JUNIPER NETWORKS | Engineering Simplicity

SRX345 Firewall Hardware Guide

Published
2023-08-15

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

SRX345 Firewall Hardware Guide
Copyright © 2023 Juniper Networks, Inc. All rights reserved.

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 | vii

1 Overview

SRX345 Firewall Overview | 2

- SRX345 Firewall Description | 2
- SRX345 Firewall Field Replaceable Units Overview | 3
- Benefits of the SRX345 Firewall | 3

SRX345 Chassis | 4

- SRX345 Firewall Chassis Overview | 4
- SRX345 Firewall Front Panel | 5
- SRX345 Firewall Back Panel | 10
- SRX345 Firewall Interface Modules Overview | 12

SRX345 Cooling System | 13

SRX345 Power System | 14

- SRX345 Firewall Power Supply | 15
- SRX345 Firewall Power Specifications and Requirements | 16
- SRX345 Firewall Supported AC Power Cords | 17

2 Site Planning, Preparation, and Specifications

SRX345 Site Preparation Checklist | 20

SRX345 Site Guidelines and Requirements | 22

- General Site Installation Guidelines for the SRX345 Firewall | 22
- SRX345 Firewall Environmental Specifications | 23
- SRX345 Firewall Electrical Wiring Guidelines | 23
- SRX345 Firewall Physical Specifications | 25
- SRX345 Firewall Clearance Requirements for Airflow and Hardware Maintenance | 25

Rack Requirements | 26

Cabinet Requirements | 26

SRX345 Transceiver Specifications and Pinouts | 27

SRX345 Transceiver Support | 28

RJ-45 Connector Pinouts for the SRX345 Firewall Ethernet Port | 28

RJ-45 Connector Pinouts for the SRX345 Firewall Console Port | 29

Mini-USB Connector Pinouts for the SRX345 Firewall Console Port | 30

3 **Initial Installation and Configuration**

SRX345 Installation Overview | 32

SRX345 Firewall Installation Overview | 32

SRX345 Firewall Autoinstallation Overview | 32

Unpacking and Mounting the SRX345 | 33

Unpacking the SRX345 Firewall | 34

Verifying Parts Received with the SRX345 Firewall | 35

Preparing the SRX345 Firewall for Rack-Mount Installation | 36

Installing the SRX345 Firewall into a Rack | 37

Connecting the SRX345 to Power | 38

Required Tools and Parts for Grounding the SRX345 Services Gateway | 39

Connecting the SRX345 Firewall Grounding Cable | 39

Connecting the SRX345 Firewall to an AC Power Supply | 41

Connecting the SRX345 Firewall to a DC Power Supply | 42

Powering On the SRX345 Firewall | 44

Powering Off the SRX345 Services Gateway | 45

Connecting the SRX345 to External Devices | 46

Connecting the Dial-Up Modem to the Console Port on the SRX345 Services Gateway | 46

Connecting to the SRX345 Firewall CLI Using a Dial-Up Modem | 47

Configuring Junos OS on the SRX345 | 48

SRX345 Firewall Factory-Default Settings | **48**

Initial Configuration Using the CLI | **51**

Connect to the Serial Console Port | **51**

Connect to the Mini-USB Console Port | **52**

Configure the SRX345 Using the CLI | **53**

Initial Configuration Using J-Web | **54**

Configure Using J-Web | **54**

Customize the Configuration for Junos OS Release 19.2 | **56**

Customize the Configuration for Junos OS Release 15.1X49-D170 | **57**

Configure the Device Using ZTP with Juniper Networks Network Service Controller | **58**

Installing the Optional SATA Solid-State Drive in SRX340 and SRX345 Services Gateways | 59

4 **Maintaining Components**

Maintaining the SRX345 Components | 65

Required Tools and Parts for Maintaining the SRX345 Firewall Hardware Components | **65**

Routine Maintenance Procedures for the SRX345 Services Gateway | **65**

Maintaining the SRX345 Firewall Cooling System Components | **66**

Maintaining the SRX345 Firewall Power Supply | **66**

Replacing Mini-Physical Interface Modules in the SRX345 Firewall | **67**

5 **Troubleshooting Hardware**

Troubleshooting the SRX345 | 69

Troubleshooting Resources for the SRX345 Firewall Overview | **69**

Troubleshooting Chassis and Interface Alarm Messages on the SRX345 Firewall | **69**

Troubleshooting the Power System on the SRX345 Firewall | **71**

Using the RESET CONFIG Button | **73**

Changing the RESET CONFIG Button Behavior | **73**

6 **Contacting Customer Support and Returning the Chassis or Components**

Returning the SRX345 Chassis or Components | 76

Contacting Customer Support | 76

Returning a SRX345 Firewall Component to Juniper Networks | 77

Locating the SRX345 Firewall Chassis Serial Number and Agency Labels | 77

Locating the Mini-PIM Serial Number Label | 78

Listing the SRX345 Firewall Component Details with the CLI | 78

Required Tools and Parts for Packing the SRX Series Services Gateway | 78

Packing the SRX Series Services Gateway for Shipment | 79

Packing SRX Series Services Gateway Components for Shipment | 79

7 Safety and Compliance Information

Definitions of Safety Warning Levels | 82

General Safety Guidelines and Warnings | 83

Restricted Access Warning | 85

Qualified Personnel Warning | 86

Prevention of Electrostatic Discharge Damage | 87

Fire Safety Requirements | 88

Laser and LED Safety Guidelines and Warnings | 90

Radiation from Open Port Apertures Warning | 92

Maintenance and Operational Safety Guidelines and Warnings | 93

Action to Take After an Electrical Accident | 99

General Electrical Safety Guidelines and Warnings | 99

AC Power Electrical Safety Guidelines | 100

DC Power Electrical Safety Guidelines | 101

SRX345 Firewall Agency Approvals | 108

SRX345 Firewall Acoustic Noise Compliance Statements | 110

SRX345 Firewall EMC Requirements | 110

About This Guide

Use this guide to install hardware and perform initial software configuration, routine maintenance, and troubleshooting for the SRX345 Firewall. After completing the installation and basic configuration procedures covered in this guide, refer to the Junos OS documentation for information about further software configuration.

RELATED DOCUMENTATION

- Day One+ for SRX345 (Quick Start)
- SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference
- Wi-Fi Mini-PIM Installation Guide
- LTE Mini-PIM and Antenna Installation Guide

1

CHAPTER

Overview

SRX345 Firewall Overview | 2

SRX345 Chassis | 4

SRX345 Cooling System | 13

SRX345 Power System | 14

SRX345 Firewall Overview

IN THIS SECTION

- SRX345 Firewall Description | 2
- SRX345 Firewall Field Replaceable Units Overview | 3
- Benefits of the SRX345 Firewall | 3

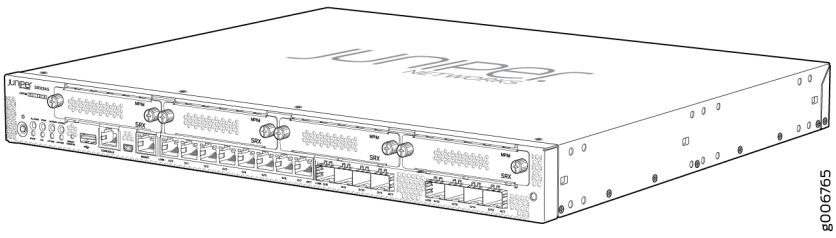
SRX345 Firewall Description

The SRX345 Firewall consolidates security, routing, switching, and WAN interfaces for midsize distributed enterprises. With advanced threat mitigation capabilities, the services gateway provides cost-effective and secure connectivity across distributed enterprises. The services gateway simplifies network complexity, protects and prioritizes network resources, and improves user and application experience.

The SRX345 Firewall has a capacity of 5 gigabits per second (Gbps) and is 1 rack unit (U) tall. The services gateway has eight 1 G Ethernet ports, eight 1 G SFP ports, one management port, 4 GB of DRAM memory, 8 GB of flash memory, and four Mini-Physical Interface Module (Mini-PIM) slots. The chassis installs in standard 800–mm (or larger) enclosed cabinets, 19 in. equipment racks, or telecommunications open-frame racks.

Figure 1 on page 2 shows the SRX345 Firewall.

Figure 1: SRX345 Firewall



The SRX345 Firewall runs the Junos operating system (Junos OS). The following are a few of the features supported:

- Firewall support with key features such as VPN
- Intrusion Detection and Prevention (IDP), AppSecure, and Content Security
- High availability
- QoS
- MPLS
- Juniper ATP Cloud
- MACsec support on all the ports (starting in Junos OS Release 15.1X49-D100)
- LTE support (starting in Junos OS Release 15.1X49-D100)
- Zero Touch Provisioning (starting in Junos OS Release 15.1X49-D100)

For more information about the features supported on SRX345 Services Gateways, see Feature Explorer.

You can manage the SRX345 Firewall by using the same interfaces that you use for managing other devices that run Junos OS—the CLI, the J-Web graphical interface, and Junos Space.

The SRX345 Firewall is available with a single AC power supply (Junos OS Release 15.1X49-D35 and later), dual AC power supplies (Junos OS Release 15.1X49-D110 and later), or a single DC power supply (Junos OS Release 17.4R1 and later).

SRX345 Firewall Field Replaceable Units Overview

Field-replaceable units (FRUs) are components that you can replace at your site. The Mini-Physical Interface Module (MPIM) is the only FRU on the SRX345 Firewall.

The Mini-PIMs are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

Benefits of the SRX345 Firewall

- **High performance**—The SRX345 supports up to 5-Gbps firewall and 800-Mbps IPsec VPN, and is suited for midsize to large distributed enterprise branch office deployments.

- **Simplified deployment with minimal manual intervention**—The Zero Touch Provisioning (ZTP) feature enables you to provision and configure the SRX300 line automatically, thereby reducing operational complexity and simplifying the provisioning of new sites.
- **Multiple WAN connectivity options**—The SRX345 supports multiple options such as Ethernet, serial, T1/E1, VDSL2, and 3G/4G LTE wireless for WAN or Internet connectivity to link sites.
- **Threat protection**—The SRX300 line supports IPsec VPN, Media Access Control Security (MACsec), Juniper Juniper Advanced Threat Prevention Cloud, and Trusted Platform Module (TPM) to protect against potential vulnerabilities.

RELATED DOCUMENTATION

SRX345 Installation Overview | 32

SRX345 Chassis

IN THIS SECTION

- SRX345 Firewall Chassis Overview | 4
- SRX345 Firewall Front Panel | 5
- SRX345 Firewall Back Panel | 10
- SRX345 Firewall Interface Modules Overview | 12

SRX345 Firewall Chassis Overview

The SRX345 Firewall chassis is a rigid sheet metal structure that houses all of the other services gateway components. The chassis installs in standard 800–mm (or larger) enclosed cabinets, 19 in. equipment racks, or telecommunications open-frame racks.



CAUTION: Before removing or installing components of a functioning services gateway, attach an electrostatic discharge (ESD) strap to an ESD point and place the other end of

the strap around your bare wrist. Failure to use an ESD strap could result in damage to the device.

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

SRX345 Firewall Front Panel

IN THIS SECTION

- Chassis Status LEDs | **8**
- Management Port LEDs | **9**
- Network Port LEDs | **10**

Figure 2 on page 5 shows the front panel of the SRX345 Firewall with a single AC or DC power supply.

Figure 2: SRX345 Firewall (Single AC or DC Power Supply) Front Panel

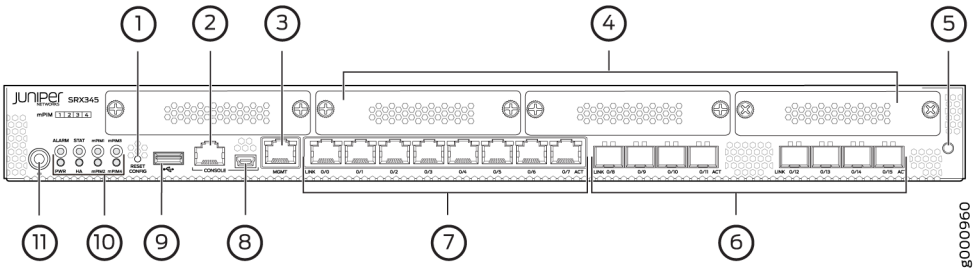


Figure 3 on page 6 shows the front panel of the SRX345 Firewall with dual AC power supplies.

Figure 3: SRX345 Firewall (Dual AC Power Supplies) Front Panel

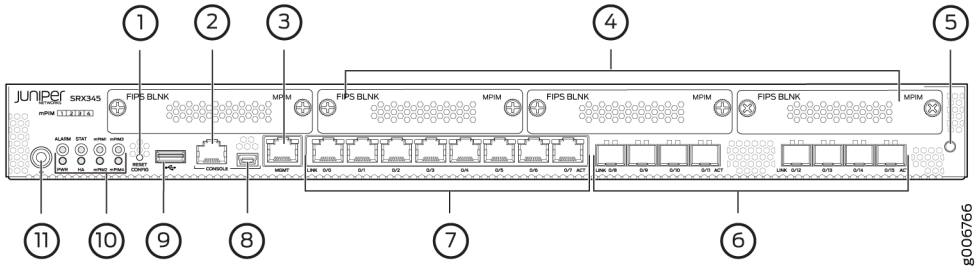


Table 1 on page 6 provides details about the front panel components.

Table 1: SRX345 Firewall Front Panel Components

Callout	Component	Description
1	Reset Config button	Returns the services gateway to the rescue configuration or the factory-default configuration.
2, 8	Console ports	• Serial—Connects a laptop to the services gateway for CLI management. The port uses an RJ-45 serial connection and supports the RS-232 (EIA-232) standard. • USB—Connects a laptop to the services gateway for CLI management through a USB interface. The port accepts a Mini-B type USB cable plug. A USB cable with Mini-B and Type A USB plugs is supplied with the services gateway. To use the mini-USB console port, you must download a USB driver to the management device from the Downloads page at https://www.juniper.net/support/downloads/?p=junos-srx#sw. To download the driver for Windows OS, select 6.5 from the **Version** drop-down list. To download the driver for Mac OS, select 4.10 from the **Version** drop-down list.
3	Management port	Use the management (MGMT) port to connect to the device over the network.

Table 1: SRX345 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
4	Mini-PIM slots	Four slots for Mini-PIMs. Mini-PIMs can be used to provide LAN and WAN functionality along with connectivity to various media types. **NOTE**: The SRX345 device with dual AC power supplies ships with tamper-proof labels.
5	ESD point	For personal safety, while working on the services gateway, use the ESD outlet to plug in an ESD grounding strap to prevent your body from sending static charges to the services gateway.
6	1-GbE small form-factor pluggable (SFP) ports	Eight 1-GbE MACsec-capable SFP ports for network traffic.
7	1-GbE Ethernet ports	Eight LAN ports (0/0 to 0/7), which are MACsec capable. The ports have the following characteristics: • Use an RJ-45 connector • Operate in full-duplex and half-duplex modes • Support autonegotiation The Gigabit Ethernet ports can be used to: • Function as front-end network ports • Provide LAN and WAN connectivity to hubs, switches, local servers, and workstations • Forward incoming data packets to the services gateway • Receive outgoing data packets from the services gateway
9	USB port	The services gateway has one USB port that accepts a USB storage device.
10	LEDs	Indicate component and system status at a glance.

Table 1: SRX345 Firewall Front Panel Components *(Continued)*

Callout	Component	Description
11	Power button	Use the Power button to power on or power off the services gateway.

Chassis Status LEDs

Figure 4 on page 8 shows the LEDs on the front panel.

Figure 4: SRX345 Firewall Front Panel LEDs

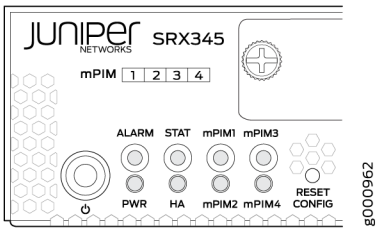


Table 2 on page 8 lists the front panel LEDs.

Table 2: SRX345 Firewall Front Panel LEDs

Component	Description
ALARM	• Solid amber (noncritical alarm) • Solid red (critical alarm) • Off (no alarms)
STAT	• Solid green (operating normally) • Solid red (error detected)

Table 2: SRX345 Firewall Front Panel LEDs *(Continued)*

Component	Description
PWR	• Solid green (receiving power) • Solid amber (Power-off triggered) • Off (no power)
HA	• Solid green (all HA links are available) • Solid amber (some HA links are unavailable) • Solid red (HA links are not functional) • Off (HA is disabled)
mPIM1 , mPIM2, mPIM3, and mPIM4	• Solid green (Mini-PIM is functioning normally) • Solid red (Mini-PIM hardware failure) • Off (Mini-PIM is not present or Mini-PIM is not detected by the device)

Management Port LEDs

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

Table 3 on page 9 describes the LEDs.

Table 3: Management Port LEDs

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

Table 3: Management Port LEDs *(Continued)*

LED	Description
Activity (LED on the right)	• Blinking green—There is activity on the link. • Off—There is no link activity.

Network Port LEDs

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

Table 4: Network Port LEDs

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

SRX345 Firewall Back Panel

Figure 5 on page 11 and Figure 6 on page 11 show the back panel of the SRX345 Firewall with a single AC power supply and dual AC power supplies, respectively.

Figure 5: SRX345 Firewall Back Panel (Single AC Power Supply)

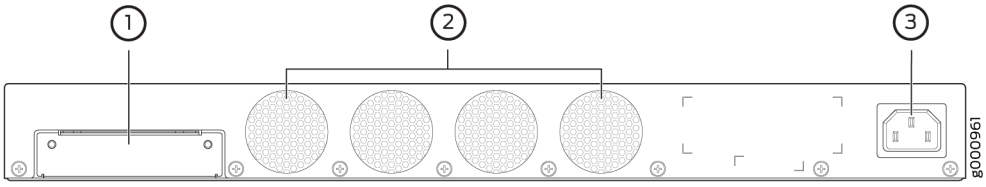


Figure 6: SRX345 Firewall Back Panel (Dual AC Power Supplies)

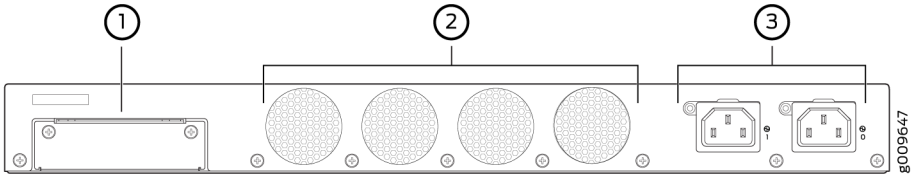


Figure 7 on page 11 shows the back panel of the SRX345 Firewall with a DC power supply.

Figure 7: SRX345 Firewall Back Panel (DC Power Supply)

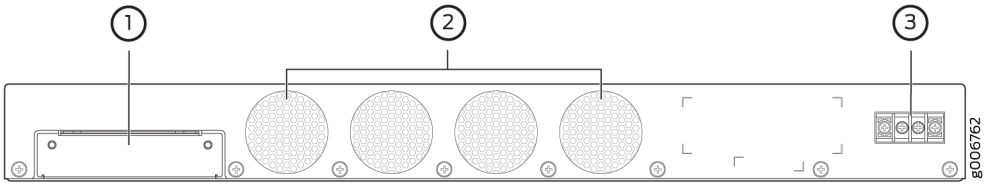


Table 5 on page 11 lists the components on the back panel.

Table 5: SRX345 Firewall Back Panel Components

Callout	Component	Description
1	SSD slot	SSD storage device slot for optional logging device.
2	Fans	Keeps all the services gateway components within the acceptable temperature range.

Table 5: SRX345 Firewall Back Panel Components *(Continued)*

Callout	Component	Description
3	Power supply input	Connects the services gateway to the AC power supply.

Table 6 on page 12 describes the LEDs on the AC power supplies for the SRX345 Firewall with dual AC power supplies.

Table 6: SRX345 Firewall (with Dual AC Power Supplies) Back Panel LEDs

LED Color	Description
Green	Receiving power
Off	No power

SRX345 Firewall Interface Modules Overview

Mini-Physical Interface Modules (Mini-PIMs) are field-replaceable network interface cards (NICs) supported on the SRX300 line of services gateways. You can easily insert or remove Mini-PIMs from the front slots of the services gateway chassis. The Mini-PIMs provide physical connections to a LAN or a WAN. The Mini-PIMs receive incoming packets from the network and transmit outgoing packets to the network. During this process, they perform framing and line-speed signaling for the medium type.

CAUTION: The Mini-PIMs are not hot-swappable. You must power off the services gateway before removing or installing Mini-PIMs.

The following Mini-PIMs are supported on the SRX345 Firewall:

- 1-Port Serial Mini-Physical Interface Module (SRX-MP-1SERIAL-R)
- 1-Port T1/E1 Mini-Physical Interface Module (SRX-MP-1T1E1-R)
- 1-Port VDSL2 (Annex A) Mini-Physical Interface Module (SRX-MP-1VDSL2-R)
- LTE Mini-Physical Interface Module (SRX-MP-LTE-AE and SRX-MP-LTE-AA)

- Wi-Fi Mini-Physical Interface Module (SRX-MP-WLAN-US, SRX-MP-WLAN-IL, and SRX-MP-WLAN-WW)

> **NOTE**: Gigabit-Backplane Physical Interface Modules (GPIMs) are not supported on the SRX345 Firewall.

For more information on the Mini-PIMs, see SRX300 Series and SRX550 High Memory Gateway Interface Modules Reference.

RELATED DOCUMENTATION

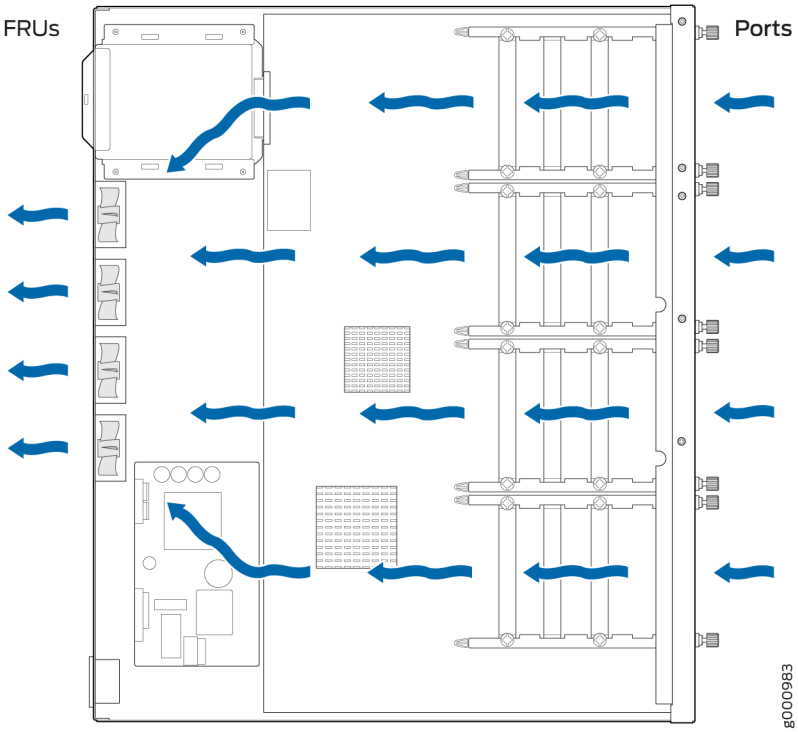
SRX345 Installation Overview | 32

SRX345 Cooling System

The cooling system for the SRX345 Firewall includes four fixed fans. The fans draw air through vents on the front of the chassis and exhaust the air through the back of the chassis. The airflow produced by the fans keeps device components within the acceptable temperature range.

Figure 8 on page 14 shows the airflow through the SRX345 Firewall chassis.

Figure 8: Airflow Through the SRX345 Firewall Chassis



RELATED DOCUMENTATION

Maintaining the SRX345 Firewall Cooling System Components | 66

SRX345 Power System

IN THIS SECTION

- SRX345 Firewall Power Supply | 15
- SRX345 Firewall Power Specifications and Requirements | 16
- SRX345 Firewall Supported AC Power Cords | 17

SRX345 Firewall Power Supply

The SRX345 Firewall is available with either a single AC power supply (Junos OS Release 15.1X49-D35 and later), dual AC power supplies (Junos OS Release 15.1X49-D110 and later), or a single DC power supply (Junos OS Release 17.4R1 and later). The power supply distributes the different output voltages to the device components according to their voltage requirements. The power supply is fixed in the chassis and is not a field-replaceable unit.

To identify the SRX345 model, check the `Description` field in the output of the `show chassis hardware` command.

The following are sample outputs for the different SRX345 models..

- **SRX345 with single AC power supply**

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CZ2916AF0098      SRX345
Routing Engine   REV 0x07 650-065042   CZ2916AF0098      RE-SRX345
FPC 0                                                    FPC
  PIC 0                                                  8xGE,8xGE SFP Base PIC
Power Supply 0
```

- **SRX345 with single DC power supply**

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                DT1917AF0037      SRX345-DC
Routing Engine   REV 0x01 650-073731   DT1917AF0037      RE-SRX345-DC
FPC 0                                                    FPC
  PIC 0                                                  8xGE,8xGE SFP Base PIC
Power Supply 0
```

- **SRX345 with dual AC power supplies**

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                DS2617AF0021      SRX345-DUAL-AC
```

```
Routing Engine   REV 0x03 650-073730   DS2617AF0021      RE-SRX345-DUAL-AC
FPC 0                                                  FPC
  PIC 0                                                8xGE,8xGE SFP Base PIC
Power Supply 0
```

SEE ALSO

Maintaining the SRX345 Firewall Power Supply | 66

SRX345 Firewall Power Specifications and Requirements

The AC power system electrical specifications for the SRX345 Firewall are listed in Table 7 on page 16.

Table 7: Power System Electrical Specifications for the SRX345 Firewall (AC Models)

Power Requirement	Specification
AC input voltage	100 to 240 VAC
AC input line frequency	50 to 60 Hz
AC system current rating	1 to 1.5 A
Maximum AC inrush current	7.3 A at 220 V/50 Hz (with four Mini-PIMs installed)

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

The DC power system electrical specifications for the SRX345 Firewall are listed in Table 8 on page 17.

Table 8: Power System Electrical Specifications for the SRX345 Firewall (DC Model)

Power Requirement	Specification
Rated DC voltage range	–48 to –60 VDC (with -15% and +20% tolerance)
Operating voltage range	–40.8 to –72 VDC
DC system current rating	6 A at –48 VDC
DC output	12 V@150W

SRX345 Firewall Supported AC Power Cords

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

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

Table 9 on page 17 provides power cord specifications, and Figure 9 on page 18 depicts the plug on the AC power cord provided for each country or region.

Table 9: AC Power Cord Specifications

Country	Electrical Specification	Plug Standards
Australia	250 VAC, 10 A, 50 Hz	AS/NZ 3112-1993
China	250 VAC, 10 A, 50 Hz	GB2099.1 1996 and GB 1002 1996 (CH1-10P)

Table 9: AC Power Cord Specifications *(Continued)*

Country	Electrical Specification	Plug Standards
Europe (except Italy and United Kingdom)	250 VAC, 10 A, 50 Hz	CEE (7) VII
Italy	250 VAC, 10 A, 50 Hz	CEI 23-16/VII
Japan	125 VAC, 12 A, 50 or 60 Hz	JIS 8303
North America	125 VAC, 10 A, 60 Hz	NEMA 5-15
United Kingdom	250 VAC, 10 A, 50 Hz	BS 1363A

Figure 9: AC Plug Types



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

RELATED DOCUMENTATION

SRX345 Firewall Electrical Wiring Guidelines | 23

2

CHAPTER

Site Planning, Preparation, and Specifications

SRX345 Site Preparation Checklist | 20

SRX345 Site Guidelines and Requirements | 22

SRX345 Transceiver Specifications and Pinouts | 27

SRX345 Site Preparation Checklist

Table 10 on page 20 provides a checklist of tasks you need to perform when preparing a site for installing the SRX345 Firewall.

Table 10: Site Preparation Checklist for SRX345 Firewall Installation

Item or Task	Additional Information
Environment	
Verify that environmental factors such as temperature and humidity do not exceed device tolerances.	"SRX345 Services Gateway Environmental Specifications" on page 23
Power	
Measure the distance between the external power sources and the device installation site.	"SRX345 Services Gateway Electrical Wiring Guidelines" on page 23
Locate sites for connection of system grounding.	"Connecting the SRX345 Services Gateway Grounding Cable" on page 39
Calculate the power consumption and requirements.	"SRX345 Services Gateway Power Specifications and Requirements" on page 16
Rack Requirements	
Verify that your rack meets the minimum requirements.	*Rack Requirements*
Rack Installation	

Table 10: Site Preparation Checklist for SRX345 Firewall Installation *(Continued)*

Item or Task	Additional Information
Plan the rack location, including required space clearances.	"Preparing the SRX345 Services Gateway for Rack-Mount Installation" on page 36
Secure the rack to the floor and building structure.	
Cabinet Requirements	
Verify that your cabinet meets the minimum requirements.	*Cabinet Requirements*
Plan the cabinet location, including required space clearances.	
Cables	
• Acquire cables and connectors. • Review the maximum distance allowed for each cable. Choose the length of cable based on the distance between the hardware components being connected. • Plan the cable routing and management.	

RELATED DOCUMENTATION

General Site Installation Guidelines for the SRX345 Firewall | 22

SRX345 Site Guidelines and Requirements

IN THIS SECTION

- General Site Installation Guidelines for the SRX345 Firewall | 22
- SRX345 Firewall Environmental Specifications | 23
- SRX345 Firewall Electrical Wiring Guidelines | 23
- SRX345 Firewall Physical Specifications | 25
- SRX345 Firewall Clearance Requirements for Airflow and Hardware Maintenance | 25
- Rack Requirements | 26
- Cabinet Requirements | 26

General Site Installation Guidelines for the SRX345 Firewall

The following precautions help you plan an acceptable operating environment for your SRX345 Firewall and avoid environmentally caused equipment failures:

- For the cooling system to function properly, the airflow around the chassis must be unrestricted. Allow sufficient clearance between the front and back of the chassis and adjacent equipment. Ensure that there is adequate circulation in the installation location.
- Follow the ESD procedures to avoid damaging equipment. Static discharge can cause components to fail completely or intermittently over time. For more information, see *Prevention of Electrostatic Discharge Damage*.
- Ensure that a blank Mini-PIM panel is installed in the empty slot to prevent any interruption or reduction in the flow of air across internal components.

SRX345 Firewall Environmental Specifications

Table 11 on page 23 provides the required environmental conditions for normal SRX345 Firewall operations.

Table 11: Environmental Specifications for the SRX345 Firewall

Description	Value
Altitude	No performance degradation up to 10,000 ft (3048 m)
Relative humidity	5% to 95%, noncondensing
Temperature	• Operational temperature—32° F (0° C) to 104° F (40° C) • Nonoperational temperature—4° F (-20° C) to 158° F (70° C)
Average power consumption	122 W
Average heat dissipation	420 BTU/hr
Noise level	36.9 dBA

SRX345 Firewall Electrical Wiring Guidelines

Table 12 on page 24 describes the factors you must consider while planning the electrical wiring for the services gateway at your site.

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

Table 12: Site Electrical Wiring Guidelines for the SRX345 Firewall

Site Wiring Factor	Guideline
Signaling Limitations	To ensure that signaling functions optimally: • Install wires correctly. Improperly installed wires can emit radio interference. • Do not exceed the recommended distances or pass wires between buildings. The potential for damage from lightning strikes increases if wires exceed recommended distances or if wires pass between buildings. • Shield all conductors. The electromagnetic pulse (EMP) caused by lightning can damage unshielded conductors and destroy electronic devices.
Radio Frequency Interference (RFI)	To reduce or eliminate the emission of RFI from your site wiring: • Use twisted-pair cable with a good distribution of grounding conductors. • Use a high-quality twisted-pair cable with one ground conductor for each data signal when applicable, if you must exceed the recommended distances.
Electromagnetic Compatibility (EMC)	Provide a properly grounded and shielded environment and use electrical surge-suppression devices. Strong sources of electromagnetic interference (EMI) can cause the following damage: • Destroy the signal drivers and receivers in the device • Conduct power surges over the lines into the equipment, resulting in an electrical hazard **NOTE**: If your site is susceptible to problems with EMC, particularly from lightning or radio transmitters, you may want to seek expert advice.

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

SRX345 Firewall Physical Specifications

Table 13 on page 25 lists the physical specifications for the services gateway.

Table 13: Physical Specifications for the SRX345 Firewall

Physical Specification of Chassis	With Single AC Power Supply	With Dual AC Power Supplies	With Single DC Power Supply
Depth	14.57 in. (37.01 cm)	18.70 in. (47.50 cm)	14.57 in. (37.01 cm)
Width	17.36 in. (44.09 cm)	17.36 in. (44.09 cm)	17.36 in. (44.09 cm)
Height	1.72 in. (4.37 cm)	1.72 in. (4.37 cm)	1.72 in. (4.37 cm)
Weight	10.80 lb (4.90 kg)	14.34 lb (6.50 kg)	11.02 lb (5 kg)

SRX345 Firewall Clearance Requirements for Airflow and Hardware Maintenance

When planning the installation site for the SRX345 Firewall, you need to allow sufficient clearance around the device. Consider the following:

- For the operating temperature of the services gateway to be optimal, the airflow around the chassis must be unrestricted. The fan tray contains four fans and provides front-to-back chassis cooling.
- For service personnel to remove and install hardware components, there must be adequate space at the front and back of the device. Allow at least 24 in. (61 cm) both in front of and behind the device.

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

For information on the airflow through the SRX345 Firewall chassis, see "SRX345 Cooling System" on page 13.

Rack Requirements

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

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

- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.3 cm).
- The front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting ears.
- Maximum permissible ambient temperature when two devices are placed side by side in a 19 in. rack is 40° C.

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

- The holes within each rack set are spaced at 1 U (1.75 in. or 4.5 cm).
- The mounting brackets and front-mount flanges used to attach the chassis to a rack are designed to fasten to holes spaced at rack distances of 1 U (1.75 in.).
- The mounting holes in the mounting brackets provided with the device are spaced 1.25 in. (3.2 cm) apart (top and bottom mounting hole).

Always secure the rack in which you are installing the services gateway to the structure of the building. If your geographical area is subject to earthquakes, bolt the rack to the floor. For maximum stability, also secure the rack to ceiling brackets.

Cabinet Requirements

You can install the services gateway in a 19 in. (48.7 cm) cabinet as defined in Cabinets, Racks, Panels, and Associated Equipment (document number EIA-310-D) published by the Electronic Industries

Alliance (http://www.ecaus.org/eia/site/index.html). You must mount the services gateway horizontally in the cabinet using appropriate rack adapters.

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

- The cabinet is at least 1U (3.50 in. or 8.89 cm) and can accommodate the services gateway.
- The outer edges of the mounting brackets extend the width of either chassis to 19 in. (48.7 cm), and the front of the chassis extends approximately 0.5 in. (1.27 cm) beyond the mounting brackets.
- The minimum total clearance inside the cabinet is 30.7 in. (78 cm) between the inside of the front door and the inside of the rear door.

NOTE: A cabinet larger than the minimum required provides better airflow and reduces the chance of overheating.

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

- Ensure that the cool air supply you provide through the cabinet can adequately dissipate the thermal output of the services gateway.
- Install the services gateway as close as possible to the front of the cabinet so that the cable management system clears the inside of the front door. Installing the chassis close to the front of the cabinet maximizes the clearance in the rear of the cabinet for critical airflow.
- Route and dress all cables to minimize the blockage of airflow to and from the chassis.

RELATED DOCUMENTATION

SRX345 Installation Overview | 32

SRX345 Transceiver Specifications and Pinouts

IN THIS SECTION

SRX345 Transceiver Support | 28

- RJ-45 Connector Pinouts for the SRX345 Firewall Ethernet Port | 28
- RJ-45 Connector Pinouts for the SRX345 Firewall Console Port | 29
- Mini-USB Connector Pinouts for the SRX345 Firewall Console Port | 30

SRX345 Transceiver Support

You can find information about the pluggable transceivers supported on your Juniper Networks device by using the Hardware Compatibility Tool. In addition to transceiver and connector type, the optical and cable characteristics—where applicable—are documented for each transceiver. The Hardware Compatibility Tool enables you to search by product, displaying all the transceivers supported on that device, or category, by interface speed or type. The list of supported transceivers for the SRX345 is located at https://apps.juniper.net/hct/product/#prd=SRX345.

RJ-45 Connector Pinouts for the SRX345 Firewall Ethernet Port

Table 14 on page 28 describes the RJ-45 connector pinouts for the Ethernet port.

Table 14: RJ-45 Connector Pinouts for the SRX345 Firewall Ethernet Port

Pin	Signal
1	BI_DA+
2	BI_DA
3	BI_DB+
4	BI_DC+
5	BI_DC
6	BI_DB

Table 14: RJ-45 Connector Pinouts for the SRX345 Firewall Ethernet Port *(Continued)*

Pin	Signal
7	BI_DD+
8	BI_DD

RJ-45 Connector Pinouts for the SRX345 Firewall Console Port

Table 15 on page 29 describes the RJ-45 connector pinouts for the console port.

Table 15: RJ-45 Connector Pinouts for the SRX345 Firewall Console Port

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

Mini-USB Connector Pinouts for the SRX345 Firewall Console Port

The SRX345 Firewall has two console ports: an RJ-45 Ethernet port and a mini-USB Type-B port. If your management device (laptop or PC) does not have a DB-9 plug connector pin or an RJ-45 connector pin, you can connect your management device to the Mini-USB Type-B console port of the services gateway by using a cable that has a standard Type-A USB connector on one end and a Mini-USB Type-B (5-pin) connector on the other end. Table 16 on page 30 describes the Mini-USB Type-B connector pinouts for the console port.

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

Table 16: Mini-USB Type-B Connector Pinouts for the Services Gateway Console Port

Pin	Signal	Cable Color	Description
1	VCC	Red	+5 VDC
2	D-	White	Data -
3	D+	Green	Data +
X	N/C		Could be not connected (N/C), connected to ground (GND), or used as an attached device presence indicator
4	GND	Black	Ground

3

CHAPTER

Initial Installation and Configuration

SRX345 Installation Overview | 32

Unpacking and Mounting the SRX345 | 33

Connecting the SRX345 to Power | 38

Connecting the SRX345 to External Devices | 46

Configuring Junos OS on the SRX345 | 48

Installing the Optional SATA Solid-State Drive in SRX340 and SRX345 Services Gateways | 59

SRX345 Installation Overview

IN THIS SECTION

- SRX345 Firewall Installation Overview | 32
- SRX345 Firewall Autoinstallation Overview | 32

SRX345 Firewall Installation Overview

After you have prepared the site for installation and unpacked the SRX345 Firewall, you are ready to install the device. It is important to proceed through the installation process in the following order:

1. Review the safety guidelines explained in *General Electrical Safety Guidelines and Warnings*.
2. Prepare the services gateway for installation as described in "Preparing the SRX345 Services Gateway for Rack-Mount Installation" on page 36.
3. Install the services gateway as described in "Installing the SRX345 Services Gateway into a Rack" on page 37.
4. Connect cables to external devices.
5. Connect the grounding cable as described in "Connecting the SRX345 Services Gateway Grounding Cable" on page 39.
6. Power on the services gateway as described in "Powering On the SRX345 Services Gateway" on page 44.

SRX345 Firewall Autoinstallation Overview

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

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

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

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

NOTE: If the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

By issuing the `set system autoinstallation usb disable` command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

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

- Installation and Upgrade Guide for Security Devices
- Network Monitoring and Troubleshooting Guide

Unpacking and Mounting the SRX345

IN THIS SECTION

- Unpacking the SRX345 Firewall | 34
- Verifying Parts Received with the SRX345 Firewall | 35

Preparing the SRX345 Firewall for Rack-Mount Installation | 36
Installing the SRX345 Firewall into a Rack | 37

Unpacking the SRX345 Firewall

Ensure that you have the following parts and tools available:

- Phillips (+) screwdriver, number 2
- Blank panels to cover any slots not occupied by a component

The SRX345 Firewall is shipped in a cardboard carton and secured with foam packing material. The carton also contains an accessory box and quick start instructions.

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

To unpack the SRX345 Firewall:

1. Move the cardboard carton to a staging area as close to the installation site as possible, where you have enough room to remove the components from the chassis.
2. Position the cardboard carton with the arrows pointing up.
3. Carefully open the top of the cardboard carton.
4. Remove the foam covering the top of the services gateway.
5. Remove the accessory box.
6. Verify the parts received against the lists in "Verifying Parts Received with the SRX345 Services Gateway" on page 35.
7. Store the brackets and bolts inside the accessory box.
8. Save the shipping carton and packing materials in case you need to move or ship the services gateway at a later time.

Verifying Parts Received with the SRX345 Firewall

The SRX345 Firewall shipment package contains a packing list. Check the parts in the shipment against the items on the packing list. The packing list specifies the part numbers and carries a brief description of each part in your order.

If any part 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.

A fully configured services gateway contains the chassis with installed components, listed in Table 17 on page 35, and an accessory box, which contains the parts listed in Table 18 on page 36.

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

Table 17: Parts List for a Fully Configured SRX345 Firewall

Component	Quantity
SRX345 Firewall chassis (includes blank covers for Mini-PIM slots)	1
Mounting brackets	2
Mounting screws to attach the mounting brackets to the chassis	8
USB console cable with Type-A and Mini-B USB plugs	1
Power cord appropriate for your geographical location	1 (for services gateways with a single AC power supply) 2 (for services gateways with dual AC power supplies)

Table 18: Accessory Parts List for the SRX345 Firewall

Part	Quantity
RoHS Card	1
End User License Agreement	1
Documentation Roadmap and Product Warranty	1

Preparing the SRX345 Firewall for Rack-Mount Installation

You can mount an SRX345 Firewall on four-post (telco) racks, enclosed cabinets, and open-frame racks. Center-mount racks are not supported.

Before mounting the SRX345 Firewall in a rack:

- Verify that the site meets the requirements described in "SRX345 Site Preparation Checklist" on page 20.
- Verify that you have the following parts available in your rack-mounting kit for the SRX345 Firewall:
  - Rack-mounting brackets
  - Eight mounting screws to attach the mounting brackets to the chassis of the services gateway
  - Four mounting screws to attach the mounting brackets to the rack rail
- Verify that the racks or cabinets meet the specific requirements described in SRX345 Services Gateway Rack Size and Strength Requirements.
- Place the rack or cabinet in its permanent location, allowing adequate clearance for airflow and maintenance, and secure it to the building structure. For more information, see SRX345 Services Gateway Cabinet Airflow Requirements.
- Remove the gateway chassis from the shipping carton. For unpacking instructions, see "Unpacking the SRX345 Services Gateway" on page 34.

Installing the SRX345 Firewall into a Rack

You can front-mount the SRX345 Firewall in a rack. Many types of racks are acceptable, including four-post (telco) racks, enclosed cabinets, and open-frame racks.

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

To install the services gateway in a rack:

1. Position a mounting bracket on each side of the chassis.
2. Use a number-2 Phillips (+) screwdriver to install the screws that secure the mounting brackets to the chassis. Use either the front mount position, as shown in Figure 10 on page 37, or the center mount position, as shown in Figure 11 on page 37.

Figure 10: Installing the Rack Mount Brackets (Front Mount Position)

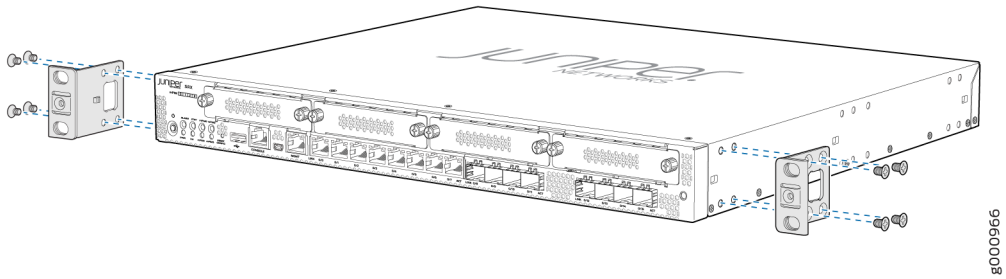
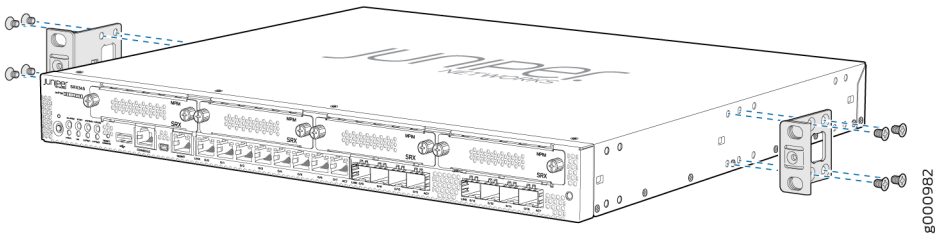


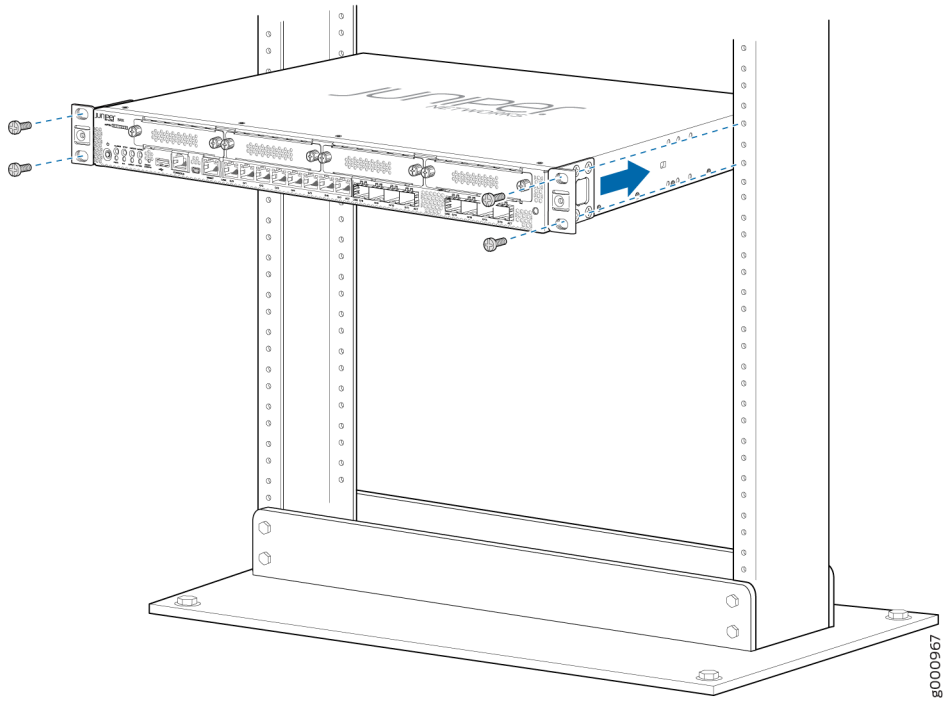
Figure 11: Installing the Rack Mount Brackets (Center Mount Position)



3. Have one person grasp the sides of the services gateway, lift it, and position it in the rack.
4. Align the bottom hole in each mounting bracket with a hole in each rack rail, making sure the chassis is level.
5. Have a second person install a mounting screw into each of the two aligned holes.

6. Install the second screw in each mounting bracket as shown in Figure 12 on page 38.

Figure 12: Installing the Services Gateway in the Rack (Front Mount Shown, Center Mount Similar)



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

RELATED DOCUMENTATION

- Configuring Junos OS on the SRX345 | **48**

Connecting the SRX345 to Power

IN THIS SECTION

- Required Tools and Parts for Grounding the SRX345 Services Gateway | **39**
- Connecting the SRX345 Firewall Grounding Cable | **39**

- Connecting the SRX345 Firewall to an AC Power Supply | **41**
- Connecting the SRX345 Firewall to a DC Power Supply | **42**
- Powering On the SRX345 Firewall | **44**
- Powering Off the SRX345 Services Gateway | **45**

Required Tools and Parts for Grounding the SRX345 Services Gateway

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

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

Connecting the SRX345 Firewall Grounding Cable

To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must connect the SRX345 Firewall to earth ground before you connect power to the services gateway.

You ground the services gateway by connecting a grounding cable to earth ground and then attaching it to the chassis grounding point located on the side of the device using two #10-32 UNF screws.

You must install the SRX345 in a restricted-access location and ensure that the chassis is always properly grounded. The SRX345 has a two-hole protective grounding terminal provided on the chassis. See Figure 13 on page 40. Under all circumstances, use this grounding connection to ground the chassis. For AC-powered systems, you must also use the grounding wire in the AC power cord along with the two-hole grounding lug connection. This tested system meets or exceeds all applicable EMC regulatory requirements with the two-hole protective grounding terminal.

You must provide the following items:

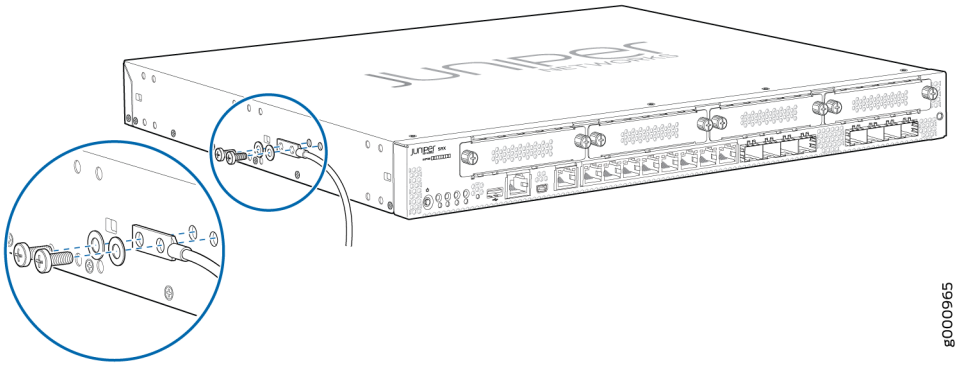
- Screws to secure the grounding lug: Two #10-32 UNF screws, with recommended length of 6 mm through 8 mm
- Grounding cable: #14 - #10 AWG or as permitted by the local code
- Cable lug: Panduit LCD10-10A-L or equivalent

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

To ground the device:

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

Figure 13: Connecting the Grounding Cable to the SRX345 Firewall



5. Secure the grounding cable lug to the grounding point, first with the washer, then with the screws.
6. Dress the grounding cable and verify that it does not touch or block access to the services gateway components and that it does not drape where people could trip on it.

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

Connecting the SRX345 Firewall to an AC Power Supply

You connect AC power to the services gateway by attaching a power cord from the AC power source to the AC appliance inlet located on the power supply faceplate. To connect the device to the power supply:

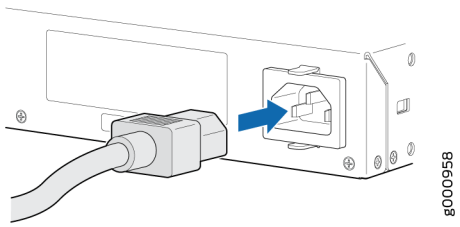
NOTE: The services gateway must be connected to earth ground during normal operation. The protective earthing terminal on the side of the chassis is provided to connect the services gateway to ground.

1. Attach an electrostatic discharge (ESD) grounding strap to your bare wrist, and connect the other end of the ESD strap to the ESD point on the rack.
2. Insert the appliance coupler end of the power cord into the appliance inlet on the power supply faceplate.

   NOTE: We strongly recommend that you use only the 3-prong power cord supplied with your services gateway.

3. Insert the power cord plug into an external AC power source receptacle as shown in Figure 14 on page 41. Verify that the power cord does not block the air exhaust and access to services gateway components or drape where people could trip on it.

Figure 14: Connecting the SRX345 Firewall to an AC Power Supply



4. If you are using a SRX345 Firewall with dual AC power supplies, then repeat steps 1 through 3 for the second power supply.

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

Connecting the SRX345 Firewall to a DC Power Supply

You connect DC power to the services gateway by attaching power cables from the external DC power sources to the terminal studs on the rear panel of the services gateway.

WARNING: To meet safety and electromagnetic interference (EMI) requirements and to ensure proper operation, you must properly ground the services gateway chassis before connecting power. See "Connecting the SRX345 Services Gateway Grounding Cable" on page 39 for instructions.

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

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

To connect the DC source power cables to the services gateway:

1. Switch off the dedicated facility circuit breakers. Ensure that the voltage across the DC power source cable leads is 0 V and that there is no chance that the cable leads might become active during installation.
2. Remove the clear plastic cover that protects the terminal studs.
3. Verify that the DC power cables are correctly labeled before making connections to the power supply.

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

4. Install heat-shrink tubing insulation around the power cables:

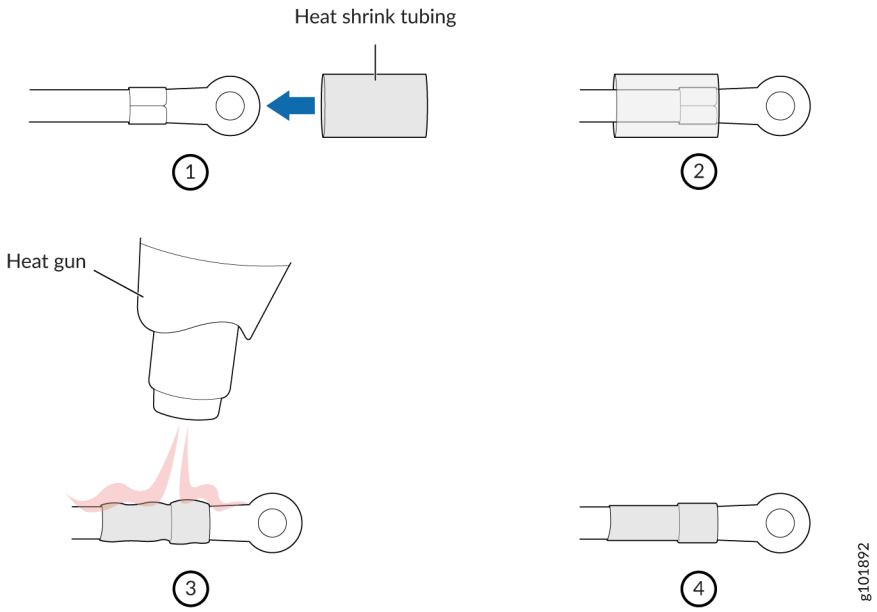
   a. Slide the tubing over the portion of the cable where it is attached to the lug barrel. Ensure that the tubing covers the end of the wire and the barrel of the lug attached to it.

   b. Shrink the tubing with a heat gun. Ensure that you heat all sides of the tubing evenly so that it shrinks around the cable tightly.

   NOTE: Do not overheat the tubing.

   Figure 15 on page 43 shows how to install heat-shrink tubing.

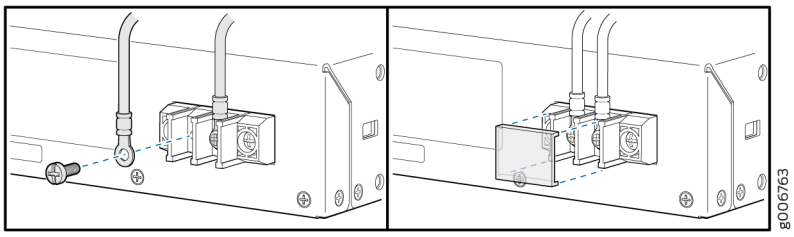
Figure 15: How to Install Heat-Shrink Tubing



5. Remove the screws and square washers from the terminals, using a Phillips (+) screwdriver, number 2.
6. Secure each power cable lug to the terminals with the square washers and the screws. Apply between 23 lb-in. (2.6 Nm) and 25 lb-in. (2.8 Nm) of torque to each screw. See Figure 16 on page 44

   - Secure the positive (+) DC source power cable lug to the **+** (return) terminal.
   - Secure the negative (–) DC source power cable lug to a **–** (input) terminal.

Figure 16: Connecting the SRX345 Firewall to a DC Power Supply



7. Replace the clear plastic cover over the terminal studs on the faceplate.
8. Verify that the power cables are connected correctly, that they do not touch or block access to services gateway components, and they do not cause a tripping hazard.

Powering On the SRX345 Firewall

To power on the services gateway:

1. Insert the power cord plug into the AC power source receptacle.
2. Turn on the power to the AC power receptacle. Observe the power supply faceplate LED. If the power supply is installed correctly and functioning normally, the LED glows steady green.
3. If you are using a SRX345 Firewall with dual AC power supplies, then repeat steps 1 and 2 for the second power supply.

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

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

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

Powering Off the SRX345 Services Gateway

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

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

  CAUTION: Use the graceful shutdown method to power off or reboot the services gateway.

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

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

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

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

NOTE: To remove power completely from the device, unplug the power cord or switch off the AC power source.

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

The Power button on the services gateway is a standby power switch, which will not turn off the input power to the services gateway.

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

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

Connecting the SRX345 to External Devices

IN THIS SECTION

- Connecting the Dial-Up Modem to the Console Port on the SRX345 Services Gateway | **46**
- Connecting to the SRX345 Firewall CLI Using a Dial-Up Modem | **47**

Connecting the Dial-Up Modem to the Console Port on the SRX345 Services Gateway

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

1. Turn off power to the services gateway.
2. Turn off power to the modem.
3. Connect one end of the Ethernet cable into the console port on the services gateway.
4. Connect the other end of the CAT-5e cable (Ethernet cable) into the RJ-45 to DB-9 serial port adapter.
5. Connect the serial port adapter to a separately purchased DB-9 socket to DB-25 plug adapter or other adapter appropriate for your modem.
6. Plug the modem adapter into the DB-25 connector on the modem.
7. Connect the modem to your telephone network.
8. Turn on the power to the modem.
9. Power on the services gateway by pressing the Power button on the front panel. Verify that the PWR LED on the front panel turns green.

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

NOTE: We no longer include a DB-9 to RJ-45 cable or a DB-9 to RJ-45 adapter with a CAT5E copper cable as part of the device package. If you require a console cable, you can order it separately with the part number JNP-CBL-RJ45-DB9 (DB-9 to RJ-45 adapter with a CAT5E copper cable).

Connecting to the SRX345 Firewall CLI Using a Dial-Up Modem

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

1. Connect a modem at your remote location to a management device such as a PC or laptop computer.
2. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) on the PC or laptop computer.
3. Select the COM port to which the modem is connected (for example, COM1).
4. Configure the port settings :
   - Bits per second—9600
   - Data bits—8
   - Parity—None
   - Stop bits—1
   - Flow control—None
5. In the HyperTerminal window, enter **AT**.

   For more information on the AT commands, see the following topics:

   - Installation and Upgrade Guide for Security Devices
   - Network Monitoring and Troubleshooting Guide

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

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

   The services gateway login prompt appears.

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

Configuring Junos OS on the SRX345

IN THIS SECTION

- SRX345 Firewall Factory-Default Settings | **48**
- Initial Configuration Using the CLI | **51**
- Initial Configuration Using J-Web | **54**
- Configure the Device Using ZTP with Juniper Networks Network Service Controller | **58**

The services gateway is shipped with the Juniper Networks Junos operating system (Junos OS) preinstalled and ready to be configured when the device is powered on. You can perform the initial software configuration of the services gateway by using the browser-based setup wizard or by using the command-line interface (CLI).

SRX345 Firewall Factory-Default Settings

IN THIS SECTION

- How to View Factory-Default Settings | **50**

The SRX345 device is shipped with the following factory-default settings:

Table 19: Security Policies

Source Zone	Destination Zone	Policy Action
trust	trust	permit
trust	untrust	permit

Table 20: NAT Rules

Source Zone	Destination Zone	Policy Action
trust	untrust	Source NAT to untrust zone interface

Table 21: Ethernet Interfaces

Port Label	Interface	Security Zone	DHCP State	IP Address
0/0 and 0/15	ge-0/0/0 and ge-0/0/15	untrust	Client	Unassigned
0/1 to 0/14	VLAN Interface irb.0 (ge-0/0/1 to ge-0/0/14)	trust	Server	192.168.2.1/24
MGMT	fxp0		Server	192.168.1.1/24

Table 22: LTE Interfaces

Interface	Security Zone	IP Address
cl-1/0/0	N/A	N/A
dl0 (logical)	untrust	ISP assigned*

Only if the LTE Mini-PIM is present

The SRX345 device is shipped with the following services and protocols enabled by default:

Table 23: Services, Protocols, and Startup Mode

Services	Protocols	Device Startup Mode
SSH HTTPS NETCONF over SSH	RSTP (all interfaces)	Switching

To provide secure traffic, a basic set of screens are configured on the untrust zone.

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

How to View Factory-Default Settings

To view the factory-default settings on your device:

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

```
user@host> file list /etc/config
```

3. View the required default configuration file.

```
user@host> file show /etc/config/<config file name>
```

When you commit changes to the configuration, a new configuration file is created, which becomes the active configuration. If the current active configuration fails, you can use the `load factory-default` command to revert to the factory-default configuration.

Initial Configuration Using the CLI

IN THIS SECTION

- Connect to the Serial Console Port | 51
- Connect to the Mini-USB Console Port | 52
- Configure the SRX345 Using the CLI | 53

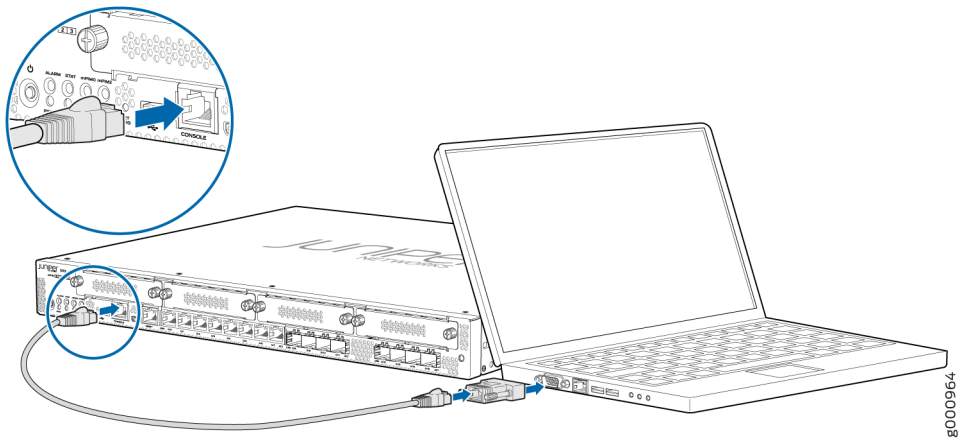
You can use either the serial or the mini-USB console port on the device.

Connect to the Serial Console Port

To connect to the serial console port:

1. Plug one end of the Ethernet cable into the RJ-45 to DB-9 serial port adapter.
2. Plug the RJ-45 to DB-9 serial port adapter into the serial port on the management device.
3. Connect the other end of the Ethernet cable to the serial console port on the SRX345.

Figure 17: Connect to the Console Port on the SRX345



4. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate COM port to use (for example, COM1).
5. Configure the serial port settings with the following values:
   - Baud rate—9600

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

Connect to the Mini-USB Console Port

To connect to the mini-USB console port:

1. Download the USB driver to the management device from the Downloads page. To download the driver for Windows OS, select **6.5** from the **Version** drop-down list. To download the driver for macOS, select **4.10** from the **Version** drop-down list.
2. Install the USB console driver software:

   > **NOTE**: Install the USB console driver software before attempting to establish a physical connection between the SRX345 and the management device, otherwise the connection will fail.

   a. Copy and extract the **.zip** file to your local folder.

   b. Double-click the **.exe** file. The installer screen appears.

   c. Click **Install**.

   d. Click **Continue Anyway** on the next screen to complete the installation.

      If you chose to stop the installation at any time during the process, then all or part of the software will fail to install. In such a case, we recommend that you uninstall the USB console driver and then reinstall it.

   e. Click **OK** when the installation is complete.
3. Plug the large end of the USB cable supplied with the SRX320 into a USB port on the management device.
4. Connect the other end of the USB cable to the mini-USB console port on the SRX345.
5. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the new COM port installed by the USB console driver software. In most cases, this is the highest-numbered COM port in the selection menu.

   You can locate the COM port under **Ports (COM & LPT)** in **Windows Device Manager** after the driver is installed and initialized. This might take several seconds.
6. Configure the port settings with the following values:

- Bits per second—9600
- Parity—None
- Data bits—8
- Stop bits—1
- Flow control—None

7. If you have not already done so, power on the SRX345 by pressing the **Power** button on the front panel. Verify that the **PWR** LED on the front panel turns green.

   The terminal emulation screen on your management device displays the startup sequence. When the SRX345 has finished starting up, a login prompt appears.

Configure the SRX345 Using the CLI

To configure the SRX345 by using the CLI:

1. Start the CLI.

```
root@%cli
root>
```

NOTE: You can view the factory-default settings by using the `show configuration` command.

2. Enter configuration mode.

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

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

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

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

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

Initial Configuration Using J-Web

IN THIS SECTION

- Configure Using J-Web | 54
- Customize the Configuration for Junos OS Release 19.2 | 56
- Customize the Configuration for Junos OS Release 15.1X49-D170 | 57

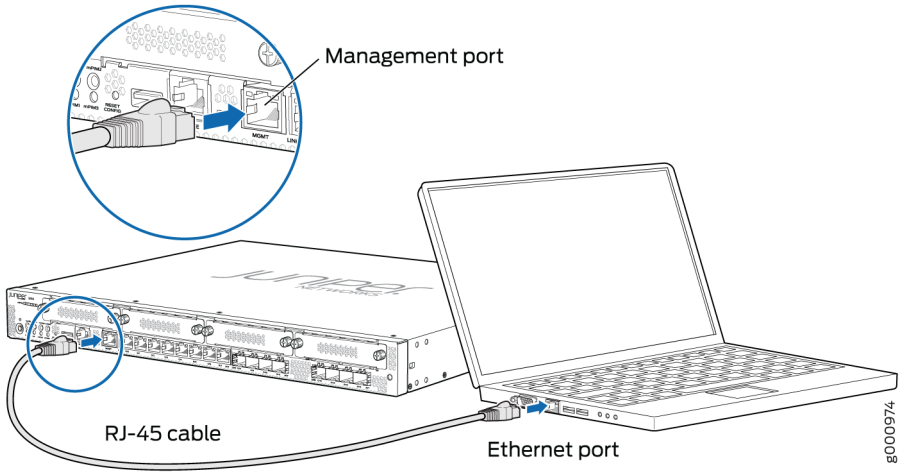
Configure Using J-Web

To configure the device by using J-Web:

1. Connect one end of the Ethernet cable to the management port (labeled **MGMT**) on the device.

   The ge-0/0/0 and ge-0/0/15 interfaces (ports **0/0** and **0/15**) are WAN interfaces. Do not use these ports for the initial configuration procedure.
2. Connect the other end of the Ethernet cable to the management device.

Figure 18: Connecting the SRX345 to a Management Device



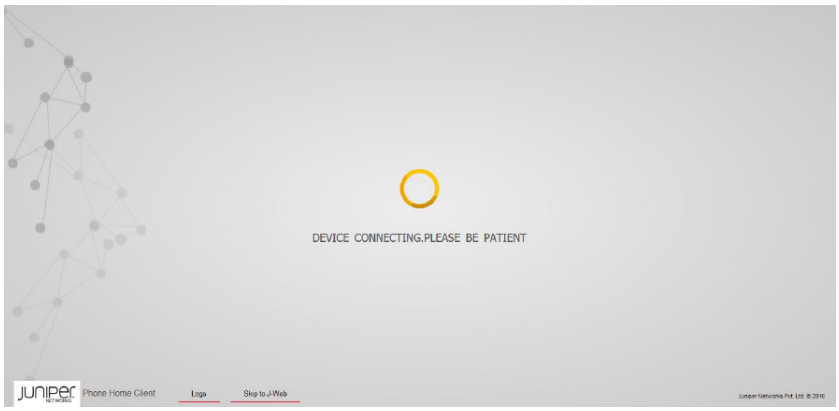
The SRX345 functions as a DHCP server and automatically assigns an IP address to the laptop.

3. Ensure that the management device acquires an IP address on the 192.168.1.0/24 network from the device.

   If an IP address is not assigned to the management device, manually configure an IP address in the 192.168.1.0/24 network.

   NOTE: Do not assign the 192.168.1.1 IP address to the management device, as this IP address is assigned to the services gateway.

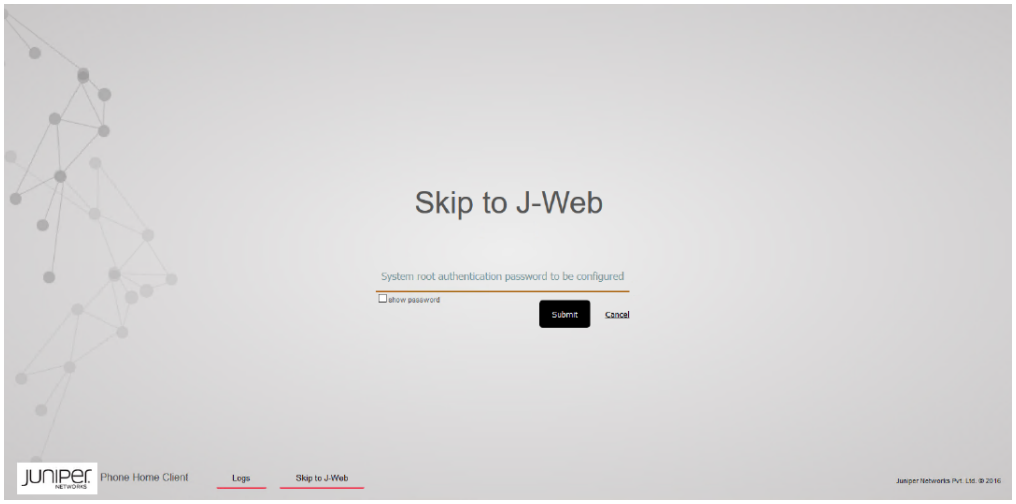
4. Open a browser and type https://192.168.1.1. The Phone Home Client page appears.



5. To configure the device:

   - Using zero-touch provisioning (ZTP)—Follow the procedure in "Configure the Device Using ZTP with Juniper Networks Network Service Controller" on page 58
   - Using J-Web—Click **Skip to J-Web**.

6. Set a root authentication password in the Skip to J-Web page and click **Submit**.



   The J-Web login page appears. The SRX345 already has factory-default settings configured to make it a plug-and-play device. So all you have to do to get the SRX345 up and running is connect it to your LAN and WAN networks.

7. Connect the WAN network to port **0/0** to obtain a dynamic IP address.
8. Connect the LAN network to any of the ports from **0/1** through **0/14**.
9. Check to see if the SRX345 is connected to the Internet. Go to http://www.juniper.net. If the page does not load, check the Internet connection.

   After you complete these steps, you can start using the SRX345 on your network right away.

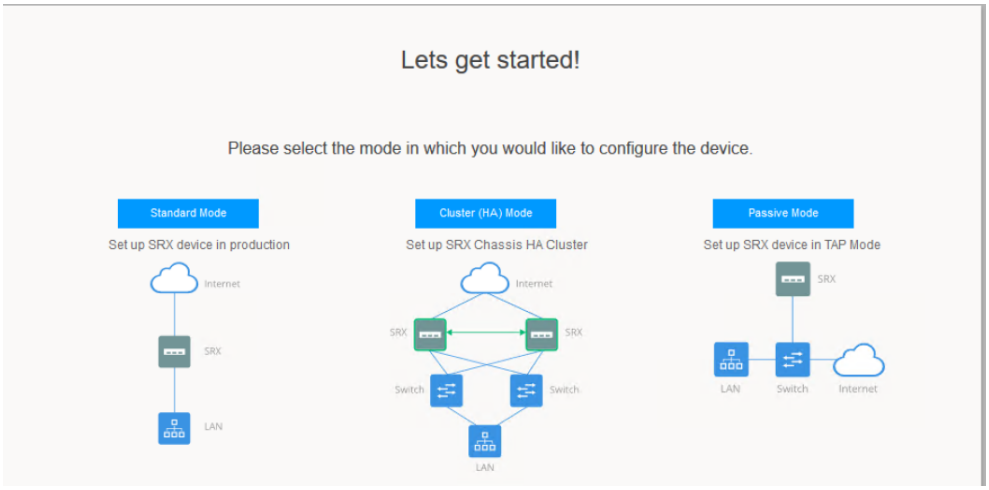
You can continue to customize the settings by logging in to J-Web and selecting the configuration mode that's right for you. You can then follow the screens as they appear in the Setup wizard.

- To customize the configuration in Junos OS Release 19.2, see "Customize the Configuration for Junos OS Release 19.2" on page 56.
- To customize the configuration in Junos OS Release 15.1X49-D170, see "Customize the Configuration for Junos OS Release 15.1X49-D170" on page 57.

Customize the Configuration for Junos OS Release 19.2

You can select any one of the configuration modes to customize the configuration:

- Standard—Configure basic security settings for the SRX345.
- Cluster (HA)—Set up the SRX345 in chassis cluster mode.
- Passive—Set up the SRX345 in Tap mode. Tap mode enables the SRX345 to passively monitor traffic flows across a network.



Customize the Configuration for Junos OS Release 15.1X49-D170

You can select any one of the configuration modes to customize the configuration:

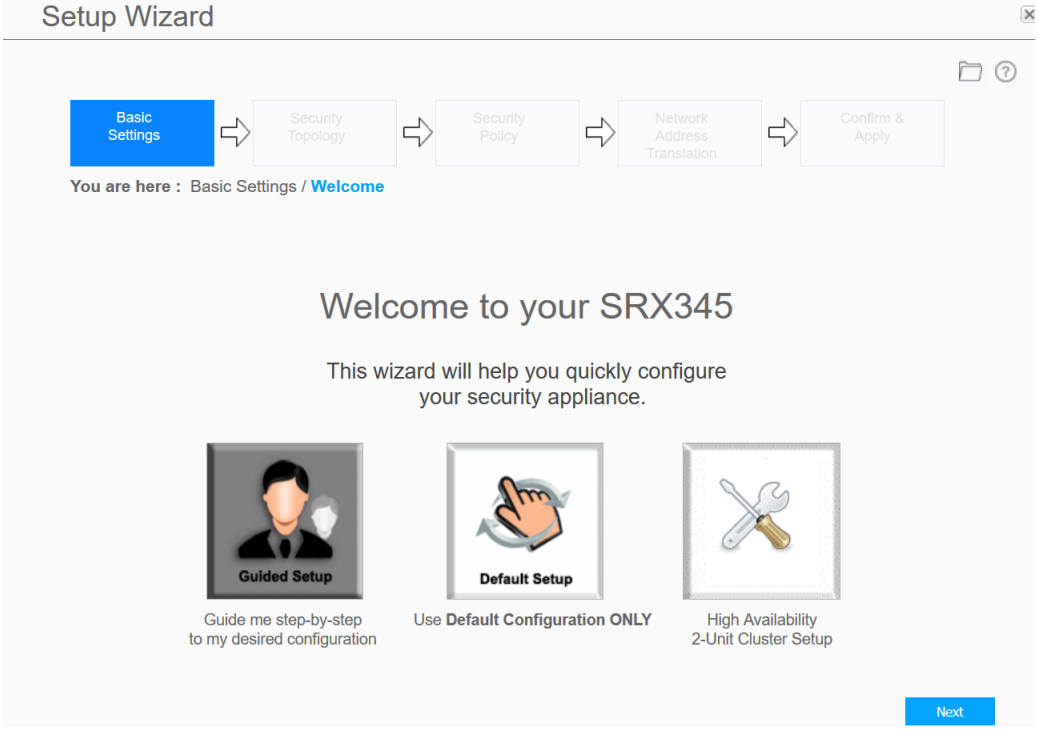
- Guided Setup (uses a dynamic IP address)—Enables you to set up the SRX345 in a custom security configuration. You can select either the Basic or the Expert option.

  The following table compares the Basic and Expert levels:

Options	Basic	Expert
Number of internal zones allowed	3	≥ 3
Internet zone configuration options	• Static IP • Dynamic IP	• Static IP • Static pool • Dynamic IP
Internal zone service configuration	Allowed	Allowed
Internal destination NAT configuration	Not Allowed	Allowed

NOTE: If you change the IP address of the port to which the laptop is connected, you might lose connectivity to the device when applying the configuration in the Guided Setup mode. To access J-Web again, open a new browser window and type https:// *new IP address*.

- Default Setup (uses a dynamic IP address)—Enables you to quickly set up the SRX345 with the default configuration. Any additional configuration can be done after the wizard setup is completed.
- High Availability—Enables you to set up a chassis cluster with a default basic configuration.



Configure the Device Using ZTP with Juniper Networks Network Service Controller

NOTE: You can configure using ZTP for Junos OS Release 19.2 and earlier releases.

You can use ZTP to complete the initial configuration of the SRX345 in your network automatically, with minimum intervention.

Network Service Controller is a component of the Juniper Networks Contrail Service Orchestration platform that simplifies and automates the design and implementation of custom network services that use an open framework.

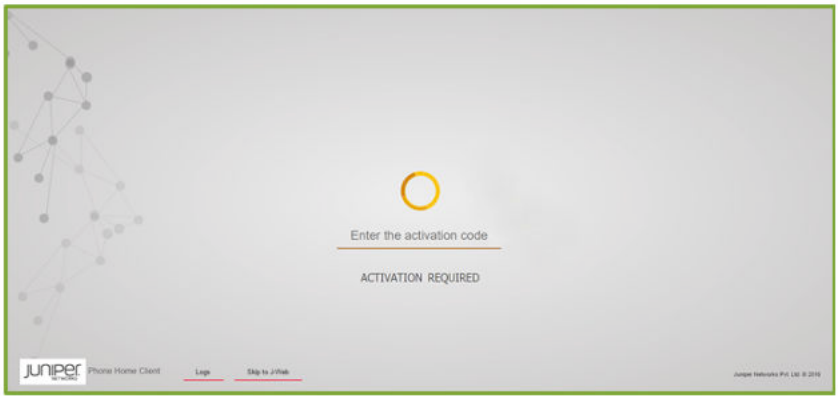
For more information, refer to the Network Service Controller section in the datasheet at http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000559-en.pdf.

To configure the device automatically using ZTP:

NOTE: To complete the ZTP process, ensure that the SRX345 is connected to the Internet.

- If you already have the authentication code, enter the code in the webpage displayed.

Figure 19: Authentication Code Page



On successful authentication, the initial configuration is applied and committed on the SRX345. Optionally, the latest Junos OS image is installed on the SRX345 before the initial configuration is applied.

- If you do not have the authentication code, you can use the J-Web setup wizard to configure the SRX345. Click **Skip to J-Web** and configure the SRX345 using J-Web.

Installing the Optional SATA Solid-State Drive in SRX340 and SRX345 Services Gateways

The SRX340 and SRX345 services gateways allows optional installation of a 100 GB serial advanced technology attachment (SATA) solid-state drive (SSD), which can be used for storing traffic log entries. The SATA SSD is not hot-swappable.

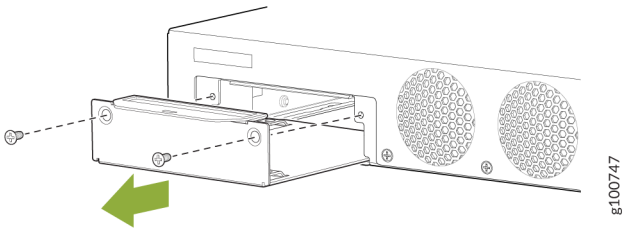
NOTE: Use only a Juniper-qualified SATA SSD.

Before you install the SSD, ensure that you have taken the necessary precautions to prevent electrostatic discharge (ESD) damage (see *Prevention of Electrostatic Discharge Damage*).

To install the SSD:

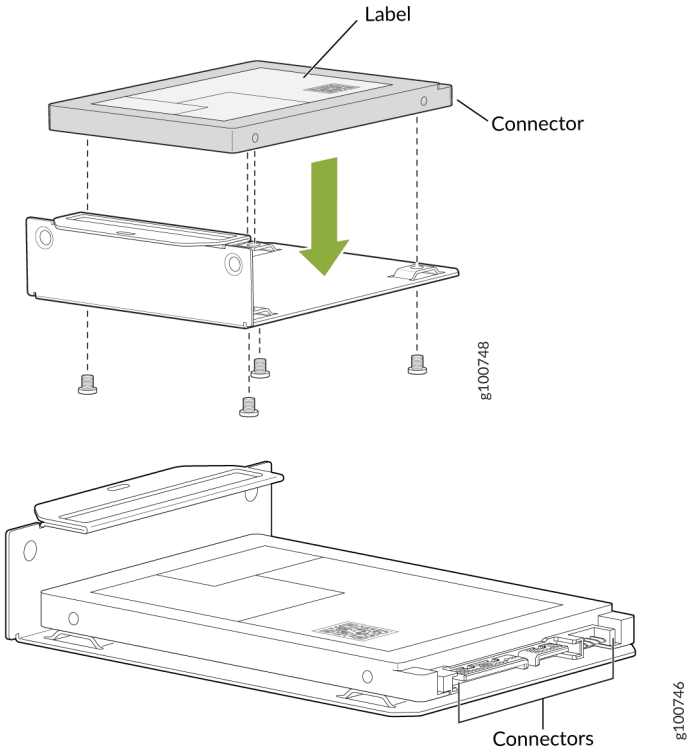
1. Power off the services gateway.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis.
3. Remove the two screws securing the SSD cover plate located on the rear panel, and remove the SSD tray from the slot.

Figure 20: Removing the SSD Tray



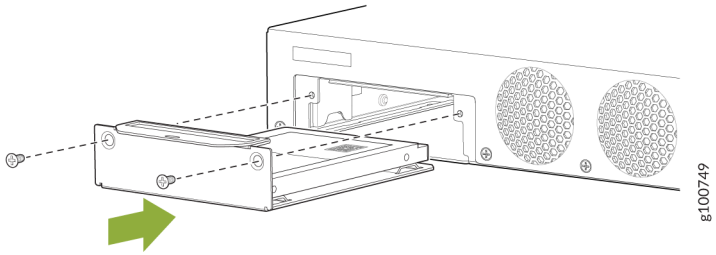
4. Place the SSD on the tray, with the label facing up. Secure the SSD to the tray by using four M3x6 mm screws. Apply between 4.5 in.-lb (0.51 N-m) and 6 in.-lb (0.67 N-m) of torque to each screw.

Figure 21: Securing the SSD to the SSD Tray



5. Slide the SSD tray into the slot and secure the cover plate.

Figure 22: Installing the SSD



6. Power on the services gateway.

   If the SSD is unformatted, the SSD is formatted during the bootup process. A single partition in the Unix (UFS) format is created, which occupies the entire SSD. The partition is mounted on the **/var/ssd** directory automatically. A symbolic link (symlink) from the **/mfs/var/traffic-log** directory to the **/var/ssd/traffic-log** directory is created.

7. Verify that the SSD information is displayed in the output of the `show chassis hardware detail` and `show system storage detail` commands.

```
user@host> show chassis hardware detail
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CZ2916AF0098      SRX345
Routing Engine   REV 0x07 650-065042   CZ2916AF0098      RE-SRX345
  da0    7718 MB  ATP CG eUSB                           Nand Flash
  ad0   95396 MB  SFSA100GQ1AA4TO-C-LB-21 000060158419A3000068 Hard Disk
  usb0 (addr 1)  product 0x0000 0      vendor 0x0000     uhub0
  usb0 (addr 2)  product 0x1000 4096   vendor 0x090c     umass0
FPC 0                                                   FPC
  PIC 0                                                 8xGE,8xGE SFP Base PIC
    Xcvr 12      REV 01   740-021308   AD154130TYA       SFP+-10G-SR
FPC 1            REV 01   650-073957   AG49041294        FPC
  PIC 0                                                 LTE for AA mPIM
FPC 2            REV 06   750-064613   BCAN2181          FPC
  PIC 0                                                 1x Serial mPIM (RoHS)
FPC 3            REV 09   750-064612   BCBB9371          FPC
  PIC 0                                                 1x VDSL2 mPIM (RoHS)
FPC 4            REV 06   750-064611   BCAZ1189          FPC
  PIC 0                                                 1x T1E1 mPIM (RoHS)
Power Supply 0
```

```
user@host> show system storage detail
Filesystem       1024-blocks       Used      Avail   Capacity   Mounted on
/dev/da0s1a           592690     400812     144464        74%  /
devfs                      1          1          0       100%  /dev
/dev/md0               20012      11884       6528        65%  /junos
/cf/packages          592690     400812     144464        74%  /junos/cf/packages
devfs                      1          1          0       100%  /junos/cf/dev
/dev/md1              1383532    1383532          0       100%  /junos
/cf                    20012      11884       6528        65%  /junos/cf
devfs                      1          1          0       100%  /junos/dev/
/cf/packages          592690     400812     144464        74%  /junos/cf/packages1
procfs                     4          4          0       100%  /proc
/dev/bo0s3e           189432         20     174258         0%  /config
/dev/bo0s3f          5239224      27584    4792504         1%  /cf/var
/dev/md2             1056324     100514     871306        10%  /mfs
```

```
/cf/var/jail          5239224      27584    4792504         1%  /jail/var
/cf/var/jails/rest-api    5239224      27584    4792504    1%  /web-api/var
/cf/var/log           5239224      27584    4792504         1%  /jail/var/log
devfs                       1          1          0       100%  /jail/dev
/dev/md3                 1884          4       1730         0%  /jail/mfs
/dev/ssd             96138198       3406   88443738         0%  /var/ssd
```

4

CHAPTER

Maintaining Components

Maintaining the SRX345 Components | 65

Maintaining the SRX345 Components

IN THIS SECTION

- Required Tools and Parts for Maintaining the SRX345 Firewall Hardware Components | 65
- Routine Maintenance Procedures for the SRX345 Services Gateway | 65
- Maintaining the SRX345 Firewall Cooling System Components | 66
- Maintaining the SRX345 Firewall Power Supply | 66
- Replacing Mini-Physical Interface Modules in the SRX345 Firewall | 67

Required Tools and Parts for Maintaining the SRX345 Firewall Hardware Components

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

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

Routine Maintenance Procedures for the SRX345 Services Gateway

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

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

Maintaining the SRX345 Firewall Cooling System Components

The services gateway fan controller works to maintain an optimal temperature for the services gateway. If the fan controller fails, the services gateway temperature will exceed the maximum working temperature and it will fail. Make sure that you maintain the recommended clearances behind the services gateway to enable the fan controller to function optimally.

Maintaining the SRX345 Firewall Power Supply

To maintain the power supplies of the services gateway:

- Make sure that all power cables are arranged so that they do not obstruct access to other services gateway components.
- Routinely check the POWER LED on the front panel. If this LED is solid green, the power supplies are functioning normally.

  NOTE: For SRX345 Services Gateways with dual AC power supplies, check the LEDs on the power supplies at the rear of the chassis. If the LEDs are solid green, then the power supplies are functioning normally.

- Periodically inspect the site to ensure that the power cables connected to the services gateway are securely in place and that there is no moisture accumulating near the services gateway.
- To check the status of the power supplies on an SRX345 Firewall with dual AC power supplies, use the `show chassis environment` or `show chassis hardware` command. The output is similar to the following:

```
user@host> show chassis environment
Class Item                          Status     Measurement
Temp  Routing Engine                OK         41 degrees C / 105 degrees F
      Routing Engine CPU            OK         76 degrees C / 168 degrees F
Fans  SRX345 Chassis fan 0          OK         Spinning at normal speed
      SRX345 Chassis fan 1          OK         Spinning at normal speed
      SRX345 Chassis fan 2          OK         Spinning at normal speed
      SRX345 Chassis fan 3          OK         Spinning at normal speed
```

```
Power Power Supply 0                Failed
      Power Supply 1                OK
```

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                DS2617AF0039      SRX345-DUAL-AC
Routing Engine   REV 0x03 650-073730   DS2617AF0039      RE-SRX345-DUAL-AC
FPC 0                                                    FPC
  PIC 0                                                  8xGE,8xGE SFP Base PIC
Power Supply 1
```

NOTE: If one of the power supplies on an SRX345 Firewall with dual AC power supplies has failed, the output of the `show chassis hardware` command displays only the power supply that is operational.

Replacing Mini-Physical Interface Modules in the SRX345 Firewall

The Mini-PIMs available on the SRX345 Firewall are not hot-swappable. You need to power off the device before removing or installing Mini-PIMs. For information on replacing Mini-PIMs, see the SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference.

SEE ALSO

SRX345 Firewall Field Replaceable Units Overview | 3

CHAPTER 5

Troubleshooting Hardware

Troubleshooting the SRX345 | 69

Troubleshooting the SRX345

IN THIS SECTION

- Troubleshooting Resources for the SRX345 Firewall Overview | 69
- Troubleshooting Chassis and Interface Alarm Messages on the SRX345 Firewall | 69
- Troubleshooting the Power System on the SRX345 Firewall | 71
- Using the RESET CONFIG Button | 73
- Changing the RESET CONFIG Button Behavior | 73

Troubleshooting Resources for the SRX345 Firewall Overview

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

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

Troubleshooting Chassis and Interface Alarm Messages on the SRX345 Firewall

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

Table 24 on page 70 describes alarms that can occur for an SRX345 Firewall chassis component.

Table 24: SRX345 Firewall Chassis Alarm Conditions and Corrective Actions

Component	Alarm Conditions	Action	Alarm Severity
Boot media	The services gateway boots from an alternate boot device.	• If the internal flash memory fails at startup, the services gateway automatically boots itself from the alternative boot device (USB storage device). **NOTE**: If you configured your services gateway to boot from an alternative boot device, ignore this alarm condition. • Reformat the internal flash memory and install a bootable image. (See the Installation and Upgrade Guide for Security Devices and Network Monitoring and Troubleshooting Guide for Security Devices) • If you did not configure the services gateway to boot from an alternative boot device, contact JTAC.	Amber (minor)
Hardware components on the services gateway	The services gateway chassis temperature or chassis is too warm	Check the room temperature. See "SRX345 Services Gateway Environmental Specifications" on page 23.	Amber (minor)
	The services gateway temperature is too high, either because of an internal overheating condition or because the maximum recommended room temperature has been exceeded.	The services gateway shuts down automatically in 4 minutes.	Red (major)

Table 24: SRX345 Firewall Chassis Alarm Conditions and Corrective Actions *(Continued)*

Component	Alarm Conditions	Action	Alarm Severity
Mini-PIM	A Mini-PIM has failed.	• Contact the Juniper Networks Technical Assistance Center (JTAC). • If you must replace the failed Mini-PIM, see SRX300 Series and SRX550 High Memory Services Gateway Interface Modules Reference for information about replacing the Mini-PIMs.	Red (major)

Troubleshooting the Power System on the SRX345 Firewall

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

Table 25 on page 71 describes different PWR LED status settings and their corrective actions.

Table 25: SRX345 Firewall Power LED Status

LED Status	Meaning	Possible Cause and Corrective Action
Green	Device is receiving power.	Normal indication. No action is required.
Amber	Indicates that the power button has been pressed and quickly released.	Normal indication. No action is required.

Table 25: SRX345 Firewall Power LED Status *(Continued)*

LED Status	Meaning	Possible Cause and Corrective Action
Off	Indicates that the device is not receiving power.	• Verify that the AC power cord from the power source to the device is not damaged. If the insulation is cracked or broken, immediately replace the cord or cable. • Ensure that the socket you plug in is in working condition. • Ensure the device has an AC input voltage between 100 and 240 VAC. • If you cannot determine the cause of the problem or need additional assistance, contact JTAC.

The SRX345 Firewall with dual AC power supplies provides a system alarm that alerts you when one of the power supplies fails. You can display the messages for this alarm by issuing the `show system alarms` or `show chassis alarms` operational mode command.

The following sample outputs from the `show system alarms` and `show chassis alarms` commands show the system alarm message that is displayed when one of the power supplies fails.

```
user@host> show system alarms
3 alarms currently active
Alarm time               Class  Description
2017-08-29 05:48:43 UTC  Major  PEM 0 Output Failure
2017-08-28 04:07:21 UTC  Minor  Autorecovery information needs to be saved
2017-08-28 04:07:16 UTC  Minor  Rescue configuration is not set
```

```
user@host> show chassis alarms
1 alarms currently active
Alarm time               Class  Description
2017-08-29 05:48:43 UTC  Major  PEM 0 Output Failure
```

Using the RESET CONFIG Button

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

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

The rescue configuration is a previously committed, valid configuration. You must have previously set the rescue configuration through the J-Web interface or the CLI. To press the RESET CONFIG button, insert a small probe (such as a straightened paper clip) into the pinhole on the front panel.

- By default, pressing and quickly releasing the RESET CONFIG button loads and commits the rescue configuration through the J-Web interface or the CLI. The Status LED is solid amber during this time.
- By default, pressing and holding the RESET CONFIG button for 15 seconds or more—until the Status LED is solid amber — deletes all configurations on the device, including the backup configurations and rescue configuration, and loads and commits the factory configuration.

NOTE: Resetting the configuration does not trigger a reboot automatically. Thus, configuration changes that require a reboot, such as Ethernet switching configurations, do not take effect after you reset the configuration. As a result, connectivity to the device might be lost. For the configuration to take effect, power off and power on the device after resetting the configuration.

Changing the RESET CONFIG Button Behavior

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

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

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

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

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

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

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

- To disable the button and prevent the device from resetting to either the factory-default or rescue configuration:

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

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

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

CHAPTER 6

Contacting Customer Support and Returning the Chassis or Components

Returning the SRX345 Chassis or Components | 76

Returning the SRX345 Chassis or Components

IN THIS SECTION

- Contacting Customer Support | 76
- Returning a SRX345 Firewall Component to Juniper Networks | 77
- Locating the SRX345 Firewall Chassis Serial Number and Agency Labels | 77
- Locating the Mini-PIM Serial Number Label | 78
- Listing the SRX345 Firewall Component Details with the CLI | 78
- Required Tools and Parts for Packing the SRX Series Services Gateway | 78
- Packing the SRX Series Services Gateway for Shipment | 79
- Packing SRX Series Services Gateway Components for Shipment | 79

Contacting Customer Support

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

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

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

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

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

- Your existing service request number, if you have one

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

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

Returning a SRX345 Firewall Component to Juniper Networks

To return an SRX345 Firewall or component to Juniper Networks for repair or replacement:

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

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

3. Pack the SRX345 Firewall or component for shipping.

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

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

Locating the SRX345 Firewall Chassis Serial Number and Agency Labels

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

Locating the Mini-PIM Serial Number Label

Mini-Physical Interface Modules (Mini-PIMs) are field-replaceable and each Mini-PIM has a unique serial number. The serial number label is located on the right side of the Mini-PIM, when the Mini-PIM is horizontally oriented (as it would be when installed on the device). The exact location might be slightly different on different Mini-PIMs, depending on the placement of components on the Mini-PIM.

Listing the SRX345 Firewall Component Details with the CLI

Before contacting Juniper Networks to request an RMA, you must find the serial number on the SRX345 Firewall or component.

To list all of the SRX345 Firewall components and their serial numbers, enter the following command:

```
user@host> show chassis hardware
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                CZ3615AN0003      SRX345
Routing Engine   REV 02   650-065043   CZ3615AN0003      RE-SRX345
FPC 0                                                   FPC
  PIC 0                                                 8xGE,8xGE SFP Base PIC
Power Supply 0
```

NOTE: In the `show chassis hardware` command, the Mini-PIM slot number is reported as an FPC number, and the Mini-PIM number (always 0) is reported as the PIC number.

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

Required Tools and Parts for Packing the SRX Series Services Gateway

To remove one or more components from the SRX Series Services Gateway or to remove the services gateway from a rack, you need the following tools and parts:

- Electrostatic bag or antistatic mat for each component
- Electrostatic discharge (ESD) grounding wrist strap

- Flat-blade screwdriver, approximately 1/4 in. (6 mm)
- Phillips (+) screwdrivers, numbers 1 and 2

Packing the SRX Series Services Gateway for Shipment

To pack the SRX Series Services Gateway for shipment:

1. Retrieve the shipping carton and packing materials in which the services gateway was originally shipped. If you do not have these materials, contact your Juniper Networks representative about approved packaging materials.
2. Wrap and fasten an electrostatic discharge (ESD) grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
3. On the console or other management device connected to the services gateway, enter CLI operational mode, and then shut down the services gateway software:

   ```
   user@host> request system halt
   ```

   Wait until a message appears on the console confirming that the operating system has halted.
4. Shut down power to the services gateway by pressing the Power button on the front of the services gateway.
5. Disconnect power from the services gateway.
6. Remove the cables that connect to all external devices.
7. If the device is installed on a wall or rack, have one person support the weight of the device while another person unscrews and removes the mounting screws.
8. Place the services gateway in the shipping carton.
9. Cover the services gateway with an ESD bag, and place the packing foam on top of and around the device.
10. Replace the accessory box on top of the packing foam.
11. Securely tape the box closed.
12. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.

Packing SRX Series Services Gateway Components for Shipment

To pack and ship individual components of the services gateway:

1. Make sure that it is adequately protected with packing materials and securely packed so that the pieces do not move around inside the carton.
2. Use the original shipping materials if they are available.
3. Place each component in an individual electrostatic bag.
4. Write the Return Materials Authorization (RMA) number on the exterior of the box to ensure proper tracking.



CAUTION: Do not stack any of the services gateway components while packing them.

CHAPTER 7

Safety and Compliance Information

Definitions of Safety Warning Levels | 82

General Safety Guidelines and Warnings | 83

Restricted Access Warning | 85

Qualified Personnel Warning | 86

Prevention of Electrostatic Discharge Damage | 87

Fire Safety Requirements | 88

Laser and LED Safety Guidelines and Warnings | 90

Radiation from Open Port Apertures Warning | 92

Maintenance and Operational Safety Guidelines and Warnings | 93

Action to Take After an Electrical Accident | 99

General Electrical Safety Guidelines and Warnings | 99

AC Power Electrical Safety Guidelines | 100

DC Power Electrical Safety Guidelines | 101

SRX345 Firewall Agency Approvals | 108

SRX345 Firewall Acoustic Noise Compliance Statements | 110

SRX345 Firewall EMC Requirements | 110

Definitions of Safety Warning Levels

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

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



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

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



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

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



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

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

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

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

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

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

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

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

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

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

General Safety Guidelines and Warnings

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

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

- Do not wear loose clothing or jewelry, such as rings, bracelets, or chains, which could become caught in the device.
- Wear safety glasses if you are working under any conditions that could be hazardous to your eyes.
- Do not perform any actions that create a potential hazard to people or make the equipment unsafe.
- Never attempt to lift an object that is too heavy for one person to handle.
- Never install or manipulate wiring during electrical storms.
- Never install electrical jacks in wet locations unless the jacks are specifically designed for wet environments.
- Operate the device only when it is properly grounded.
- Follow the instructions in this guide to properly ground the device to earth.
- Replace fuses only with fuses of the same type and rating.
- Do not open or remove chassis covers or sheet-metal parts unless instructions are provided in the hardware documentation for this device. Such an action could cause severe electrical shock.
- Do not push or force any objects through any opening in the chassis frame. Such an action could result in electrical shock or fire.
- Avoid spilling liquid onto the chassis or onto any device component. Such an action could cause electrical shock or damage the device.
- Avoid touching uninsulated electrical wires or terminals that have not been disconnected from their power source. Such an action could cause electrical shock.
- Some parts of the chassis, including AC and DC power supply surfaces, power supply unit handles, SFB card handles, and fan tray handles might become hot. The following label provides the warning for hot surfaces on the chassis:



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

Restricted Access Warning



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

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

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

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

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

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

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

Aviso Esta unidade foi concebida para instalação em áreas de acesso restrito. Uma área de acesso restrito é uma área à qual apenas tem acesso o pessoal de serviço autorizado,

que possua uma ferramenta, chave e fechadura especial, ou qualquer outra forma de segurança. Esta área é controlada pela autoridade responsável pelo local.

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

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

Qualified Personnel Warning



WARNING: Only trained and qualified personnel should install or replace the device.
Waarschuwing Installatie en reparaties mogen uitsluitend door getraind en bevoegd personeel uitgevoerd worden.

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

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

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

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

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

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

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

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

Prevention of Electrostatic Discharge Damage

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

- Always use an ESD wrist strap when you are handling components that are subject to ESD damage, and make sure that it is in direct contact with your skin.

  If a grounding strap is not available, hold the component in its antistatic bag (see Figure 23 on page 88) in one hand and touch the exposed, bare metal of the device with the other hand immediately before inserting the component into the device.

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

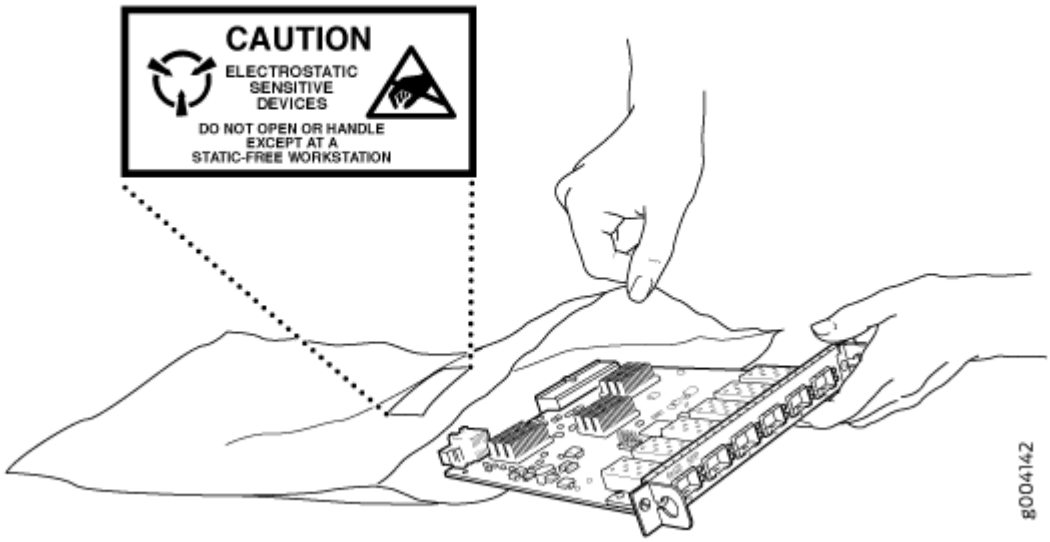
- When handling any component that is subject to ESD damage and that is removed from the device, make sure the equipment end of your ESD wrist strap is attached to the ESD point on the chassis.

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

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

- When removing or installing a component that is subject to ESD damage, always place it component-side up on an antistatic surface, in an antistatic card rack, or in an antistatic bag (see Figure 23 on page 88). If you are returning a component, place it in an antistatic bag before packing it.

Figure 23: Placing a Component into an Antistatic Bag



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

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

Fire Safety Requirements

IN THIS SECTION

- Fire Suppression | 89
- Fire Suppression Equipment | 89

In the event of a fire emergency, the safety of people is the primary concern. You should establish procedures for protecting people in the event of a fire emergency, provide safety training, and properly provision fire-control equipment and fire extinguishers.

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

Fire Suppression

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

Fire Suppression Equipment

Type C fire extinguishers, which use noncorrosive fire retardants such as carbon dioxide and Halotron™, are most effective for suppressing electrical fires. Type C fire extinguishers displace oxygen from the point of combustion to eliminate the fire. For extinguishing fire on or around equipment that draws air from the environment for cooling, you should use this type of inert oxygen displacement extinguisher instead of an extinguisher that leaves residues on equipment.

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

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

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

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

Laser and LED Safety Guidelines and Warnings

IN THIS SECTION

- General Laser Safety Guidelines | 90
- Class 1 Laser Product Warning | 91
- Class 1 LED Product Warning | 91
- Laser Beam Warning | 92

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

Observe the following guidelines and warnings:

General Laser Safety Guidelines

When working around ports that support optical transceivers, observe the following safety guidelines to prevent eye injury:

- Do not look into unterminated ports or at fibers that connect to unknown sources.
- Do not examine unterminated optical ports with optical instruments.
- Avoid direct exposure to the beam.



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

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

Class 1 Laser Product Warning



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

Varoitus Luokan 1 lasertuote.

Avertissement Produit laser de classe I.

Warnung Laserprodukt der Klasse 1.

Avvertenza Prodotto laser di Classe 1.

Advarsel Laserprodukt av klasse 1.

Aviso Produto laser de classe 1.

¡Atención! Producto láser Clase I.

Varning! Laserprodukt av klass 1.

Class 1 LED Product Warning



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

Varoitus Luokan 1 valodiodituote.

Avertissement Alarme de produit LED Class I.

Warnung Class 1 LED-Produktwarnung.

Avvertenza Avvertenza prodotto LED di Classe 1.

Advarsel LED-produkt i klasse 1.

Aviso Produto de classe 1 com LED.

¡Atención! Aviso sobre producto LED de Clase 1.

Varning! Lysdiodprodukt av klass 1.

Laser Beam Warning



LASER WARNING: Do not stare into the laser beam or view it directly with optical instruments.
Waarschuwing Niet in de straal staren of hem rechtstreeks bekijken met optische instrumenten.

Varoitus Älä katso säteeseen äläkä tarkastele sitä suoraan optisen laitteen avulla.

Avertissement Ne pas fixer le faisceau des yeux, ni l'observer directement à l'aide d'instruments optiques.

Warnung Nicht direkt in den Strahl blicken und ihn nicht direkt mit optischen Geräten prüfen.

Avvertenza Non fissare il raggio con gli occhi né usare strumenti ottici per osservarlo direttamente.

Advarsel Stirr eller se ikke direkte p strlen med optiske instrumenter.

Aviso Não olhe fixamente para o raio, nem olhe para ele directamente com instrumentos ópticos.

¡Atención! No mirar fijamente el haz ni observarlo directamente con instrumentos ópticos.

Varning! Rikta inte blicken in mot strålen och titta inte direkt på den genom optiska instrument.

Radiation from Open Port Apertures Warning



LASER WARNING: Because invisible radiation might be emitted from the aperture of the port when no fiber cable is connected, avoid exposure to radiation and do not stare into open apertures.
Waarschuwing Aangezien onzichtbare straling vanuit de opening van de poort kan komen als er geen fiberkabel aangesloten is, dient blootstelling aan straling en het kijken in open openingen vermeden te worden.

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

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

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

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

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

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

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

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

Maintenance and Operational Safety Guidelines and Warnings

IN THIS SECTION

- Battery Handling Warning | **94**
- Jewelry Removal Warning | **95**

- Lightning Activity Warning | 96
- Operating Temperature Warning | 97
- Product Disposal Warning | 98

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

Battery Handling Warning



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

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

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

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

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

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

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

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

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

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

Jewelry Removal Warning



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

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

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

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

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

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

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

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

¡Atención! Antes de operar sobre equipos conectados a líneas de alimentación, quitarse las joyas (incluidos anillos, collares y relojes). Los objetos de metal se calientan cuando se conectan a la alimentación y a tierra, lo que puede ocasionar quemaduras graves o que los objetos metálicos queden soldados a los bornes.

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

Lightning Activity Warning



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

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

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

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

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

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

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

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

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

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

Operating Temperature Warning



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

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

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

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

Warnung Um einen Router der switch vor Überhitzung zu schützen, darf dieser nicht in einer Gegend betrieben werden, in der die Umgebungstemperatur das empfohlene

Maximum von 40° C überschreitet. Um Lüftungsverschluß zu verhindern, achten Sie darauf, daß mindestens 15,2 cm lichter Raum um die Lüftungsöffnungen herum frei bleibt.

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

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

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

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

Varning! Förhindra att en Juniper Networks switch överhettas genom att inte använda den i ett område där den maximalt rekommenderade omgivningstemperaturen på 40° C överskrids. Förhindra att luftcirkulationen inskränks genom att se till att det finns fritt utrymme på minst 15,2 cm omkring ventilationsöppningarna.

Product Disposal Warning



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

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

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

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

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

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

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

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

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

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

Action to Take After an Electrical Accident

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

1. Use caution. Be aware of potentially hazardous conditions that could cause further injury.
2. Disconnect power from the device.
3. If possible, send another person to get medical aid. Otherwise, assess the condition of the victim, and then call for help.

General Electrical Safety Guidelines and Warnings

- Install the services gateway in compliance with the following local, national, or international electrical codes:
    - United States—National Fire Protection Association (NFPA 70), United States National Electrical Code

  - Canada—Canadian Electrical Code, Part 1, CSA C22.1
  - Other countries—International Electromechanical Commission (IEC) 60364, Part 1 through Part 7
  - Evaluated to the TN power system
- Locate the emergency power-off switch for the room in which you are working so that if an electrical accident occurs, you can quickly turn off the power.
- Do not work alone if potentially hazardous conditions exist anywhere in your workspace.
- Never assume that power is disconnected from a circuit. Always check the circuit before starting to work.
- Carefully look for possible hazards in your work area, such as moist floors, ungrounded power extension cords, and missing safety grounds.
- Operate the services gateway within marked electrical ratings and product usage instructions.
- For the services gateway and peripheral equipment to function safely and correctly, use the cables and connectors specified for the attached peripheral equipment, and make certain they are in good condition.

RELATED DOCUMENTATION

In Case of Electrical Accident

AC Power Electrical Safety Guidelines

AC Power Electrical Safety Guidelines

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

- Note the following warnings printed on the device:

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

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

- AC-powered devices are shipped with a three-wire electrical cord with a grounding-type plug that fits only a grounding-type power outlet. Do not circumvent this safety feature. Equipment grounding must comply with local and national electrical codes.
- You must provide an external certified circuit breaker (2-pole circuit breaker or 4-pole circuit breaker based on your device) rated minimum 20 A in the building installation.
- The power cord serves as the main disconnecting device for the AC-powered device. The socket outlet must be near the AC-powered device and be easily accessible.
- For devices that have more than one power supply connection, you must ensure that all power connections are fully disconnected so that power to the device is completely removed to prevent electric shock. To disconnect power, unplug all power cords (one for each power supply).

Power Cable Warning (Japanese)

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

注意

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

DC Power Electrical Safety Guidelines

IN THIS SECTION

- DC Power Electrical Safety Guidelines | **102**
- DC Power Disconnection Warning | **103**
- DC Power Grounding Requirements and Warning | **104**
- DC Power Wiring Sequence Warning | **105**
- DC Power Wiring Terminations Warning | **106**

DC Power Electrical Safety Guidelines

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

- A DC-powered services gateway is equipped with a DC terminal block that is rated for the power requirements of a maximally configured services gateway. To supply sufficient power, terminate the DC input wiring on a facility DC source capable of supplying at least 30 A @ -48 VDC for the system. We recommend that the 48 VDC facility DC source be equipped with a circuit breaker rated at 40 A (-48 VDC) minimum, or as required by local code. Incorporate an easily accessible disconnect device into the facility wiring. In the United States and Canada, the -48 VDC facility should be equipped with a circuit breaker rated a minimum of 125% of the power provisioned for the input in accordance with the National Electrical Code in the US and the Canadian Electrical Code in Canada. Be sure to connect the ground wire or conduit to a solid office (earth) ground. A closed loop ring is recommended for terminating the ground conductor at the ground stud.
- Run two wires from the circuit breaker box to a source of 48 VDC. Use appropriate gauge wire to handle up to 40 A.
- A DC-powered services gateway that is equipped with a DC terminal block is intended only for installation in a restricted access location. In the United States, a restricted access area is one in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code ANSI/NFPA 70.

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

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

DC Power Disconnection Warning



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

Waarschuwing Voordat u een van de onderstaande procedures uitvoert, dient u te controleren of de stroom naar het gelijkstroom circuit uitgeschakeld is. Om u ervan te verzekeren dat alle stroom UIT is geschakeld, kiest u op het schakelbord de stroomverbreker die het gelijkstroom circuit bedient, draait de stroomverbreker naar de UIT positie en plakt de schakelaarhendel van de stroomverbreker met plakband in de UIT positie vast.

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

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

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

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

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

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

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

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

DC Power Grounding Requirements and Warning

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



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

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

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

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

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

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

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

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

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

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

DC Power Wiring Sequence Warning



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

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

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

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

Warnung Die Stromzufuhr ist nur mit geeigneten Ringösen an das DC Netzteil anzuschliessen. Die richtige Anschlusssequenz ist: Erdanschluss zu Erdanschluss, +RTN zu +RTN und dann -48V zu -48V. Die richtige Sequenz zum Abtrennen der

Stromversorgung ist -48V zu -48V, +RTN zu +RTN und dann Erdanschluss zu Erdanschluss. Es ist zu beachten dass der Erdanschluss immer zuerst angeschlossen und als letztes abgetrennt wird.

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

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

Aviso Ate con alambre la fuente de potencia cc Usando los terminales apropiados en el extremo del cableado. Al conectar potencia, la secuencia apropiada del cableado se muele para moler, +RTN a +RTN, entonces -48 V a -48 V. Al desconectar potencia, la secuencia apropiada del cableado es -48 V a -48 V, +RTN a +RTN, entonces molió para moler. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último. Observe que el alambre de tierra se debe conectar siempre primero y desconectar por último.

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

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

DC Power Wiring Terminations Warning



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

Waarschuwing Wanneer geslagen bedrading vereist is, dient u bedrading te gebruiken die voorzien is van goedgekeurde aansluitingspunten, zoals het gesloten-lus type of het

grijperschop type waarbij de aansluitpunten omhoog wijzen. Deze aansluitpunten dienen de juiste maat voor de draden te hebben en dienen zowel de isolatie als de geleider vast te klemmen.

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

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

Warnung Wenn Litzenverdrahtung erforderlich ist, sind zugelassene Verdrahtungsanschlüsse, z.B. Ringoesen oder gabelförmige Kabelschuhe mit nach oben gerichteten Enden zu verwenden. Diese Abschlüsse sollten die angemessene Größe für die Drähte haben und sowohl die Isolierung als auch den Leiter festklemmen.

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

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

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

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

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

RELATED DOCUMENTATION

AC Power Electrical Safety Guidelines

SRX345 Firewall Agency Approvals

IN THIS SECTION

- Compliance Statement for Argentina | **109**

The services gateway complies with the following standards:

- Safety
  - CAN/CSA-C22.2 No.60950-1 (2007) Information Technology Equipment
  - UL 60950-1 (2nd Ed.) Information Technology Equipment
  - EN 60950-1 (2006+ A11:2010) Information Technology Equipment - Safety
  - IEC 60950-1 (2005 +A1:2009) Information Technology Equipment - Safety (All country deviations): CB Scheme report
  - EN 60825-1 (2007) Safety of Laser Products - Part 1: Equipment classification and requirements
- EMC
  - EN 300 386 V1.6.1 Telecom Network Equipment - EMC requirements
  - EN 55032:2012 + EN55032:2012/AC:2013 Electromagnetic compatibility of multimedia equipment - Emission requirements
  - CISPR 32:2012
  - EN 55022:2010/AC:2011 European Radiated Emissions
  - CISPR 22 edition 6.0 : 2008-09
  - EN 55024: 2010 Information Technology Equipment Immunity Characteristics
  - CISPR 24 edition 2b :2010 COREC 2011 IT Equipment Immunity Characteristics

- EMI
  - FCC 47CFR , Part 15 Class A (2012) USA Radiated Emissions
  - ICES-003 Issue 5, August 2012 Canada Radiated Emissions
  - VCCI-V-3/2013.04 and V-4/2012.04 Japanese Radiated Emissions
  - BSMI CNS 13438 and NCC C6357 Taiwan Radiated Emissions
- Immunity
  - EN-61000-3-2 Power Line Harmonics
  - EN-61000-3-3 Voltage Fluctuations and Flicker
  - EN-61000-4-2 Electrostatic Discharge
  - EN-61000-4-3 Radiated Immunity
  - EN-61000-4-4 (2004) Electrical Fast Transients
  - EN-61000-4-5 (2006) Surge
  - EN-61000-4-6 (2007) Low Frequency Common Immunity
  - EN-61000-4-11 (2004) Voltage Dips and Sags
  - EN 55024 +A1+A2 (1998) Information Technology Equipment Immunity Characteristics
- Environmental
  - Reduction of Hazardous Substances (ROHS) 6
- Telco
  - Common Language Equipment Identifier (CLEI) code

Compliance Statement for Argentina

EQUIPO DE USO IDÓNEO.

RELATED DOCUMENTATION

SRX345 Firewall Acoustic Noise Compliance Statements | 110

SRX345 Firewall EMC Requirements | 110

SRX345 Firewall Acoustic Noise Compliance Statements

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

German Translation:

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

RELATED DOCUMENTATION

SRX345 Firewall Agency Approvals | 108

SRX345 Firewall EMC Requirements | 110

SRX345 Firewall EMC Requirements

IN THIS SECTION

- Canada | 110
- European Community | 111
- Israel | 111
- Japan | 111
- United States | 112

Canada

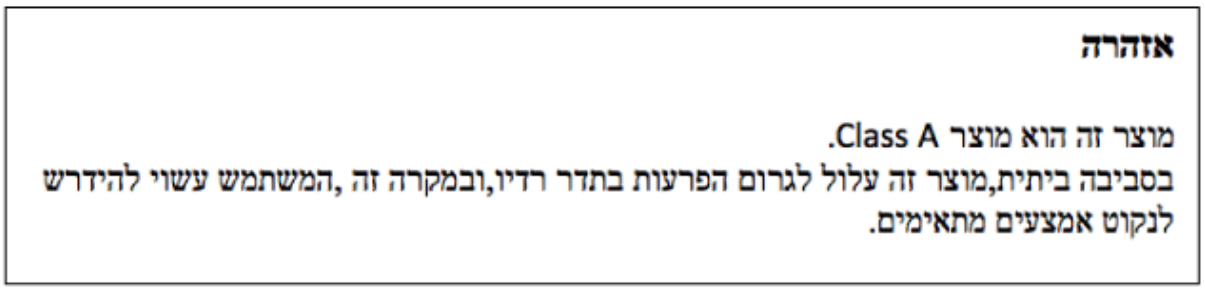
This Class A digital apparatus complies with Canadian ICES-003.

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

European Community

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

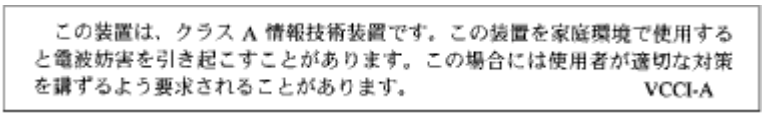
Israel



The preceding translates as follows:

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

Japan



The preceding translates as follows:

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

VCCI-A

United States

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

RELATED DOCUMENTATION

SRX345 Firewall Agency Approvals | **108**

SRX345 Firewall Acoustic Noise Compliance Statements | **110**