

SRX345 Quick Start

Published
2024-05-22

RELEASE

Table of Contents

Step 1: Begin

Meet the SRX345 | 1

Install the SRX345 in a Rack | 2

What's in the Box? | 2

What Else Do I Need? | 2

Rack It | 3

Power On | 4

Step 2: Up and Running

SRX345 Provisioning Options | 6

Initial Configuration Using the CLI | 6

Connect to the Serial Console Port | 7

Perform Initial Configuration | 8

Congratulations! Your SRX is Up and Running | 10

Step 3: Keep Going

What's Next? | 11

General Information | 12

Learn With Videos | 13

Step 1: Begin

IN THIS SECTION

- [Meet the SRX345 | 1](#)
- [Install the SRX345 in a Rack | 2](#)
- [Power On | 4](#)

In this guide, we provide a simple, three-step path, to quickly get you up and running with your new SRX345. We've simplified and shortened the installation and configuration steps, and included how-to videos. You'll learn how to install the SRX345 in a rack, power it up, and deploy it on your network using the CLI.

NOTE: We think you'll want to check out our [Guided Setup: SRX300 Line Firewalls](#). Our Guided Setup picks up where this Day One+ ends, providing step-by-step instructions on how to easily secure and validate your branch location.

Are you interested in getting hands-on experience with the topics and operations covered in this guide? Visit [Juniper Networks Virtual Labs](#) and reserve your free sandbox today! You'll find the Junos Day One Experience sandbox in the stand alone category.

Meet the SRX345

The Juniper Networks® SRX345 Firewall securely consolidates security, routing, switching, and WAN connectivity in a compact 1-U chassis. It supports up to 5-Gbps firewall throughput and 800-Mbps IPsec VPN to meet the needs of midsize, distributed-enterprise locations. Along with Juniper Sky™ Enterprise and Contrail Service Orchestration® (CSO), the SRX345 delivers fully automated SD-WAN to both enterprises and service providers. A zero-touch provisioning (ZTP) feature simplifies branch network connectivity for initial deployment and ongoing management.

The SRX345 has eight 1 GbE RJ-45 ports, eight 1 GbE SFP ports, one management port, one console port, and four Mini-Physical Interface Module (Mini-PIM) slots. The RJ-45 and SFP ports are MACsec capable. The SRX345 AC models have either a single AC power supply or dual AC power supplies. The SRX345 DC models have a single power supply. This guide covers SRX345 AC models.



Install the SRX345 in a Rack

IN THIS SECTION

- [What's in the Box? | 2](#)
- [What Else Do I Need? | 2](#)
- [Rack It | 3](#)

What's in the Box?

- SRX345 Firewall
- A power cord appropriate for your geographic location
- Two mounting brackets
- Eight mounting screws to attach the mounting brackets to the SRX345

What Else Do I Need?

You'll also need:

- Someone to help you do the installation
- Rack mount screws appropriate for your rack
- A number two Phillips (+) screwdriver
- A console cable with the required adapter

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

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

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

Rack It

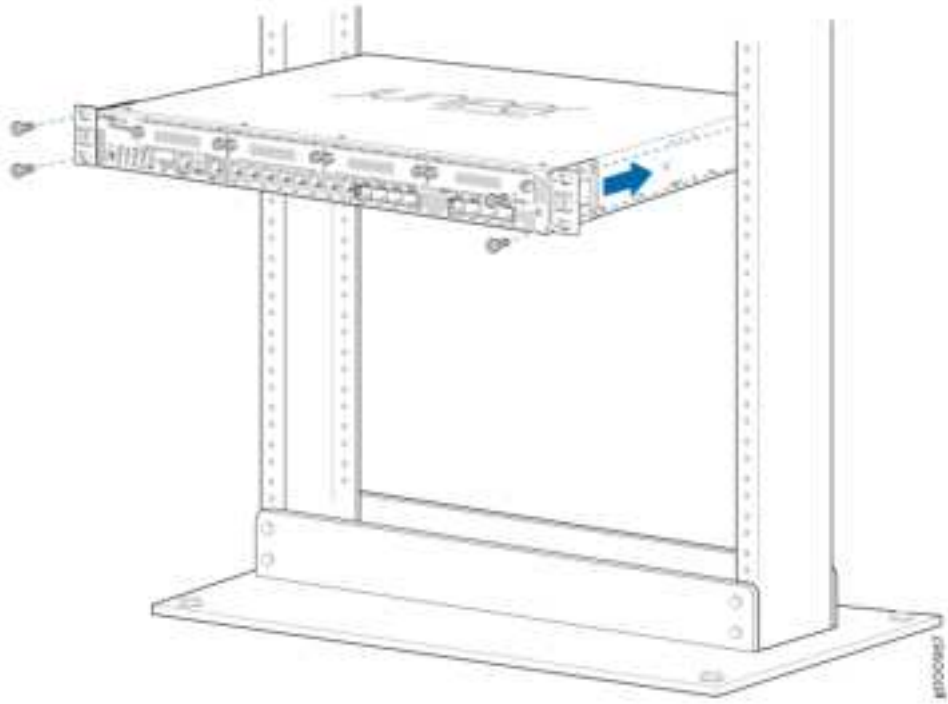
Here's how to install the SRX345 in a rack:

1. Review [General Safety Guidelines and Warnings](#).
2. Wrap and fasten one end of the electrostatic discharge (ESD) grounding strap around your bare wrist, and connect the other end to a site ESD point.
3. Attach the mounting brackets to the sides of the SRX345 using the eight mounting screws and the screwdriver.

Depending on how you'd like the SRX345 to sit in the rack, you can attach the mounting brackets to the front or center mounting holes.



4. Lift the SRX345 and position it in the rack. Line up the bottom hole in each mounting bracket with a hole in each rack rail, making sure that the SRX345 is level.
5. While you're holding the SRX345 in place, have a second person insert and tighten the rack mount screws to secure the mounting brackets to the rack. Make sure to tighten the screws in the two bottom holes first and then tighten the screws in the two top holes.

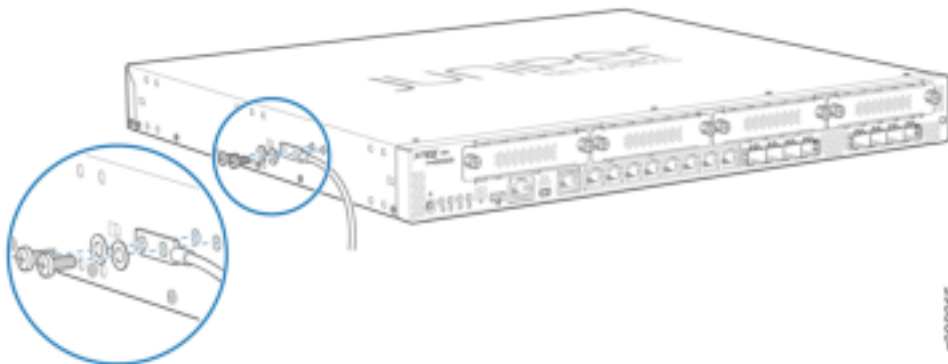


6. Check that the mounting brackets on each side of the rack are level.

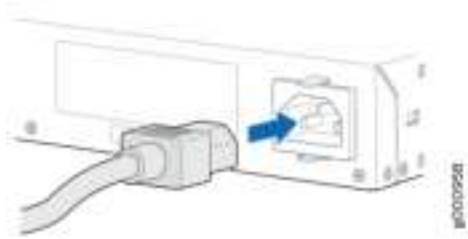
Power On

Now that you've installed your SRX345 in the rack, you're ready to connect it to power.

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. Attach a grounding cable to earth ground, and then attach the other end to the grounding point on the side panel of the SRX345.



3. Plug the power cord into the SRX345 rear panel.



4. If the AC power source outlet has a power switch, turn it off.
5. Plug the other end of the power cord into the AC power source outlet.
6. If the AC power source outlet has a power switch, turn it on.
7. If you are using a SRX345 Firewall with dual AC power supplies, then repeat Step 3 through Step 5 for the second power supply.

The SRX345 powers up as soon as you connect it to power. When the **PWR** and **STAT** LEDs on the front panel are lit solid green, the SRX345 is ready to use.



Step 2: Up and Running

IN THIS SECTION

- [SRX345 Provisioning Options | 6](#)
- [Initial Configuration Using the CLI | 6](#)

Now that the SRX345 is powered on, let's do some initial configuration to get it up and running on the network.

NOTE: Be sure to check out our [Guided Setup: SRX300 Line Firewalls](#). Our Guided Setup picks up where this Day One+ leaves off, providing step-by-step instructions on how to easily secure and validate your branch location.

SRX345 Provisioning Options

It's simple to provision and manage the SRX345 and other devices on your network. You can choose the configuration tool that's right for you:

- Junos CLI commands. In this guide we show you how to configure the SRX345 with CLI commands that leverage the plug and play factory defaults.
- J-Web, Juniper Networks Setup wizard that is preinstalled on the SRX345. For information on performing initial configuration using the J-Web setup wizard see [Configure SRX Devices Using the J-Web Setup Wizard](#) in the J-Web User Guide for SRX Series Devices.
- Juniper Sky™ Enterprise, Juniper Networks-hosted public cloud-based Software as a Service (SaaS) solution. You'll need to have a Juniper Sky Enterprise subscription service before you can use it to configure the SRX345. For more information, check out the [Juniper Sky Enterprise Getting Started Guide](#).
- Juniper Networks Contrail Service Orchestration (CSO). To use CSO, you'll need an authentication code. See the [Contrail Service Orchestration \(CSO\) Deployment Guide](#).

If you are using Junos OS Release 19.2 or earlier, you can use Juniper Networks Network Service Controller to configure the SRX345 with ZTP. Network Service Controller is a component of CSO. See [Configure the Device Using ZTP with Juniper Networks Network Service Controller](#).

Initial Configuration Using the CLI

IN THIS SECTION

- [Connect to the Serial Console Port | 7](#)
- [Perform Initial Configuration | 8](#)
- [Congratulations! Your SRX is Up and Running | 10](#)

You can use the console port on the SRX to do the initial configuration. This section assumes you start from a factory default configuration. See [SRX345 Firewall Hardware Guide](#) for details on the SRX345 factory default configuration.

After you configure the SRX345, you can log in on a local LAN port, or remotely over the WAN interface, to manage and configure the SRX using the CLI or J-Web.

We recommend that you use the ge-0/0/0 interface for WAN connectivity on the SRX345. By default, this interface is set to receive its Internet access configuration from the service provider.

NOTE: This examples assumes you are using DHCP to configure the WAN interface. If the WAN provider does not support DHCP, you'll need to manually configure the WAN interface and related static routing. See [Junos Initial Configuration](#).

Have this information handy before you begin the initial configuration:

- Root password
- Hostname

Connect to the Serial Console Port

1. Plug one end of the Ethernet cable into the RJ-45 to DB-9 serial port adapter for your SRX345.

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

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

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

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.



4. Start your asynchronous terminal emulation application (such as Microsoft Windows HyperTerminal) and select the appropriate COM port to use (for example, COM1).
5. Verify that the serial port settings are set to the default:
 - Baud rate—9600
 - Parity—N
 - Data bits—8
 - Stop bits—1
 - Flow control—none

NOTE: You can also connect to the SRX345 using a mini-USB console port. See the [SRX345 Hardware Guide](#).

Perform Initial Configuration

1. Login as the root user and start the CLI. You don't need a password if you're running the factory default.

```
login: root
root%cli
root>
```

NOTE: You can view the factory-default settings with the **show configuration** operational mode command.

2. Enter configuration mode.

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

3. Since you're doing the initial configuration manually, you'll need to remove ZTP from the configuration. This stops the periodic log messages that report on ZTP status.

Set the root authentication password and commit the change to deactivate ZTP.

```
[edit]  
root# delete chassis auto-image-upgrade  
root# delete system phone-home  
root# set system root-authentication plain-text-password  
New password: password  
Retype new password: password
```

Issue the `commit` command to activate the candidate configuration that disables ZTP:

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

4. Enable root login over SSH, and allow SSH access over the WAN interface (ge-0/0/0).

```
[edit]  
root# set system services ssh root-login allow  
root# set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic  
system-services ssh
```

5. Configure the hostname.

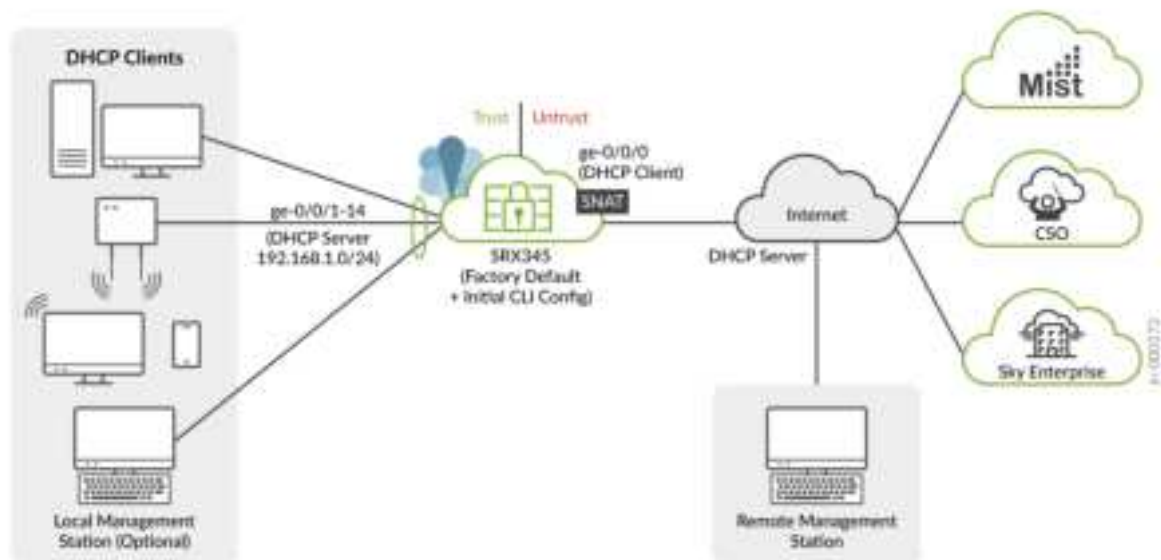
```
[edit]  
root# set system host-name host_name
```

6. That's it! The initial configuration is complete. Commit the configuration to activate the changes on the SRX.

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

Congratulations! Your SRX is Up and Running

Your SRX345 is now online and providing secure Internet access to devices attached to the LAN ports. You can manage the device locally and remotely, using the Junos CLI, J-Web, or a cloud based provisioning service. Here's what your network looks like:



A few things to keep in mind about your new SRX345 branch network:

- You access the SRX CLI or J-Web user interface locally using the 192.168.1.1 address. To access the SRX remotely, specify the IP address assigned by the WAN provider. Simply issue a `show interfaces ge-0/0/0 terse` CLI command to confirm the address in use by the WAN interface.
- The management interface is configured as a DHCP server for the 192.168.1.0/24 subnet.
- Devices attached to the LAN ports are configured to use DHCP. They receive their network configuration from the SRX. These devices obtain an IP address from the 192.168.2.0/24 address pool and use the SRX as their default gateway.
- All LAN ports are in the same subnet with Layer 2 connectivity. All traffic is permitted between trust zone interfaces.

- All traffic originating in the trust zone is permitted in the untrust zone. Matching response traffic is allowed back from the untrust to the trust zone. Traffic that originates from the untrust zone is blocked from the trust zone.
- The SRX performs source NAT (S-NAT) using the WAN interface's IP for traffic sent to the WAN that originated from the trust zone.
- Traffic associated with specific system services (HTTPS, DHCP, TFTP, and SSH) is permitted from the untrust zone to the local host. All local host services and protocols are allowed for traffic that originates from the trust zone.

Step 3: Keep Going

IN THIS SECTION

- [What's Next? | 11](#)
- [General Information | 12](#)
- [Learn With Videos | 13](#)

Congratulations! Your SRX345 is configured and ready to go. Here are some things you can do next.

What's Next?

NOTE: Quickly configure and validate a secure branch office in a few simple steps with our [Guided Setup: SRX300 Line Firewalls](#). Our Guided Setup picks up where this Day One+ guide ends and is designed to quickly get your branch location online and secured.

If you want to	Then
Change configuration settings, get another device up and running, or both	Log in to J-Web and use the wizard. Alternatively, you can use the more advanced configuration features offered by Juniper Contrail Service Orchestration (CSO) and Juniper Sky Enterprise. To use these services, you'll need an account and activation code. Check out the Contrail Service Orchestration (CSO) Deployment Guide and the Juniper Sky Enterprise Getting Started Guide .
Set up your SRX345 with advanced security measures to protect and defend your network	Visit Day One: SRX Series Up and Running With Advanced Security Services
Manage software upgrades on your SRX345	See Installing Software on SRX Series Devices
See, automate, and protect your network with Juniper Security	Visit the Security Design Center

(Continued)

Get hands-on experience with the procedures covered in this guide	Visit Juniper Networks Virtual Labs and reserve your free sandbox. You'll find the Junos Day One Experience sandbox in the stand alone category.
---	--

General Information

If you want to	Then
Download, activate, and manage your software licenses to unlock additional features for your SRX Firewall	See Activate Junos OS Licenses in the Juniper Licensing Guide
See all documentation available for the SRX345	Visit the SRX345 Documentation page in the Juniper TechLibrary

(Continued)

If you want to	Then
Configure the SRX345 with the Junos OS CLI	Start with the Day One+ for Junos OS guide
Configure the SRX345 using J-Web	See J-Web for SRX Series Documentation
Stay up-to-date on new and changed features and known and resolved issues.	See Junos OS Release Notes

Learn With Videos

Our video library continues to grow! We've created many, many videos that demonstrate how to do everything from install your hardware to configure advanced Junos OS network features. Here are some great video and training resources that will help you expand your knowledge of Junos OS.

If you want to	Then
View a Web-based training video which provides an overview of the SRX340 and describes how to install and configure it	SRX340 and SRX345 Firewalls Overview and Deployment (WBT)
Get short and concise tips and instructions that provide quick answers, clarity, and insight into specific features and functions of Juniper technologies	See Learning with Juniper on Juniper Networks main YouTube page
View a list of the many free technical trainings we offer at Juniper	Visit the Getting Started page on the Juniper Learning Portal

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. Copyright © 2024 Juniper Networks, Inc. All rights reserved.