Engineering
Simplicity

Quick Start

Onboard SRX Series Firewalls to Juniper Security Director Cloud

IN THIS GUIDE

Step 1: Begin

IN THIS SECTION

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

- "Greenfield onboarding" on page 2: Onboard new SRX Series Firewalls.

  Greenfield onboarding involves onboarding new SRX Series firewalls to Juniper Security Director Cloud. This process includes purchasing subscriptions, scanning the QR code on the device, and following the on-screen instructions to add the firewall to Juniper Security Director Cloud.

  You can also onboard new, greenfield, SRX Series Firewalls to Juniper Security Director Cloud using ZTP. For details, see Add Devices Using Zero Touch Provisioning.

- "Brownfield onboarding" on page 7: Onboard existing, in-service SRX Series Firewalls.

  Brownfield onboarding involves onboarding existing, in-service SRX Series Firewalls to Juniper Security Director Cloud. This process includes logging in to Juniper Security Director Cloud portal, adopting the device to generate the Junos OS CLI commands, copying the CLI commands into the firewall's CLI, and then committing the changes.

For supported SRX Series Firewalls, see Juniper Security Director Cloud Supported Firewalls.

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

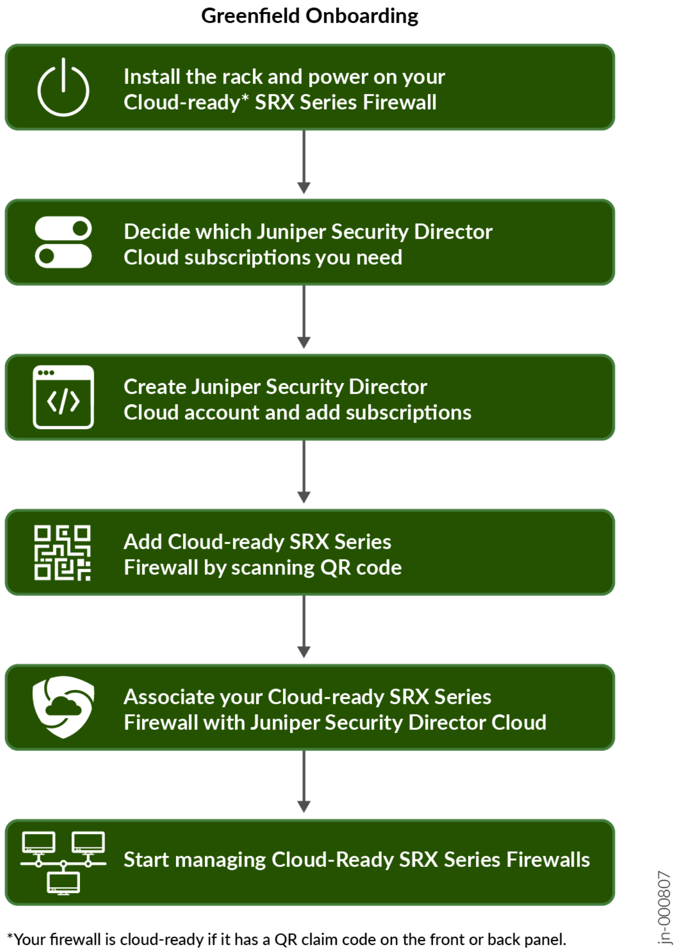
Cloud-ready SRX Series Firewalls have a QR or claim code on the chassis for quick onboarding to Juniper Security Director Cloud. Cloud-ready SRX Series Firewalls offer advanced security services, seamless integration, and protection for cloud deployments. You can onboard the cloud-ready SRX Series Firewalls using your mobile phone.

For information about supported cloud-ready and non-cloud-ready SRX Series Firewalls, see Juniper Security Director Cloud Supported Firewalls.

NOTE: To onboard non-cloud-ready SRX Series Firewalls to Juniper Security Director Cloud using ZTP, see Add Devices Using Zero Touch Provisioning.

In this section, we will learn how to onboard cloud-ready SRX Series Firewalls using a QR code.

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


Greenfield Onboarding
Install the rack and power on your Cloud-ready* SRX Series Firewall
Decide which Juniper Security Director Cloud subscriptions you need
Create Juniper Security Director Cloud account and add subscriptions
Add Cloud-ready SRX Series Firewall by scanning QR code
Associate your Cloud-ready SRX Series Firewall with Juniper Security Director Cloud
Start managing Cloud-Ready SRX Series Firewalls
jn-000807

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

Before You Begin:

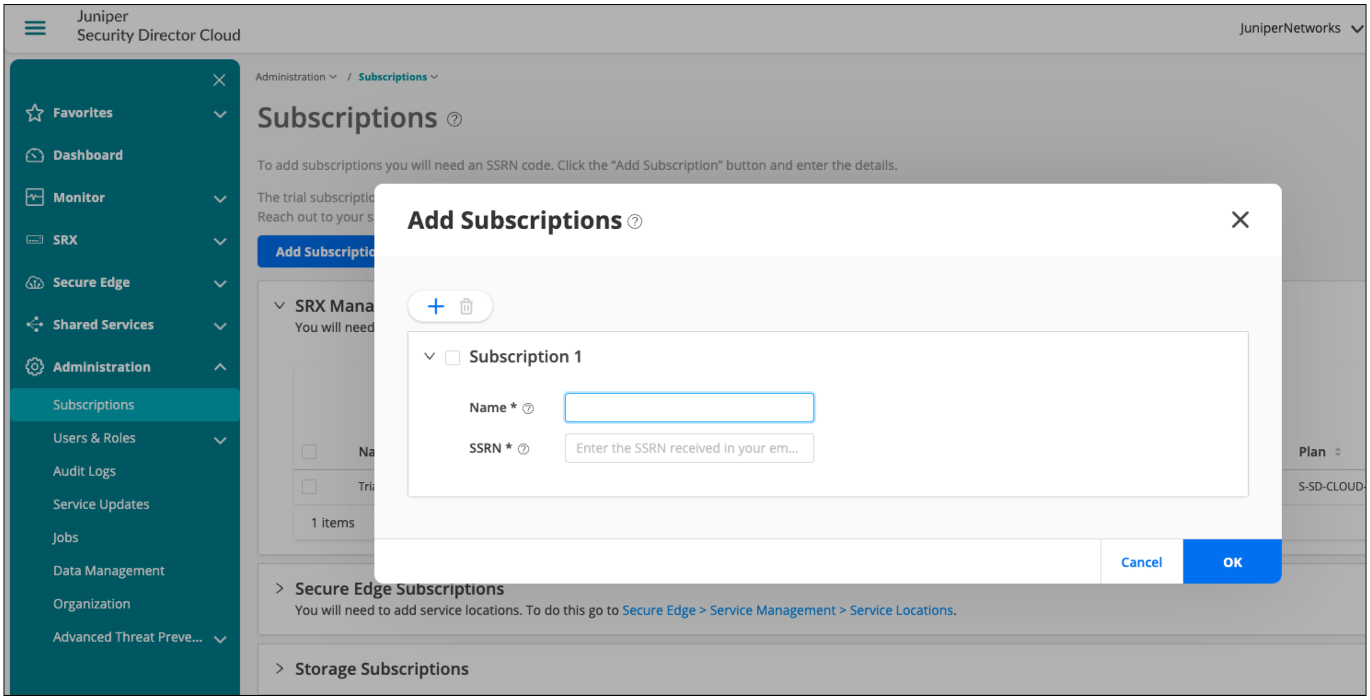
Install the rack and power on your cloud-ready SRX Series Firewall. For instructions specific to your device, see the applicable hardware guide.

NOTE: DHCP is enabled on all interfaces on cloud-ready SRX Series Firewalls 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. Contact your sales representative or account manager to purchase subscriptions. You can also use a 30-day trial subscription that is available in the portal by default.
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**.



Subscriptions

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

The trial subscriptio
Reach out to your s

SRX Mana
You will need

	Na	Plan
□	Tri	S-SD-CLOUD-

1 items

Add Subscriptions

Subscription 1

Name *

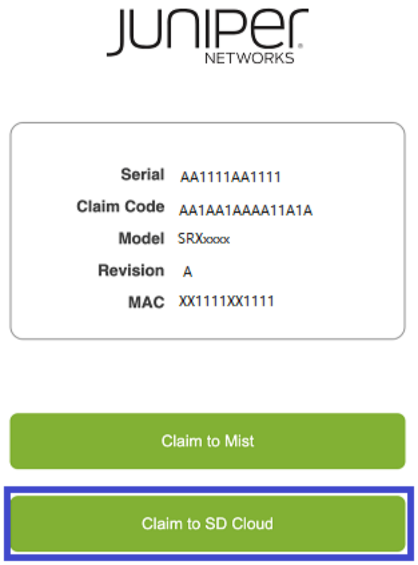
SSRN * Enter the SSRN received in your em...

Secure Edge Subscriptions
You will need to add service locations. To do this go to Secure Edge > Service Management > Service Locations.

Storage Subscriptions

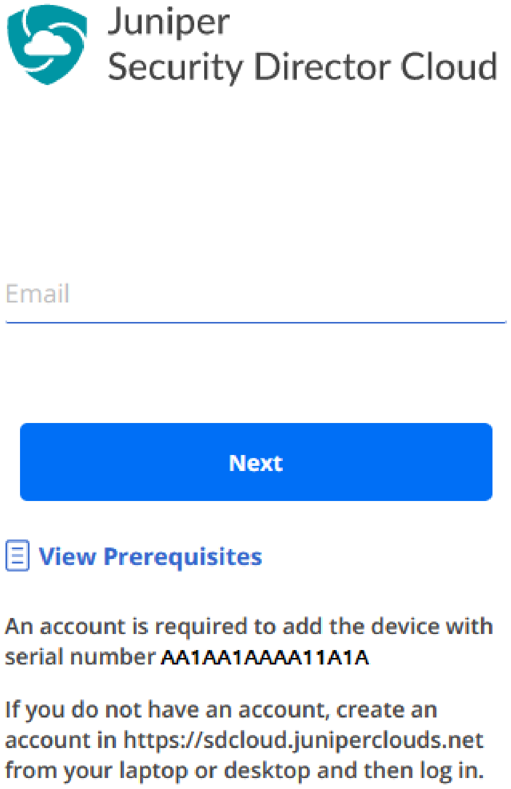
View your added subscriptions from **Subscriptions** > **SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

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

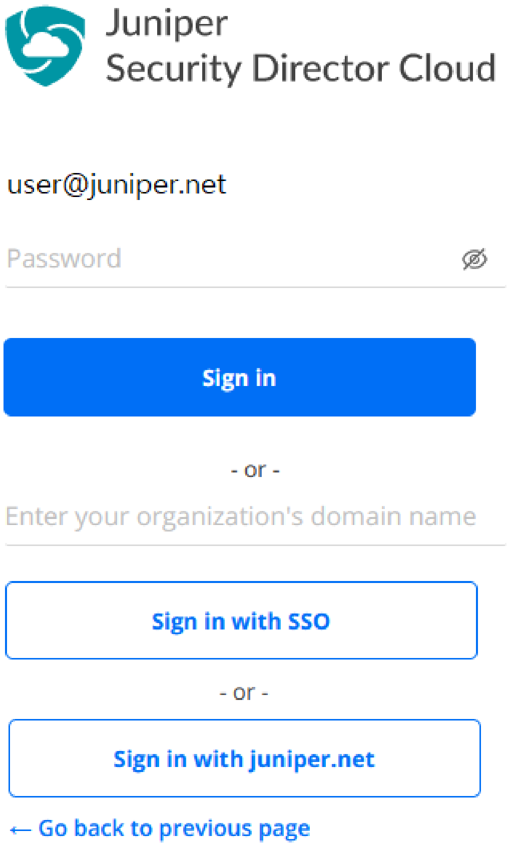
5. Read the prerequisites, enter your e-mail address, and click **Next**.



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

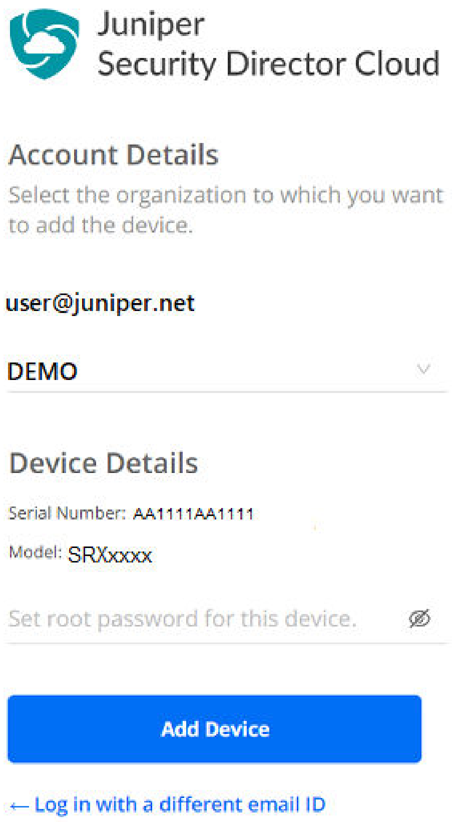
If you do not have an account, create an account in https://sdcloud.juniperclouds.net from your laptop or desktop and then log in.

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



user@juniper.net

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

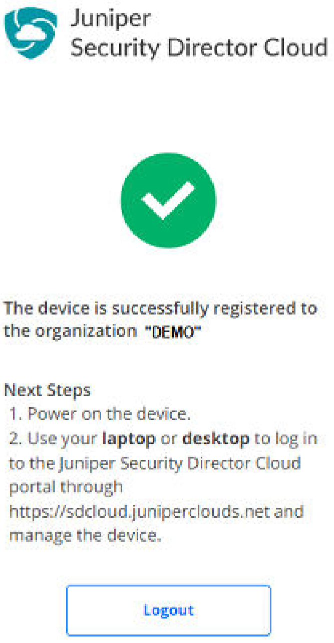
Device Details

Serial Number: AA1111AA1111

Model: SRXxxxx

Set root password for this device.

Congratulations! You've successfully registered your device to the organization and added your device to Juniper Security Director Cloud. Log out from the page in your mobile phone.



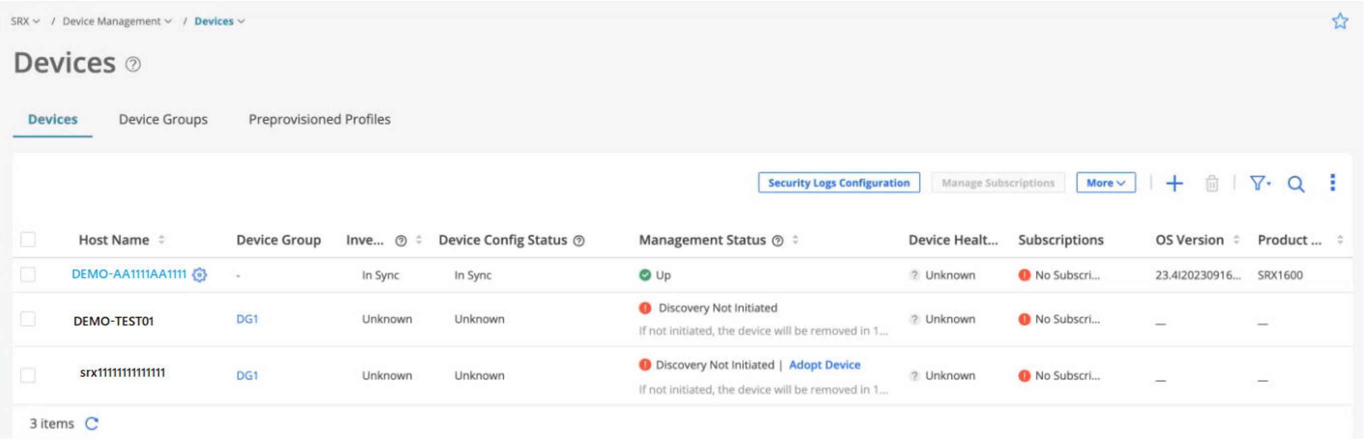
The device is successfully registered to the organization "DEMO"

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.

8. Power on your 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.



Host Name	Device Group	Inve...	Device Config Status	Management Status	Device Healt...	Subscriptions	OS Version	Product ...
DEMO-AA1111AA1111	-	In Sync	In Sync	Up	Unknown	No Subscri...	23.4I20230916...	SRX1600
DEMO-TEST01	DG1	Unknown	Unknown	Discovery Not Initiated If not initiated, the device will be removed in 1...	Unknown	No Subscri...	—	—
srx11111111111111	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:

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

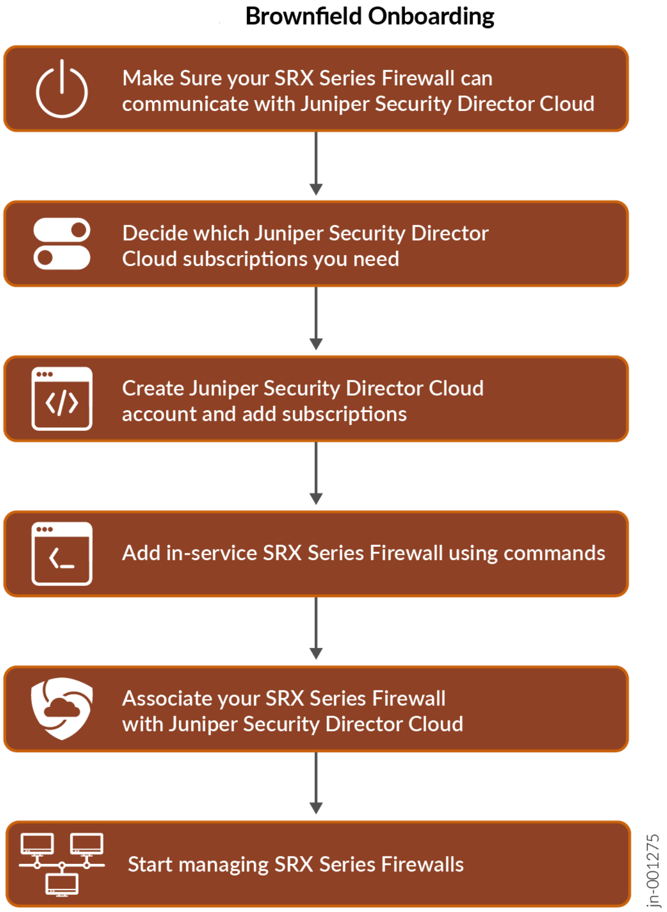
Congratulations! You've successfully onboarded your cloud-ready SRX Series Firewall. You're now ready to associate devices to your Juniper Security Director Cloud subscription.

To continue, proceed to "Step 2: Up and Running" on page 12.

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

In this section, we will learn how to onboard existing, in-service, SRX Series Firewalls using CLI commands.

Figure 2: Onboard SRX Series Firewalls to Juniper Security Director Cloud in Brownfield Deployment


Brownfield Onboarding
Make Sure your SRX Series Firewall can communicate with Juniper Security Director Cloud
Decide which Juniper Security Director Cloud subscriptions you need
Create Juniper Security Director Cloud account and add subscriptions
Add in-service SRX Series Firewall using commands
Associate your SRX Series Firewall with Juniper Security Director Cloud
Start managing SRX Series Firewalls
jn-001275

NOTE: You can also onboard existing, in-service (brownfield), SRX Series Firewalls using the following methods:

- To onboard (adopt) existing, in-service (brownfield), SRX Series Firewalls into Juniper Security Director Cloud using J-Web, see Add SRX Series Firewalls to Juniper Security Director Cloud Using J-Web.

- 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.

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 1: Home Region to FQDN Mapping

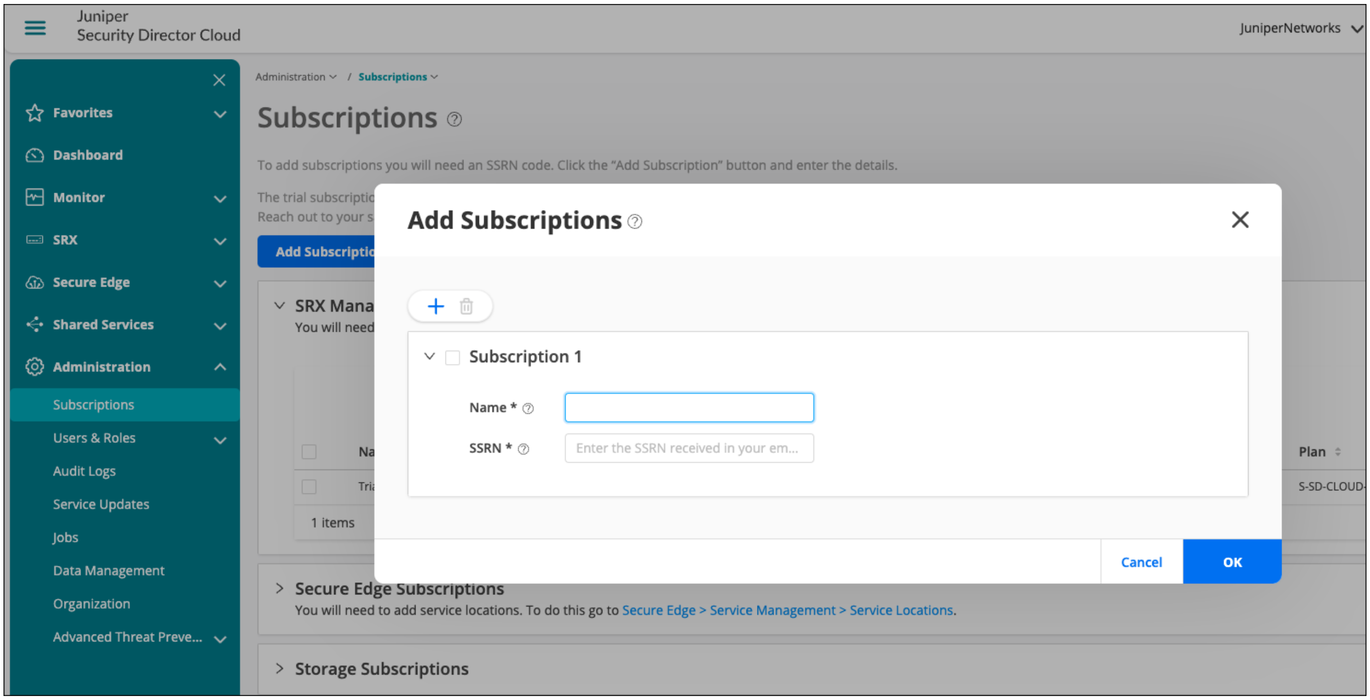
Region	Purpose	Port	FQDN
North Virginia, U.S.	ZTP	443	jsec2-virginia.juniperclouds.net
	Outbound SSH	7804	srx.sdcloud.juniperclouds.net
	Syslog TLS	6514	srx.sdcloud.juniperclouds.net
Ohio, U.S.	ZTP	443	jsec2-ohio.juniperclouds.net
	Outbound SSH	7804	srx.jsec2-ohio.juniperclouds.net
	Syslog TLS	6514	srx.jsec2-ohio.juniperclouds.net
Montreal, Canada	ZTP	443	jsec-montreal2.juniperclouds.net
	Outbound SSH	7804	srx.jsec-montreal2.juniperclouds.net
	Syslog TLS	6514	srx.jsec-montreal2.juniperclouds.net
Frankfurt, Germany	ZTP	443	jsec-frankfurt.juniperclouds.net
	Outbound SSH	7804	srx.jsec-frankfurt.juniperclouds.net
	Syslog TLS	6514	srx.jsec-frankfurt.juniperclouds.net

- 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. Contact your sales representative or account manager to purchase subscriptions. You can also use a 30-day trial subscription that is available in the portal by default.
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**.



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

The trial subscriptio

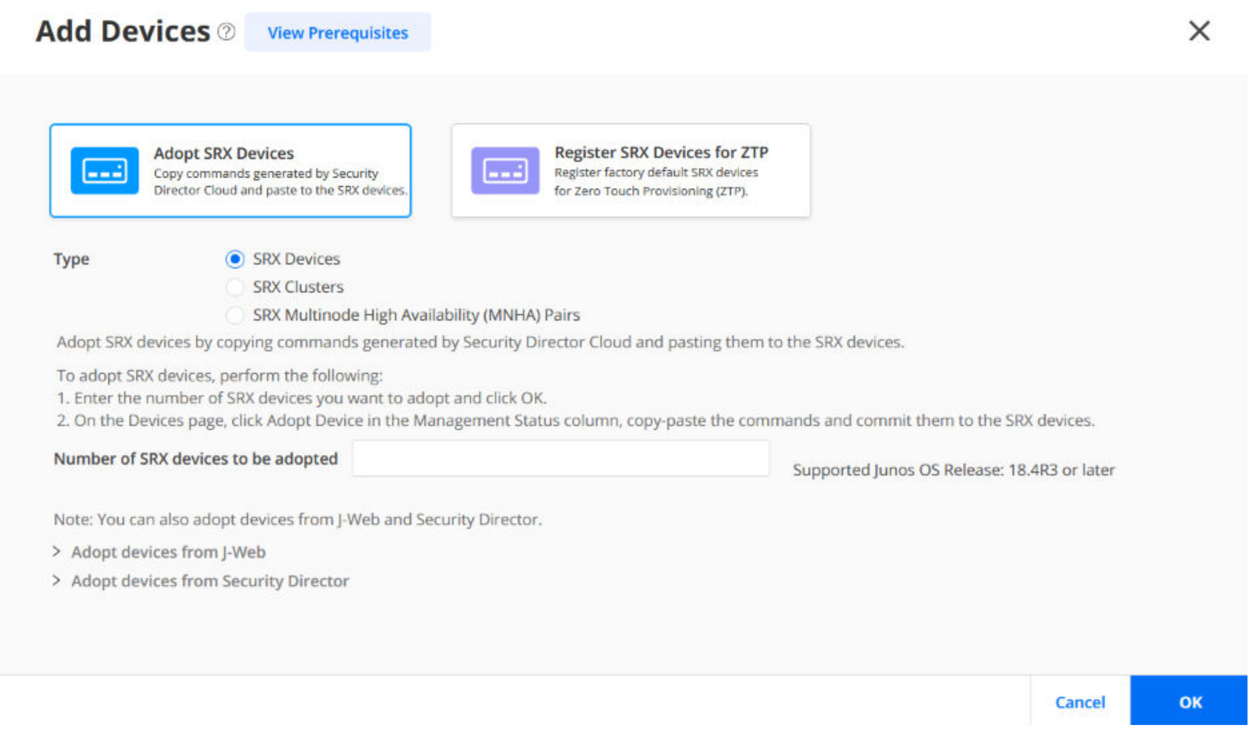
Reach out to your s

You will need

You will need to add service locations. To do this go to Secure Edge > Service Management > Service Locations.

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, select **SRX** > **Device Management** > **Devices**. Click the **+** icon to add your devices.
5. Click **Adopt SRX Devices** and select one of the following:
   - SRX Devices
   - SRX Clusters
   - SRX Multinode High Availability (MNHA) Pairs



Add Devices ⓘ View Prerequisites ✕

Adopt SRX Devices
Copy commands generated by Security Director Cloud and paste to the SRX devices.

Register SRX Devices for ZTP
Register factory default SRX devices for Zero Touch Provisioning (ZTP).

Type ● SRX Devices
○ SRX Clusters
○ SRX Multinode High Availability (MNHA) Pairs

Adopt SRX devices by copying commands generated by Security Director Cloud and pasting them to the SRX devices.

To adopt SRX devices, perform the following:
1. Enter the number of SRX devices you want to adopt and click OK.
2. On the Devices page, click Adopt Device in the Management Status column, copy-paste the commands and commit them to the SRX devices.

Number of SRX devices to be adopted ______ Supported Junos OS Release: 18.4R3 or later

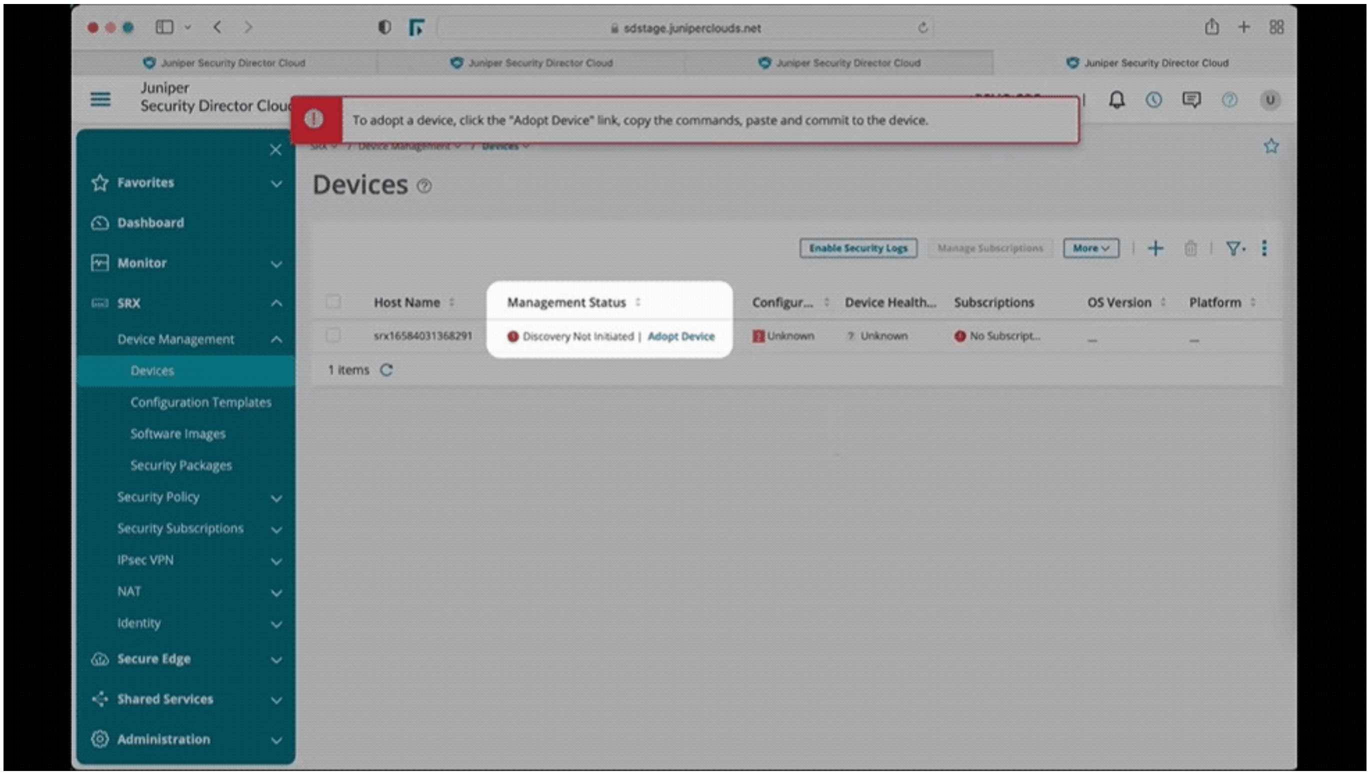
Note: You can also adopt devices from J-Web and Security Director.

> Adopt devices from J-Web
> Adopt devices from Security Director

Cancel OK

Follow the on-screen instructions to continue.

6. Copy and paste the commands from the devices page to the SRX Series Firewall. Paste the commands for the primary cluster device console or each device in the MNHA pair. Commit the changes.



To adopt a device, click the "Adopt Device" link, copy the commands, paste and commit to the device.

Devices ⓘ

Host Name	Management Status	Configur...	Device Health...	Subscriptions	OS Version	Platform
srx16584031368291	Discovery Not Initiated | Adopt Device	Unknown	? Unknown	No Subscript...	–	–

1 items

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, navigate to **Administration** > **Jobs** page to view the status.

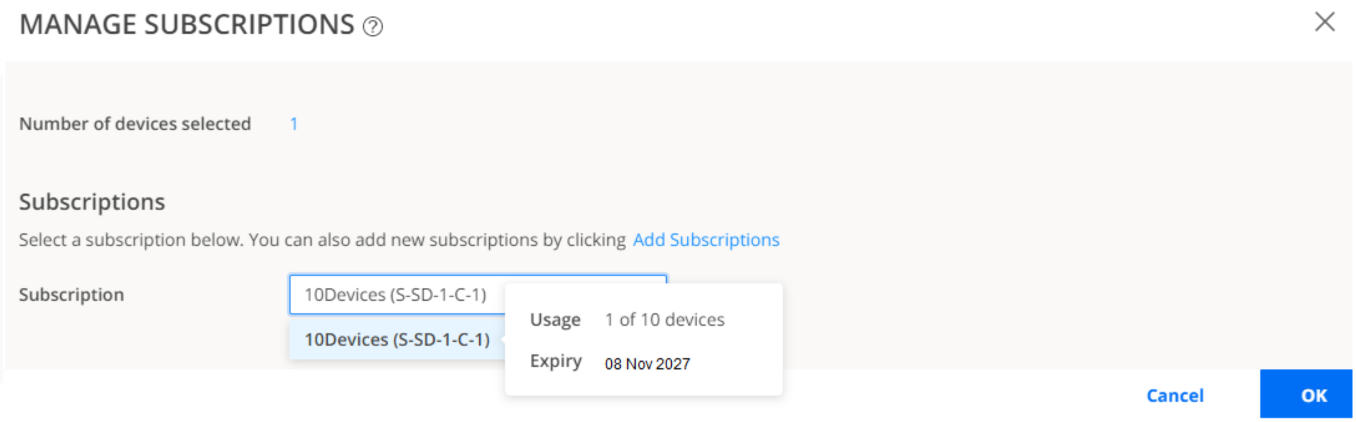
You're ready to associate devices to your Juniper Security Director Cloud subscription. To continue, proceed to "Step 2: Up and Running" on page 12.

Step 2: Up and Running

IN THIS SECTION

Associate Devices with Your Juniper Security Director Cloud Subscription

1. Go to **SRX** > **Device Management** > **Devices**, select the device, and click **Manage Subscriptions**. 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

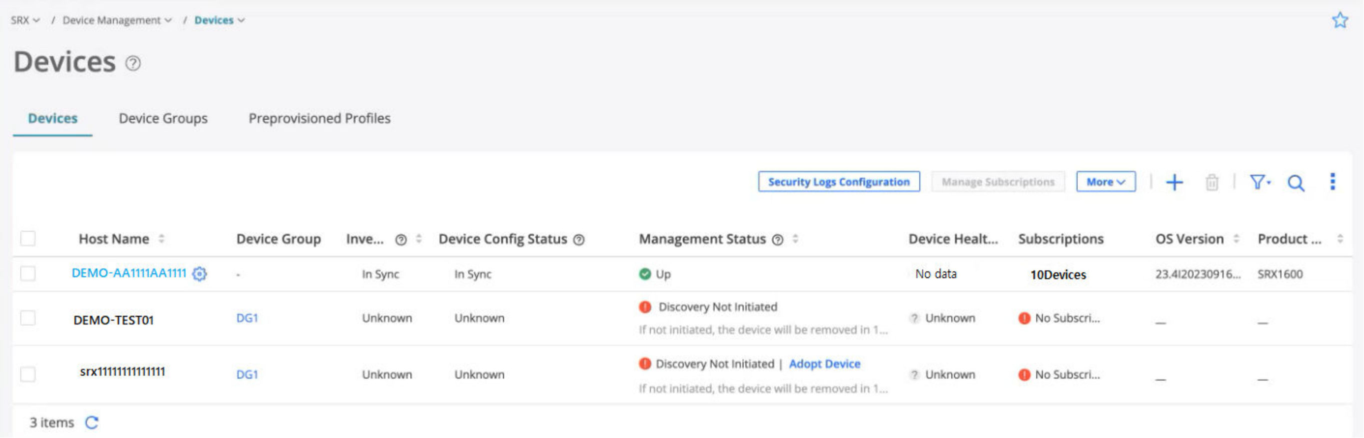
Subscription: 10Devices (S-SD-1-C-1)

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

Usage: 1 of 10 devices

Expiry: 08 Nov 2027

2. Verify that the **Subscriptions** column displays the subscription name for your device.



	Host Name	Device Group	Inve...	Device Config Status	Management Status	Device Healt...	Subscriptions	OS Version	Product ...
□	DEMO-AA1111AA1111	-	In Sync	In Sync	Up	No data	10Devices	23.4I20230916...	SRX1600
□	DEMO-TEST01	DG1	Unknown	Unknown	Discovery Not Initiated If not initiated, the device will be removed in 1...	Unknown	No Subscri...	_	_
□	srx11111111111111	DG1	Unknown	Unknown	Discovery Not Initiated | Adopt Device If not initiated, the device will be removed in 1...	Unknown	No Subscri...	_	_

Congratulations! You have successfully associated your device to Juniper Security Director Cloud.

Step 3: Keep Going

IN THIS SECTION

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 devices	See About the SRX Policy Page
Set up the Content Security profiles to secure your network from 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

(Continued)

If You Want To	Then
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 the 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