

Juniper NETWORKS Onboard SRX Series Firewalls to Security Director Cloud User Guide

[Home](#) » [JUNIPER NETWORKS](#) » Juniper NETWORKS Onboard SRX Series Firewalls to Security Director Cloud User Guide 

Juniper NETWORKS Onboard SRX Series Firewalls to Security Director Cloud



Contents

- [1 Onboard SRX Series Firewalls to Security Director Cloud](#)
- [2 Step 1: Begin](#)
- [3 Greenfield Onboarding: Add Cloud-Ready SRX Series Firewalls to Juniper Security Director Cloud Using QR Code](#)
- [4 Brownfield Onboarding: Add SRX Series Firewalls to Juniper Security Director Cloud Using Commands](#)
- [5 Step 2: Up and Running](#)
- [6 Step 3: Keep Going](#)
- [7 What's Next?](#)
- [8 General Information](#)
- [9 Learn With Videos](#)
- [10 Documents / Resources](#)
 - [10.1 References](#)

Onboard SRX Series Firewalls to Security Director Cloud

IN THIS GUIDE

- [Step 1: Begin | 1](#)
- [Step 2: Up and Running | 10](#)

Step 1: Begin

IN THIS SECTION

Greenfield Onboarding: Add Cloud-Ready SRX Series Firewalls to Juniper Security Director Cloud Using QR Code | 3

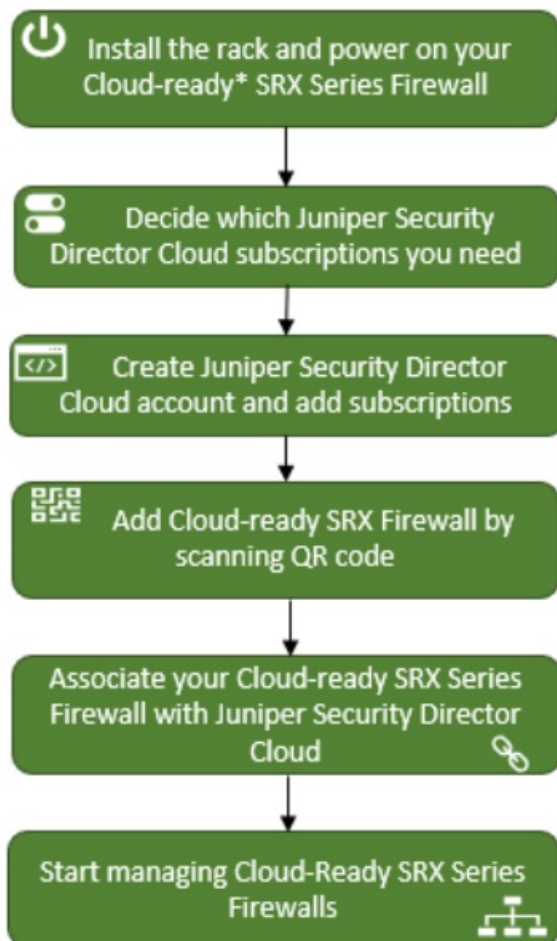
Brownfield Onboarding : Onboarding: Add SRX Series Firewalls to Juniper Security Director Cloud Using Commands | 7

This guide walks you through the simple steps to onboard Juniper Networks® SRX Series Firewalls to the Juniper® Security Director Cloud. You can onboard SRX Series Firewalls to Juniper Security Director Cloud using the following options:

- **Greenfield onboarding:** Onboard new cloud-ready SRX Series Firewalls.
- **Brownfield onboarding:** Onboard existing in-service SRX Series Firewalls.

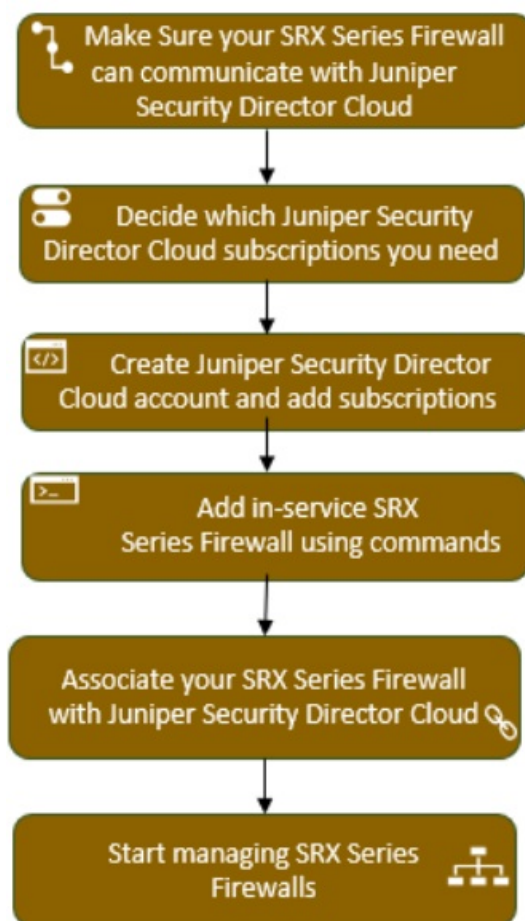
Figure 1: Onboard SRX Series Firewalls to Juniper Security Director Cloud

Option 1: Greenfield Onboarding



*Your firewall is cloud-ready if it has a QR claim code on the front or back panel.

Option 2: Brownfield onboarding



NOTE: You can also onboard SRX Series Firewalls using the following methods:

- To onboard SRX Series Firewalls to Juniper Security Director Cloud using ZTP, [see Add Devices Using Zero Touch Provisioning](#).
- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Juniper Security Director Cloud using JWeb, see [Add SRX Series Firewalls to Juniper Security Director Cloud Using JWeb](#).
- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Juniper Security Director Cloud using Security Director on-prem, see [Add Devices to Juniper Security Director Cloud](#).
- To onboard cloud-ready SRX Series Firewalls using Mist, see [Cloud-Ready SRX Firewalls with Mist](#).
- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Mist, see [SRX Adoption](#).

Greenfield Onboarding: Add Cloud-Ready SRX Series Firewalls to Juniper Security Director Cloud Using QR Code

Your firewall is cloud-ready if it has a QR claim code on the front or back panel. You can onboard one or more cloud-ready SRX Series Firewalls using your mobile phone.

Before You Begin

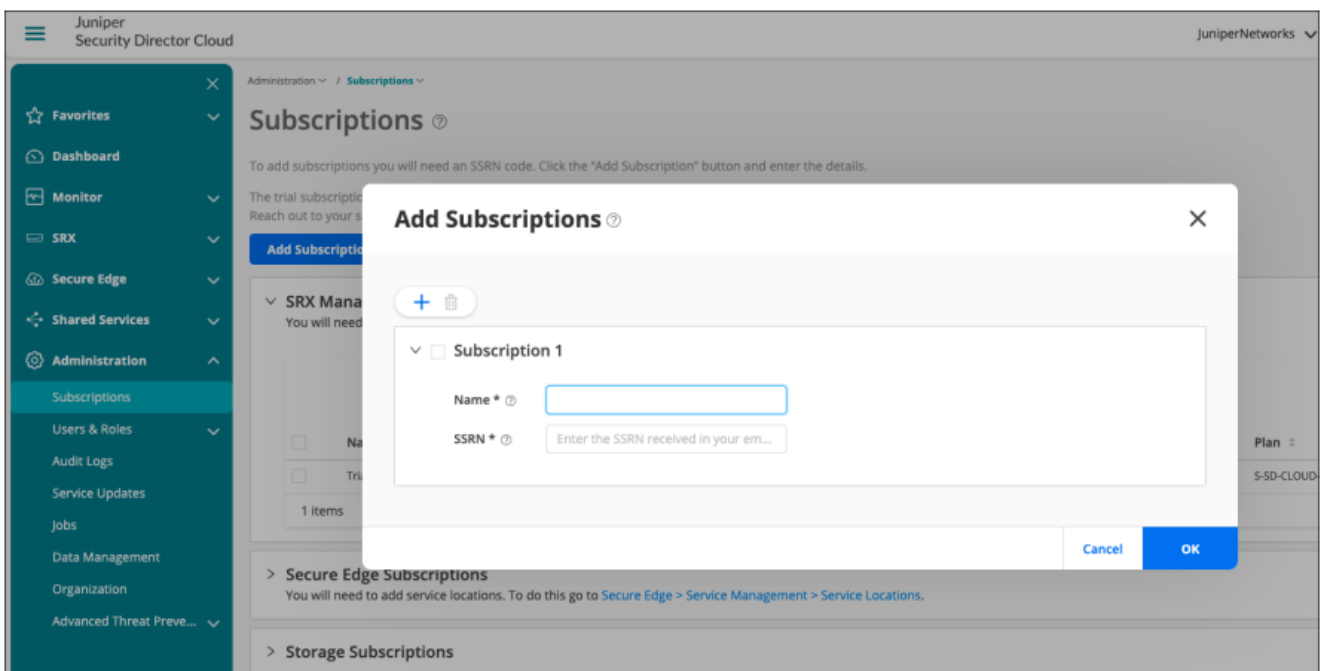
Install the rack and power on your cloud-ready SRX Series Firewall. For instructions specific to your device, see the applicable hardware guide.

Table 1: Juniper Security Director Cloud Supported Cloud-Ready SRX Series Firewalls and Related Documentation

Firewall	Install and Maintain Hardware
SRX1600	SRX1600 SRX1600 Firewall Hardware Guide
SRX2300	SRX2300 SRX2300 Firewall Hardware Guide

NOTE: All interfaces on cloud-ready SRX Series Firewalls are DHCP enabled in the factory-default configuration. Make sure that you can connect to the internet using one of the interfaces.

1. Decide which [Juniper Security Director Cloud Subscriptions](#) you need and contact your sales representative or account manager to purchase subscriptions.
2. Go to <https://sdcloud.juniperclouds.net/> and click **Create an organization account**.
Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account.
3. Log in to the Juniper Security Director Cloud portal, click **Add Subscriptions**, enter details, and click **OK**



View your added subscriptions from **Subscriptions>SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration > Jobs** page to view the status.

4. Use your mobile phone to scan the QR code on the cloud-ready SRX Series Firewall. Click the displayed link and select Claim to SD Cloud to go to Juniper Security Director Cloud login page.



Serial AA1111AA1111
Claim Code AA1AA1AAAA11A1A
Model SRXxxxx
Revision A
MAC XX1111XX1111

Claim to Mist

Claim to SD Cloud

5. Read the prerequisites, enter your e-mail address, and click Next.



Email

Next

 [View Prerequisites](#)

An account is required to add the device with serial number AA1AA1AAAA11A1A

If you do not have an account, create an account in <https://sdcloud.juniperclouds.net> from your laptop or desktop and then log in.

6. Follow the on-screen instructions to sign in.



user@juniper.net

Password



Sign in

- or -

Enter your organization's domain name

Sign in with SSO

- or -

Sign in with juniper.net

[← Go back to previous page](#)

7. Select the organization to add your device, enter the root password, and click **Add Device**.



Account Details

Select the organization to which you want to add the device.

user@juniper.net

DEMO



Device Details

Serial Number: AA1111AA1111

Model: SRXxxxx

Set root password for this device.



Add Device

[← Log in with a different email ID](#)

Congratulations! You've successfully registered your device to the organization and added your device to Juniper Security Director Cloud.



The device is successfully registered to the organization "DEMO"

Next Steps

1. Power on the device.
2. Use your **laptop** or **desktop** to log in to the Juniper Security Director Cloud portal through <https://sdcloud.juniperclouds.net> and manage the device.

[Logout](#)

8. Power on you cloud-ready SRX Series Firewall and log in to Juniper Security Director Cloud portal using your laptop or desktop. View the newly added device on the **SRX > Device Management > Devices** page.

SRX > / Device Management > / Devices

Devices

Devices | Device Groups | Preprovisioned Profiles

Security Logs Configuration | Manage Subscriptions | More > | + | - | 🔍 | ⋮

<input type="checkbox"/>	Host Name	Device Group	Inve...	Device Config Status	Management Status	Device Health...	Subscriptions	OS Version	Product ...
<input type="checkbox"/>	DEMO-AA1111AA1111	-	In Sync	In Sync	Up	Unknown	No Subscri...	23.4i20230916...	SRX1600
<input type="checkbox"/>	DEMO-TEST01	DG1	Unknown	Unknown	Discovery Not Initiated If not initiated, the device will be removed in 1...	Unknown	No Subscri...	—	—
<input type="checkbox"/>	srxt11111111111111	DG1	Unknown	Unknown	Discovery Not Initiated Adopt Device If not initiated, the device will be removed in 1...	Unknown	No Subscri...	—	—

3 items

NOTE: Device discovery takes a few seconds to complete. After successful device discovery, you can see the following status updates:

- **Management Status:** Up
- **Inventory Status:** In Sync
- **Device Config Status:** In Sync

Congratulations! You've successfully onboarded your cloud-ready SRX Series Firewall. You're now ready to associate devices to your Juniper Security Director Cloud subscription.

To continue, proceed to **"Step 2: Up and Running" on page 10** .

Brownfield Onboarding: Add SRX Series Firewalls to Juniper Security Director Cloud Using Commands

Before You Begin

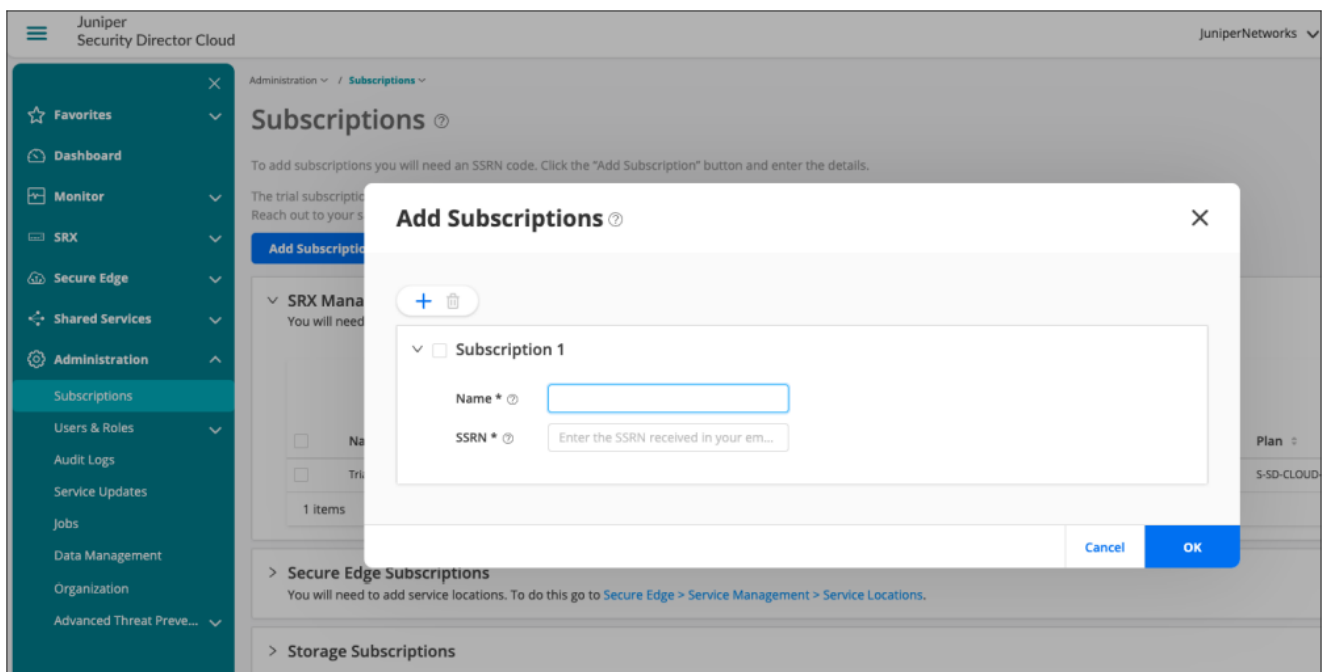
- Make sure SRX Series Firewall can communicate with Juniper Security Director Cloud fully qualified domain

name (FQDN) on respective ports. The FQDN of each home region is different. See the following table for FQDN mapping details.

Table 2: Home Region to FQDN Mapping

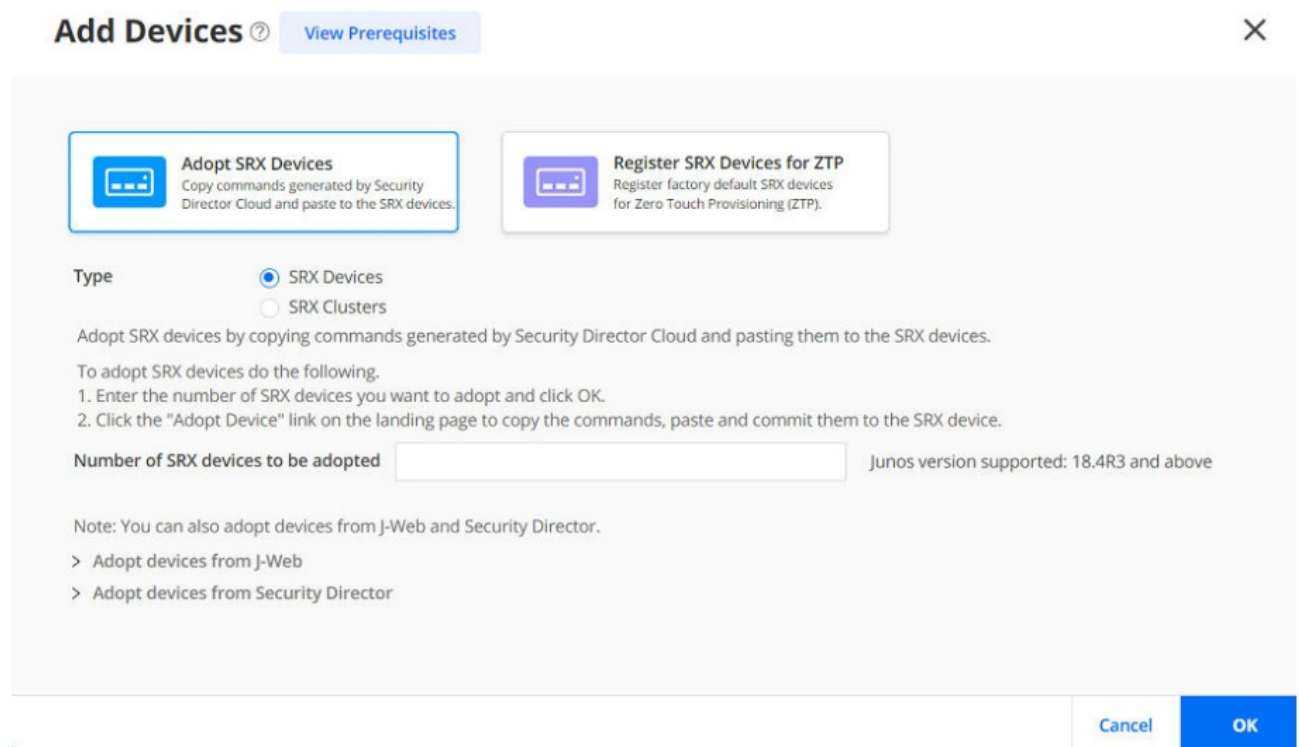
Home Region	Purpose	Port	FQDN
North Virginia	ZTP	443	jsec-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	System Log	6514	srx.sdcloud.juniperclouds.net
	messages over		
	TLS		
Ohio	ZTP	443	jsec-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec-ohio.juniperclouds.net
	System log	6514	srx.jsec-ohio.juniperclouds.net
	messages over		
	TLS		

- Use TCP port 53 and UDP port 53 to connect to Google DNS servers (IP addresses—8.8.8.8 and 8.8.4.4). The Google DNS servers are specified as the default servers in the factory settings of the SRX Series Firewalls. You must use these default DNS servers when you use ZTP to onboard the firewalls. You can use private DNS servers when you use other methods to onboard the firewalls. Note that you must make sure that the private DNS servers can resolve the Juniper Security Director Cloud FQDNs.
1. Decide which [Juniper Security Director Cloud Subscriptions](#) you need and contact your sales representative or account manager to purchase subscriptions.
 2. Go to <https://sdcloud.juniperclouds.net/> and click **Create an organization account**. Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account activation request.
 3. Log in to the [Juniper Security Director Cloud](#) portal, click **Add Subscriptions**, enter details, and click OK



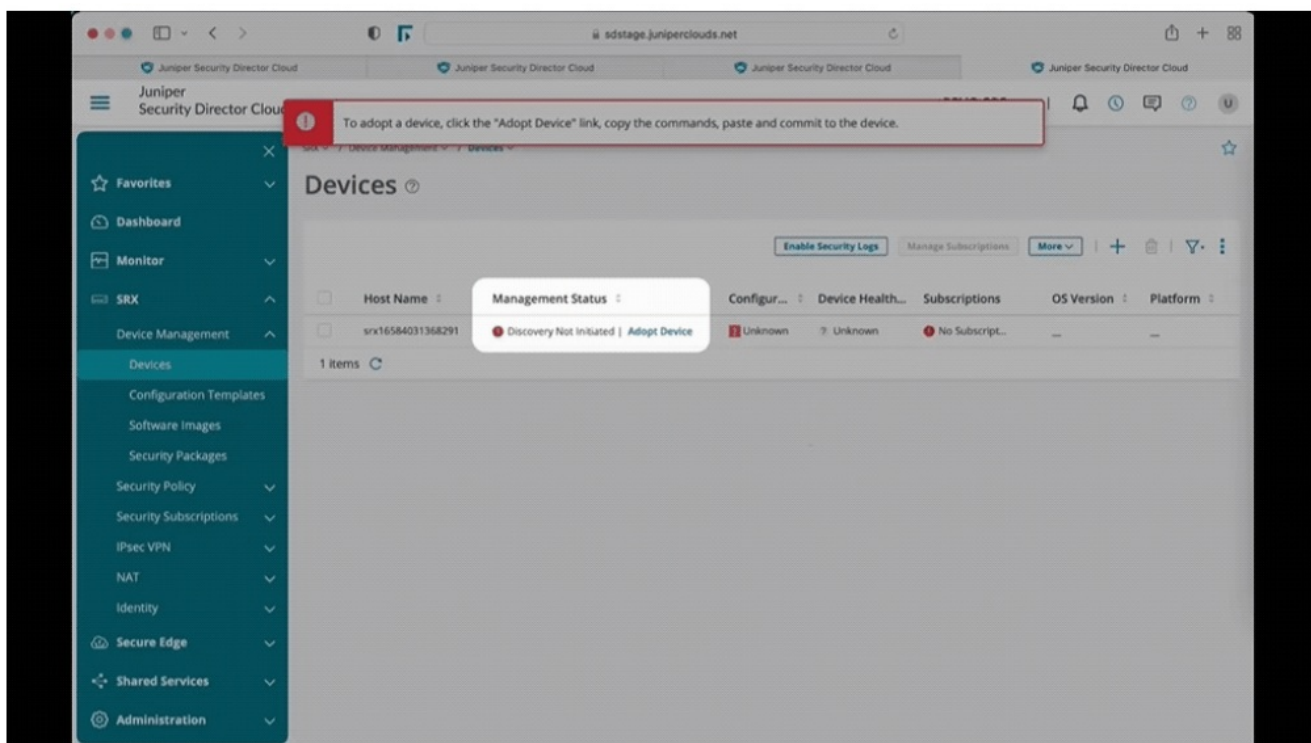
View your added subscriptions from Subscriptions>SRX Management Subscriptions. If you do not see your subscriptions, go to Administration > Jobs page to view the status.

4. Go to [Juniper Security Director Cloud](#), go to SRX > Device Management > Devices, and click the + icon to add your devices.
5. Click Adopt SRX Devices and select SRX Devices to add devices or select SRX Clusters to add device clusters.



Follow the on-screen instructions to continue

6. Copy and paste the commands from the devices page to the SRX Series Firewall or the primary cluster device console, and commit the changes.



It will take few seconds for the device discovery. After device discovery is successful, verify the following fields on the **Devices** page:

- Management Status changes from Discovery in progress to Up.
- Inventory Status and Device Config Status changes from Out of Sync to In Sync.

NOTE: In case of discovery failure, go to Administration > Jobs page to view the status.

You're ready to associate devices to your Juniper Security Director Cloud subscription. To continue, proceed to **"Step 2: Up and Running" on page 10** .

Step 2: Up and Running

IN THIS SECTION

- Associate Devices with Your Juniper Security Director Cloud "Subscrbr on | 11

Associate Devices with Your Juniper Security Director Cloud "Subscrbr on

1. Go to SRX >Device Management >Devices, click Manage Subscriptions and follow the on-screen instructions.

MANAGE SUBSCRIPTIONS ?

Number of devices selected 1

Subscriptions

Select a subscription below. You can also add new subscriptions by clicking [Add Subscriptions](#)

Subscription

10Devices (S-SD-1-C-1)

10Devices (S-SD-1-C-1)

Usage 1 of 10 devices

Expiry 08 Nov 2027

Cancel

OK

2. Verify the subscription from Administration > Subscriptions > SRX Management Subscriptions. The subscription status changes to

Active

Administration / Subscriptions

Subscriptions ?

To add subscriptions you will need an SSRN code. Click the "Add Subscription" button and enter the details.

The trial subscription for SRX is added by default. For Secure Edge, you will need to explicitly add a trial license. Reach out to your sales representative or account manager to get a Secure Edge trial subscription, or purchase new subscriptions.

[Add Subscriptions](#)

SRX Management Subscriptions

You will need to add devices and associate them to a subscription. To do this go to [SRX > Device Management > Devices](#).

	Name	Entitlement	Actual Usage	Status	Expiry Date	Plan	SSRN
<input type="checkbox"/>	DEMO-Test02	Devices: 10 Devices	1	Active	Mon, 08 Nov 2027 (GMT)	S-SD-1-C-1 (Qty 10)	XXXXXXXXXXXX

1 item

Congratulations! You have successfully added devices to Juniper Security Director Cloud!

Step 3: Keep Going

IN THIS SECTION

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

What's Next?

If You Want To	Then
Create or import a security policy, add a rule to the security policy, and deploy the security policy on the device	See About the SRX Policy Page
Set up the Content Security profiles to secure your network multiple security threat types	See About the Content Security Profiles Page
Configure ATP Cloud to protect all hosts in your network against evolving security threats	See File Inspection Profiles Overview
View the traffic logs and network events including viruses found, interfaces that are down, number of attacks, CPU spikes, system reboots, and sessions	See About the Session Page and About the All Security Events Page

General Information

If You Want To	Then
See all the available documentation for Juniper Security Director Cloud	Visit Security Director Cloud

Learn With Videos

If You Want To	Then
Learn more about Juniper Security Director Cloud	Watch What is Juniper Security Director Cloud?
See a demonstration of how to get started with a Juniper Security Director Cloud account	Watch Getting Started with Juniper Security Director Cloud Account
Learn how to manage security with Juniper Security Director Cloud and Juniper Secure Edge	Watch Manage Security Anywhere With Security Director Cloud and Juniper Secure Edge

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.



	<p>Juniper NETWORKS Onboard SRX Series Firewalls to Security Director Cloud [pdf] User Guide</p> <p>SRX1600, Onboard SRX Series Firewalls to Security Director Cloud, Series Firewalls to Security Director Cloud, Firewalls to Security Director Cloud, Security Director Cloud, Director Cloud, SRX2300</p>
---	--

References

-  sdcloud.juniperclouds.net/
-  [Juniper Security Director Cloud Documentation | Juniper Networks](#)
-  [SRX1600 Firewall Hardware Guide | Juniper Networks](#)
-  [SRX2300 Firewall Hardware Guide | Juniper Networks](#)
-  [Cloud-Ready SRX Series Firewalls with Mist | Quick Start | Step 1: Begin | Juniper Networks](#)
-  [Add an SRX Series Firewall to Juniper Security Director Cloud | J-Web for SRX Series 23.4 | Juniper Networks](#)
-  [Add Devices to Juniper Security Director Cloud | Juniper Networks](#)
-  [File Inspection Profiles Overview | SD Cloud | Juniper Networks](#)
-  [About the All Security Events Page | SD Cloud | Juniper Networks](#)
-  [About the SRX Policy Page | SD Cloud | Juniper Networks](#)
-  [About the Session Page | SD Cloud | Juniper Networks](#)
-  [About the Content Security Profiles Page | SD Cloud | Juniper Networks](#)
-  [Subscriptions Overview | SD Cloud | Juniper Networks](#)
-  [SRX Adoption - Mist](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.