (+) screwdriver, number 2 to tighten the four screws and secure the power adapter tray to the rack. Tighten the screws with a torque of 18 Nm.



8. Ensure that the firewall is level by verifying that all the screws on one side of the rack are aligned with the screws on the other side.

Connect the SRX400 Firewalls to External Devices

SUMMARY

This topic guides you on how to connect your SRX400 Firewalls to external management devices.

IN THIS SECTION

- [Connect Your Device to a Management Console Using a USB-C Connector](#) | 39

You can monitor and manage the SRX400 Firewalls by using a dedicated management channel. Use the USB 2.0 Type C console port located on the front panel of your firewall to connect to a management device.

Connect Your Device to a Management Console Using a USB-C Connector

Ensure that you have a USB cable that has a USB-C male connector at either end.

Set the HyperTerminal properties of the console server or management console as follows:

- Baud rate—115200
- Flow control—None
- Data—8
- Parity—None
- Stop bits—1

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 console cable with the USB-C male connector to the console port on the firewall.
3. Connect the other end of the cable with the appropriate connector to the console server or management console.

Figure 4: Connect Your Device to a Management Console Through a Console Server

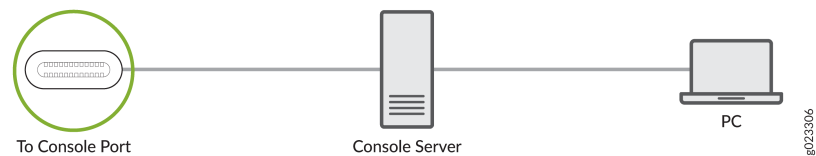


Figure 5: Connect Your Device Directly to a Management Console



Connect the SRX400 Firewalls to Power

SUMMARY

Connecting the SRX400 to power involves the following steps and safety precautions to prevent equipment damage and personal injury.

IN THIS SECTION

- [Ground the SRX400 Firewalls | 41](#)
- [Connect the Power Cord and Power On the SRX400 | 42](#)
- [Power Off the SRX400 | 43](#)

Ground the SRX400 Firewalls

Before connecting an SRX400 to an earth ground, ensure that you have the following parts and tools:

- An electrostatic discharge (ESD) grounding strap (not provided)
- Grounding cable for your firewall (not provided)—The grounding cable must be 14 AWG stranded wire and rated 90 °C or according to local electrical code.
- Grounding lug for your grounding cable (not provided)—This lug attaches to the chassis grounding point. The grounding lug required is a : Panduit LCD10-14AF-L or equivalent.
- Two M5 X 9.5 screws (not provided)
- A Phillips screwdriver to tighten the screws (not provided).

You must install heat-shrink tubing insulation around the crimped section of the power cables and lugs.



NOTE: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the SRX400 to an earth ground before you connect the firewall to power.

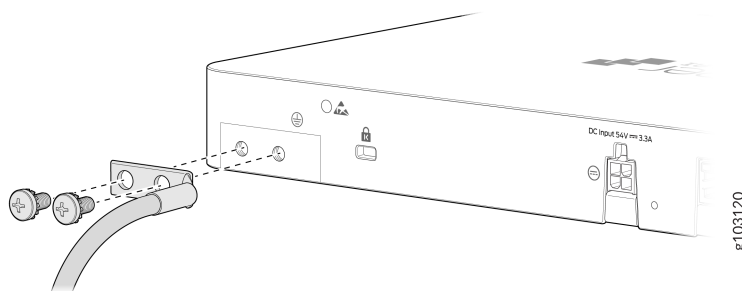
Before you connect an earth ground to the protective earthing terminal of the firewall, ensure that a licensed electrician attaches an appropriate grounding terminal to the grounding cable you supply. Using a grounding cable with an incorrectly attached terminal can damage the firewall.



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

To ground the SRX400:

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 the chassis.
2. Ensure that all grounding surfaces are clean and brought to a bright finish before making the grounding connections.
3. Connect the 14 AWG grounding cable to a proper earth ground, such as the rack in which you mount the firewall.
4. Place the grounding cable terminal over the grounding point (sized for M5 X 9.5 grounding screws) on the rear of the chassis.



5. Secure the grounding cable terminal to the grounding point with the two M5 X 9.5 screws. Apply between 2.5 Nm and 2.8 Nm of torque to the screw.
6. 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 SRX400

Ensure that you have a power cord appropriate for your geographical location.

For information about the supported AC power cord specifications for your firewall, see ["SRX400 Firewalls Power System" on page 25](#).

To connect the power cord:

1. Wrap and fasten one end of the electrostatic discharge (ESD) grounding strap around your bare wrist, and connect the other end to a site ESD point or to the ESD point on the chassis.
2. Locate the AC power cord shipped with the firewall; the cord has plug appropriate for your geographical location.

3. Insert the AC power cord coupler firmly into the power cord inlet on the AC power adapter.
4. If the AC power source outlet has a power switch, turn it off.
5. Plug the AC power cord into an AC power source outlet.
6. The SRX400 models do not have a power switch and each device powers on as soon as you plug it in.

Power Off the SRX400

You can power off the SRX400 in one of the following ways:

- Graceful shutdown—Using the CLI—Use the `request system power-off` command.

The device 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.

- Forced shutdown—Unplug the power cord or switch off the power source.



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

Use the forced shutdown method as a last resort to recover the firewall if the firewall OS is not responding to the graceful shutdown method.

Connect the SRX400 Firewalls to the Network

SUMMARY

This topic guides you on how to connect your SRX400 Firewalls to the network.

IN THIS SECTION

- [Determine Transceiver Support for SRX400 Firewalls | 45](#)
- [Install a Transceiver | 45](#)

SRX400 Firewalls support eight 10/100/1000 BASE-T RJ45 and two 1GbE onboard small form-factor pluggable (SFP) transceiver LAN ports.

The transceivers for Juniper Networks firewalls are hot-removable and hot-insertable field-replaceable units (FRUs). You can remove and replace the transceivers without powering off the device or disrupting the device functions.



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



NOTE: Use shielded cables on all the ports to connect to the network.



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 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.



NOTE: After you insert a transceiver or after you change the media-type configuration, wait for 6 seconds for the interface to display operational commands.

Determine Transceiver Support for SRX400 Firewalls

The SRX400 firewalls have two 1GbE onboard small form-factor pluggable (SFP) transceiver ports. You can use the [Hardware Compatibility Tool](#) to find information about the pluggable transceivers and connector types supported by your Juniper Networks device. The tool also documents the optical and cable characteristics, where applicable, for each transceiver. You can search for transceivers by product—and the tool displays all the transceivers supported on that device—or by category, interface speed, or type. You can find the list of supported transceivers for SRX400 firewalls at <https://apps.juniper.net/hct/product/>.



CAUTION: If you face a problem running a Juniper Networks device that uses a third-party optic or cable, the Juniper Networks Technical Assistance Center (JTAC) can help you diagnose the source of the problem. Your JTAC engineer might recommend that you check the third-party optic or cable and potentially replace it with an equivalent Juniper Networks optic or cable that is qualified for the device.

The I-temp and C-temp transceivers with various levels of power consumption on SRX400 support the following ambient temperature values:

- I-temp SFP transceivers drawing up to 1 W or 2.45 W operate normally between 32°F and 122°F (0°C to 50°C).
- C-temp SFP transceivers drawing up to 1 W or 2.45 W operate normally in the temperature range of 32°F through 104°F (0°C through 40°C).

Install a Transceiver

Before you install a transceiver in a device, ensure that you have taken the necessary precautions for the safe handling of lasers (see [Laser and LED Safety Guidelines and Warnings](#)).

Ensure that you have a rubber safety cap available to cover the transceiver.

[Figure 6 on page 46](#) shows how to install a QSFP+ transceiver. The installation procedure is same for all types of transceivers except the QSFP28 transceivers.



CAUTION: To prevent electrostatic discharge (ESD) damage to the transceiver, do not touch the connector pins at the end of the transceiver.

To install a transceiver:

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 device.
2. Remove the transceiver from its bag.
3. Check to see whether the transceiver is covered with a rubber safety cap. If it is not, cover the transceiver with a rubber safety cap.



LASER WARNING: Do not leave a fiber-optic transceiver uncovered except when inserting or removing a cable. The rubber safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.

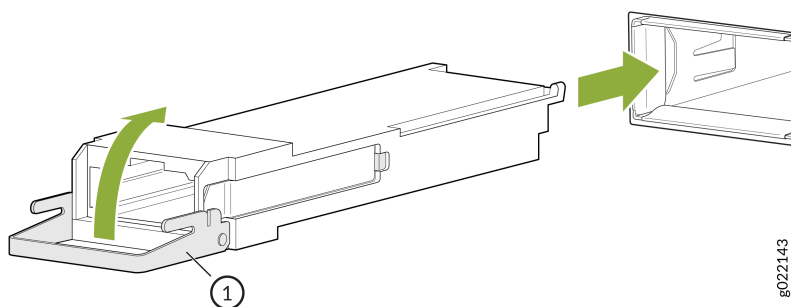
4. If the port in which you want to install the transceiver is covered with a dust cover, remove the dust cover. Save it in case you need to cover the port later. If you are hot-swapping a transceiver, wait for at least 10 seconds after removing the transceiver from the port before installing a new transceiver.
5. Using both hands, carefully place the transceiver in the empty port. The connectors must face the chassis.



CAUTION: Before you slide the transceiver into the port, ensure that the transceiver is aligned correctly to the port. Misalignment might cause the pins to bend, making the transceiver unusable.

6. Slide the transceiver in gently until it is fully seated. If you are installing a C form-factor pluggable (CFP) transceiver, use your fingers to tighten the captive screws on the transceiver.

Figure 6: Install a Transceiver



Connect a Fiber-Optic Cable

Before you connect a fiber-optic cable to an optical transceiver installed in a device, ensure that you have taken the necessary precautions for the safe handling of lasers (see [Laser and LED Safety Guidelines and Warnings](#)).



LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. Fiber-optic transceivers and fiber-optic cables connected to transceivers emit laser light that can damage your eyes.

To connect a fiber-optic cable to an optical transceiver installed in a device:

1. If the fiber-optic cable connector is covered with a rubber safety cap, remove the cap. Save the cap for subsequent use.
2. Remove the rubber safety cap from the optical transceiver. Save the cap for subsequent use.



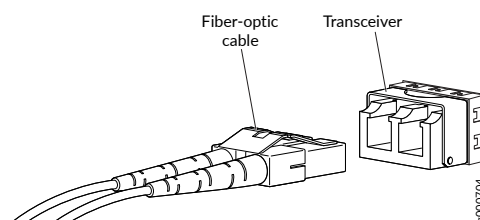
CAUTION: Do not leave a fiber-optic transceiver uncovered except when inserting or removing a cable. The safety cap keeps the port clean and protects your eyes from accidental exposure to laser light.



LASER WARNING: Do not look directly into a fiber-optic transceiver or into the ends of fiber-optic cables. The fiber-optic transceivers and the fiber-optic cables connected to a transceiver emit laser light that can damage your eyes.

3. Insert the cable connector into the optical transceiver.

Figure 7: Connect a Fiber-Optic Cable to an Optical Transceiver Installed in a Device



4. Secure the cable so that it does not support its own weight. Place excess cable out of the way in a neatly coiled loop. Placing fasteners on a loop helps cables maintain their shape.

If there is a cable management system, arrange the cable in the cable management system to prevent the cable from dislodging or developing stress points.



CAUTION: Do not bend fiber-optic cables beyond their minimum bend radius. An arc smaller than a few inches in diameter can damage the cables and cause problems that are difficult to diagnose.

Do not let fiber-optic cables hang free from the connector. Do not allow fastened loops of cables to dangle, which stresses the cables at the fastening point.

Perform Initial Software Configuration for SRX400 Firewall

IN THIS SECTION

- [Configure the SRX400 Using J-Web | 48](#)
- [Configure the SRX400 Firewall Using Juniper® Security Director Cloud | 50](#)
- [Access the CLI on the SRX400 | 50](#)
- [Configure Root Authentication and Management Interface from CLI | 50](#)
- [Factory-Default Configuration of the SRX400 | 52](#)
- [View the SRX400 Factory-Default Configuration | 53](#)

We ship the SRX400 Series Firewalls with preinstalled Junos OS Evolved, which is ready to be configured when you power on the device. You can use the J-Web GUI, Juniper® Security Director on Premise, Juniper® Security Director Cloud, or the CLI to perform the initial configuration.

For information about configuration and deployment procedures, see [Configuration Essentials: SRX400 Firewall Series](#).

Configure the SRX400 Using J-Web

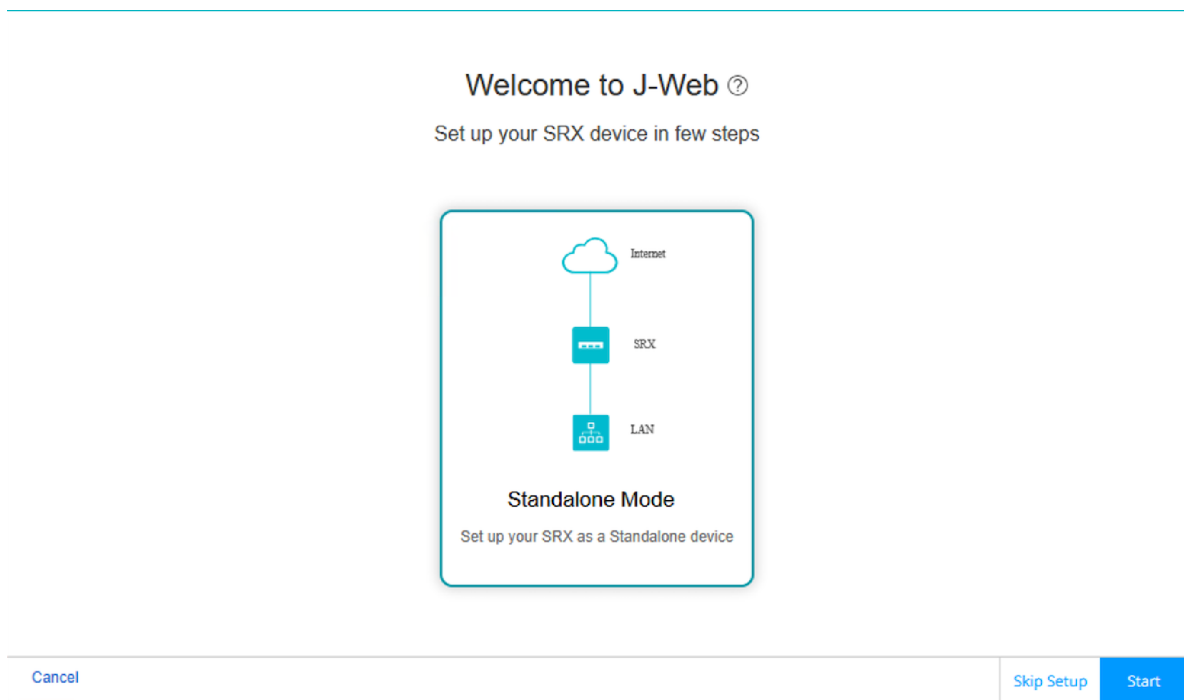
The J-Web interface is a Web-based graphical interface that allows you to operate a firewall without commands.

To access the J-Web interface on a new device that has the factory-default configuration:

1. Connect the management (**MGMT**) port (re0:mgmt-0) on your device to the Ethernet port on the management device (laptop or PC), using an RJ-45 cable. You can also use the network port **2** (ge-0/0/3) to connect to the management device.
2. Manually configure the management device with a compatible IP address in the 192.168.1.0 network (for example, 192.168.1.2). Do not use the 192.168.1.1 IP address for the management device as this IP address is assigned to the re0:mgmt-0 interface.
3. Run the following script to enable web-management.

```
sh /jail/html/includes/web_management_config_enable
```

4. Open a browser and enter **https://192.168.1.1** in the address bar.
The **J-Web Setup** page opens.



5. Using the **Standalone Mode** you can configure basic settings such as device credentials, time, management interface, zones and interfaces, and DNS servers and default gateways. Click **Start**.
The **Setup Wizard** page appears.
6. Follow the instructions in [Configure SRX Devices Using the J-Web Setup Wizard](#) to configure your device.

Configure the SRX400 Firewall 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.

Access the CLI on the SRX400

To access the CLI on your device:

1. Connect the management device to the serial console port as described in "[Connect the SRX400 Firewalls to External Devices](#)" on page 39.
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—115200
 - Parity—None
 - 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 SRX400 Firewalls to the Network](#)" on page 43.

Configure Root Authentication and Management Interface from 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 root. 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 re0:mgmt-0 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 applications j-web
```

```
[edit]  
root@# set system services web-management https system-generated-certificate
```

8. Commit the configuration changes.

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

Factory-Default Configuration of the SRX400

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 SRX400 Factory-Default Configuration

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@srx400>file list /etc/config
```

3. View the required default configuration file.

```
root@srx400>file show /etc/config/config-file-name
```

6

CHAPTER

Maintenance

IN THIS CHAPTER

- [Routine Maintenance Procedures for the SRX400 Firewalls](#) | **55**
-

Routine Maintenance Procedures for the SRX400 Firewalls

To maintain optimum performance of your router, perform the following preventative maintenance procedures on a regular basis.

- Inspect the installation site for moisture, loose wires or cables, and excessive dust.
- Check the System status LED on the front panel of the device.
- Check that the PSA status LED is lit for the DC power inputs.

7

CHAPTER

Troubleshooting and Support

IN THIS CHAPTER

- Troubleshoot the SRX400 Firewalls | **57**
 - Contact Customer Support and Return the Chassis or Components | **58**
-

Troubleshoot the SRX400 Firewalls

SUMMARY

This topic contains some common troubleshooting resources for the SRX400 Firewalls.

IN THIS SECTION

- [Troubleshooting Resources for SRX400 Firewalls | 57](#)
- [Use the RESET Button | 57](#)

Troubleshooting Resources for SRX400 Firewalls

Use the Junos OS Evolved CLI to identify alarms and troubleshoot the device. You can also contact the Juniper Networks® Technical Assistance Center (JTAC) for support.

- CLI—The CLI is the primary tool for controlling and troubleshooting hardware and network connectivity. CLI command outputs display information about network connectivity. You can use the CLI to see more information about alarm conditions.

For information about using the CLI to troubleshoot Junos OS Evolved, see the appropriate Junos OS Evolved 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.

Use the RESET Button

If a configuration fails or denies management access to the firewall, you can use the RESET button to restore the device.

The RESET button is recessed to prevent it from being pressed accidentally. To press the RESET button, insert a small probe (such as a straightened paper clip) into the pinhole on the front panel.

- Pressing the RESET button for a moment will load and commit the rescue configuration if it exists.

- Pressing and holding the RESET button for more than 15 seconds, the device will return to the rescue configuration if it exists else the factory-default configuration is committed.

Contact Customer Support and Return the Chassis or Components

SUMMARY

If you need to return a hardware component to Juniper Networks, Inc., you need a Return Material Authorization (RMA) number and the equipment serial number. Contact the Juniper Networks Technical Assistance Center (JTAC) to generate an RMA number. You may also need to locate the chassis or component details using the CLI or by referring to equipment labels. You then pack and ship the component.

IN THIS SECTION

- [Contact Customer Support | 58](#)
- [Return a Hardware Component to Juniper Networks | 59](#)
- [Locate the Serial Number of the SRX400 Firewalls | 60](#)
- [Request a Return Material Authorization | 60](#)
- [Guidelines for Packing and Shipping Hardware Components | 61](#)

Contact Customer Support

You can contact JTAC 24 hours a day, seven days a week.

Chat	Use the Ask me icon at the bottom right of the Support page. Don't see the Chat icon? Read this.
Web	Juniper Support Portal Government Support Portal

Telephone	U.S. and Canada (Toll-free): 1-888-314-JTAC (5822) Outside the US or Canada, use the relevant country number listed on the regional tabs listed on the Contact Support page. Federal Government Support: 1-833-900-1454
-----------	--



NOTE: We do not support opening new cases through e-mail. Please use one of the above options to contact JTAC.

Return a Hardware Component to Juniper Networks

If a hardware component fails, contact Juniper Networks to obtain an RMA number. We use this number to track the returned material at the factory and to return the repaired or new components to you, as needed.



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 number. Refused shipments are returned to you by collect freight.

To return a defective hardware component:

1. Determine the part number and the serial number of the defective component. See "[Locate the Serial Number of the SRX400 Firewalls](#)" on page 60.
2. Obtain an RMA number from JTAC as described in "[Request a Return Material Authorization](#)" on page 60.
3. Pack the component for shipment. See "[Guidelines for Packing and Shipping Hardware Components](#)" on page 61.

For more information about return and repair policies, see the **Support** page at <https://support.juniper.net/support/>.

Locate the Serial Number of the SRX400 Firewalls

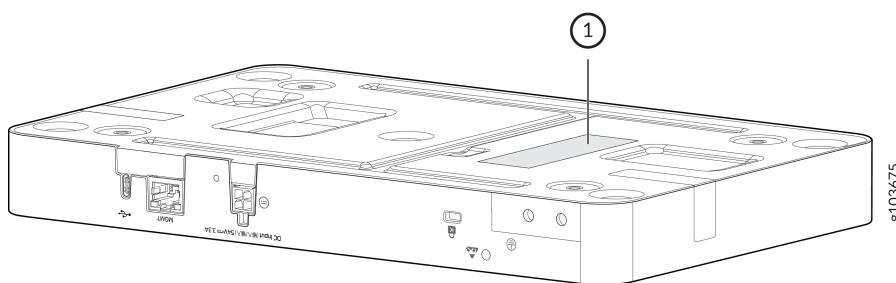
IN THIS SECTION

- [Locate the Chassis Serial Number ID Label](#) | 60

You can locate the serial number ID label on the device.

Locate the Chassis Serial Number ID Label

You can find the serial number on the bottom of the device.



1— Chassis Serial Number ID Label

Request a Return Material Authorization

If you are returning a device or hardware component to Juniper Networks for repair or replacement, obtain an RMA number from JTAC.

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

- Your existing service request number, if you have one
- Serial number of the device or component
- Your name, organization name, telephone number, fax number, and shipping address
- Details of the failure or problem
- Type of activity you were performing on the device when the problem occurred

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

You can contact JTAC using the [Support](#) page or by telephone.

If you're contacting JTAC by telephone:

- To report a new incident, press the star (*) key to be routed to the next available support engineer.
- To enquire about an existing case, enter your 12-digit service request number followed by the pound (#) key.

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

Guidelines for Packing and Shipping Hardware Components

When you return the chassis or components:

- Make sure to adequately protect them with packing materials. Pack them properly to prevent the pieces from moving around the carton.
- Use the original shipping materials, if they are available.
- Place the individual components in antistatic bags.
- Write the RMA number on the exterior of the box to ensure proper tracking.

8

CHAPTER

Safety and Compliance Information

IN THIS CHAPTER

- Safety | **63**
 - Agency Approvals for SRX400 Firewalls | **64**
-

Safety

IN THIS SECTION

- [Safety Information | 63](#)
- [Boot Time | 63](#)
- [Warning Statement for Shielded Intra-Building Criteria | 63](#)
- [Warning Statement for Unshielded Intra-Building Criteria | 63](#)

Safety Information

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 *SRX400 Firewalls* specific safety information provided in this hardware guide.

Boot Time

The boot time for SRX400 is 234 seconds.

Warning Statement for Shielded Intra-Building Criteria



WARNING: The intra-building port(s) of the equipment or subassembly must use shielded intra-building cabling or wiring that is grounded at both ends.

Warning Statement for Unshielded Intra-Building Criteria



WARNING: Certain ports of a device are designed for use as intra-building (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 requirements and protect against lightning surges and

commercial power disturbances, the intra-building ports must not be metalically connected to interfaces that connect to the OSP or its wiring. The intra-building ports on the device are suitable for connection to intra-building or unexposed wiring or cabling only. The addition of primary protectors is not sufficient protection for connecting these interfaces metalically to OSP wiring.

Agency Approvals for SRX400 Firewalls

IN THIS SECTION

- Agency Approvals | **64**
- Regulatory Compliance Information | **66**
- Compliance Statement for Canada | **66**
- Compliance Statement for Argentina | **67**
- Taiwan | **67**
- European Community | **67**
- Israel | **67**
- Japan | **67**
- Korea | **68**
- United States | **68**
- FCC Part 15 Statement | **68**

Agency Approvals

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 62368-1:2014 Audio/Video, Information and Communication Technology Equipment
- IEC 62368-1:2018 Audio/Video, Information and Communication Technology Equipment

- UL/CSA 62368-1:2019 Audio/Video, Information and Communication Technology Equipment
- IEC/EN 60825-1 Safety of Laser Products – Part 1: Equipment classification and requirements

EMC

- FCC 47 CFR Part 15
- ICES-003 / ICES-GEN
- BS EN 55032 213
- BS EN 55035
- EN 300 386 V1.6.1
- 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 15936
- KS C 9835
- KS C 9832
- KS C 9610

Environmental

- RoHS2, REACH and WEEE
- TSCA
- California Prop 65

- PFAS
- POPs
- China RoHS
- Taiwan RoHS

Regulatory Compliance Information

This product and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections as defined by the 802.3 at Standard. If you need further assistance with purchasing the power source, please contact Juniper Networks, Inc.

Compliance Statement for 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.

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

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，用戶請採取相應措施。

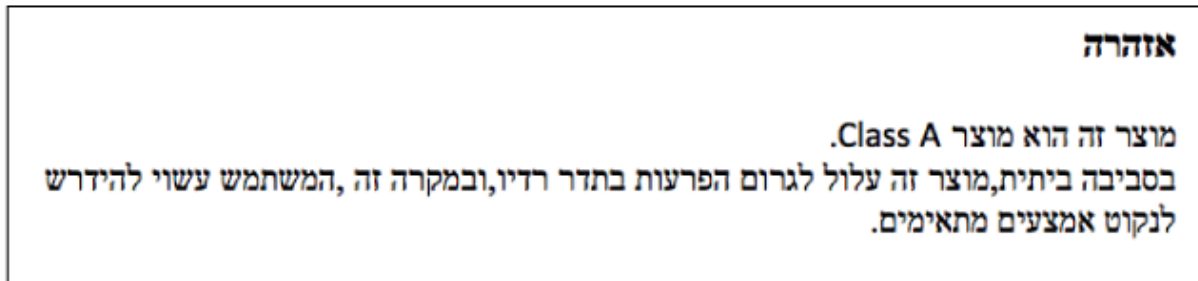
The preceding translates as follows:

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.

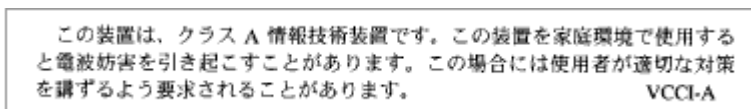
Israel



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



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.