JUNIPER NETWORKS | Engineering Simplicity

Quick Start

Onboard SRX Series Firewalls to Security Director Cloud

IN THIS GUIDE

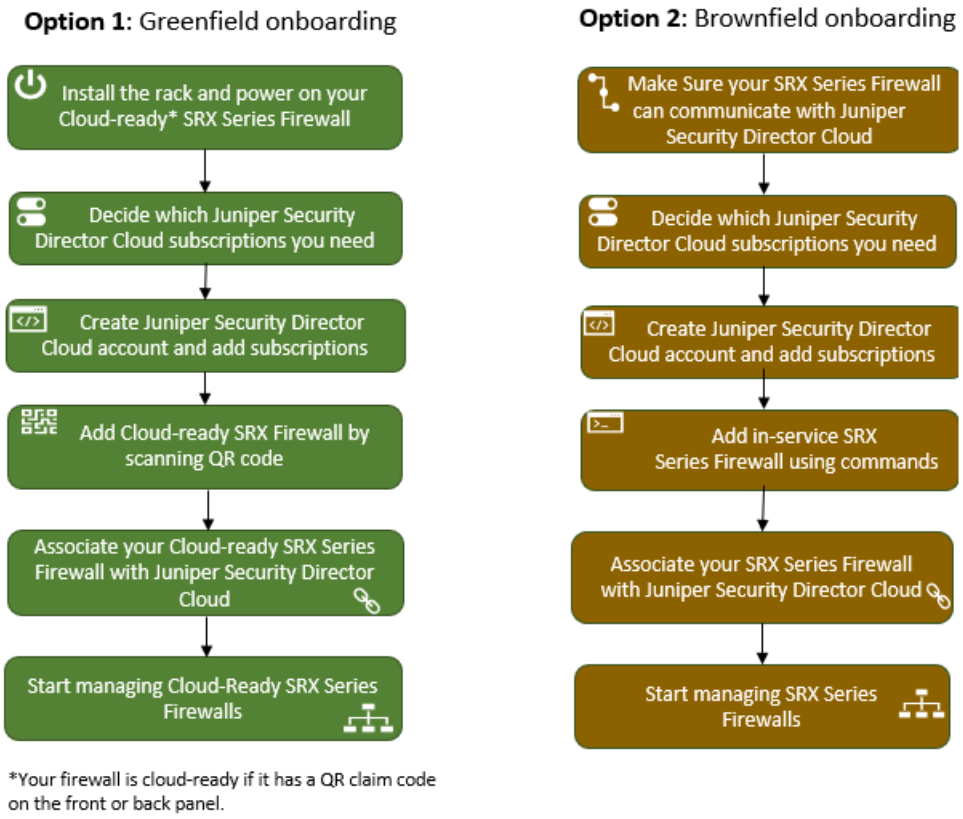
Step 1: Begin

IN THIS SECTION

This guide walks you through the simple steps to onboard Juniper Networks® SRX Series Firewalls to 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



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

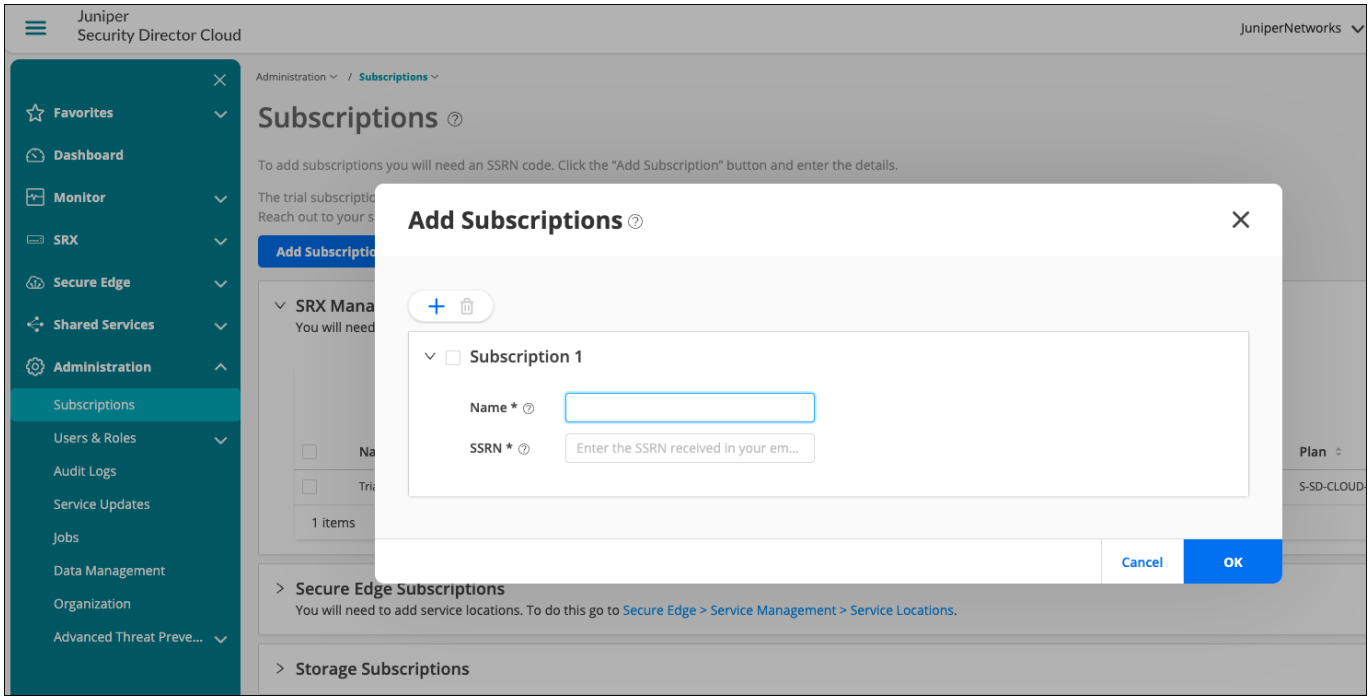
Firewall	Install and Maintain Hardware
SRX1600	SRX1600 Firewall Hardware Guide
SRX2300	SRX2300 Firewall Hardware Guide

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**.

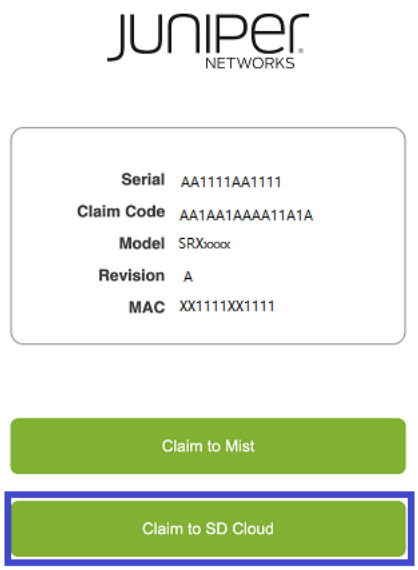
   Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account.

3. Log in to the Juniper Security Director Cloud portal, click **Add Subscriptions**, enter details, and click **OK**

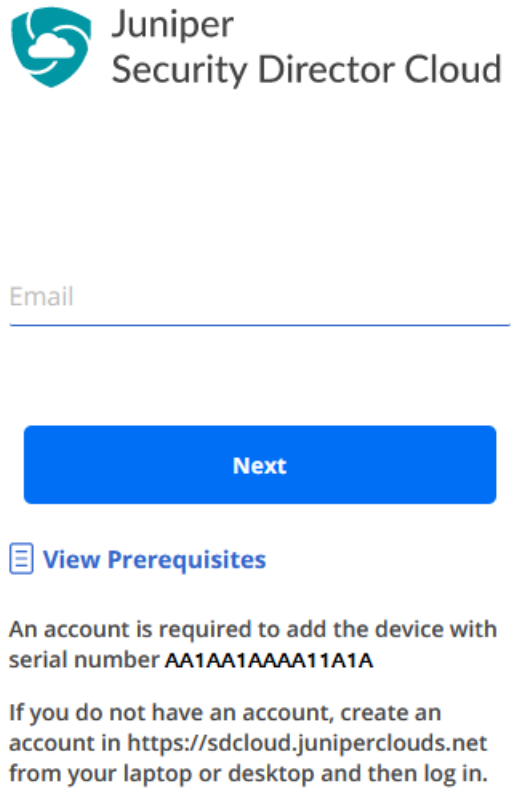


View your added subscriptions from **Subscriptions**>**SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

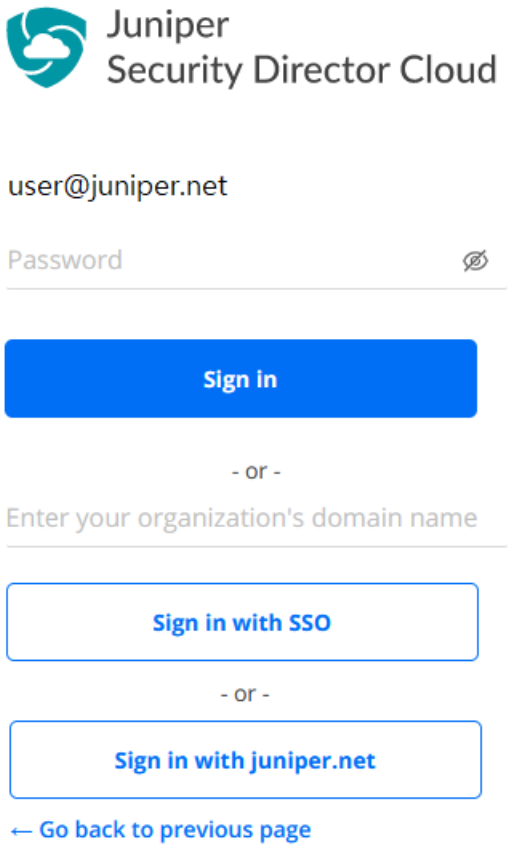
4. Use your mobile phone to scan the QR code on the cloud-ready SRX Series Firewall. Click the displayed link and select **Claim to SD Cloud** to go to Juniper Security Director Cloud login page.



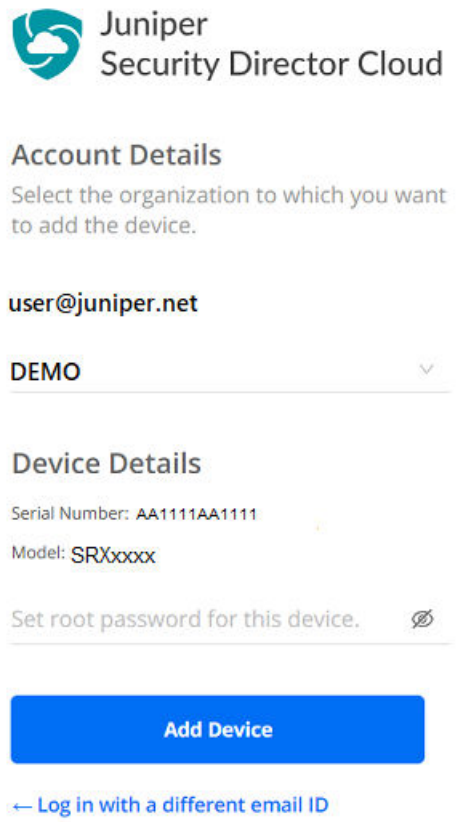
5. Read the prerequisites, enter your e-mail address, and click **Next**.



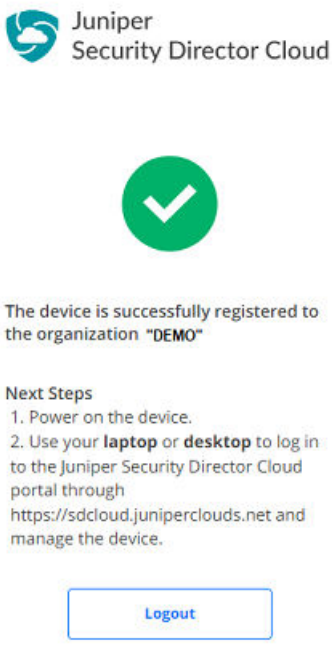
6. Follow the on-screen instructions to sign in.



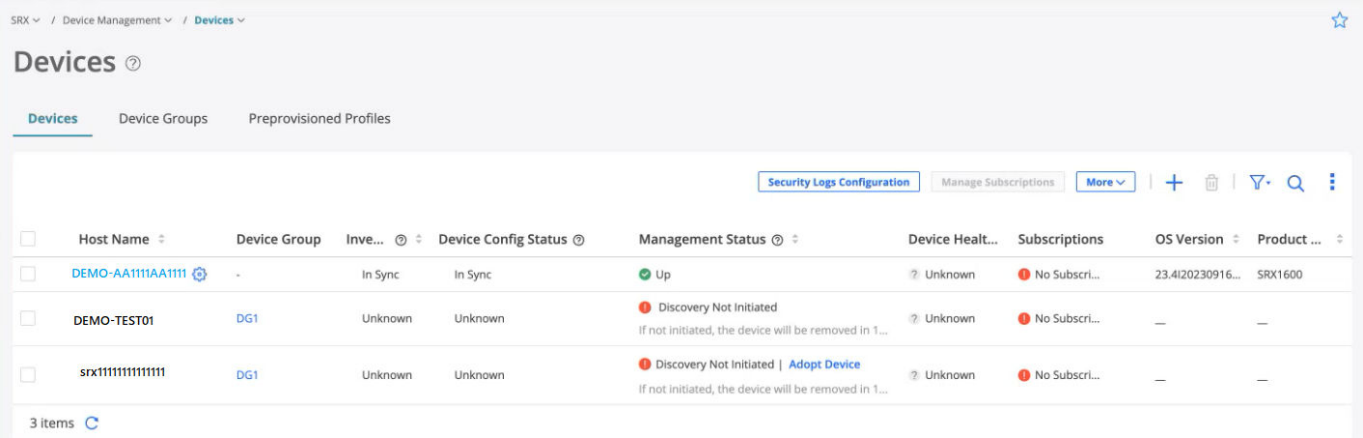
7. Select the organization to add your device, enter the root password, and click **Add Device**.



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



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.



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

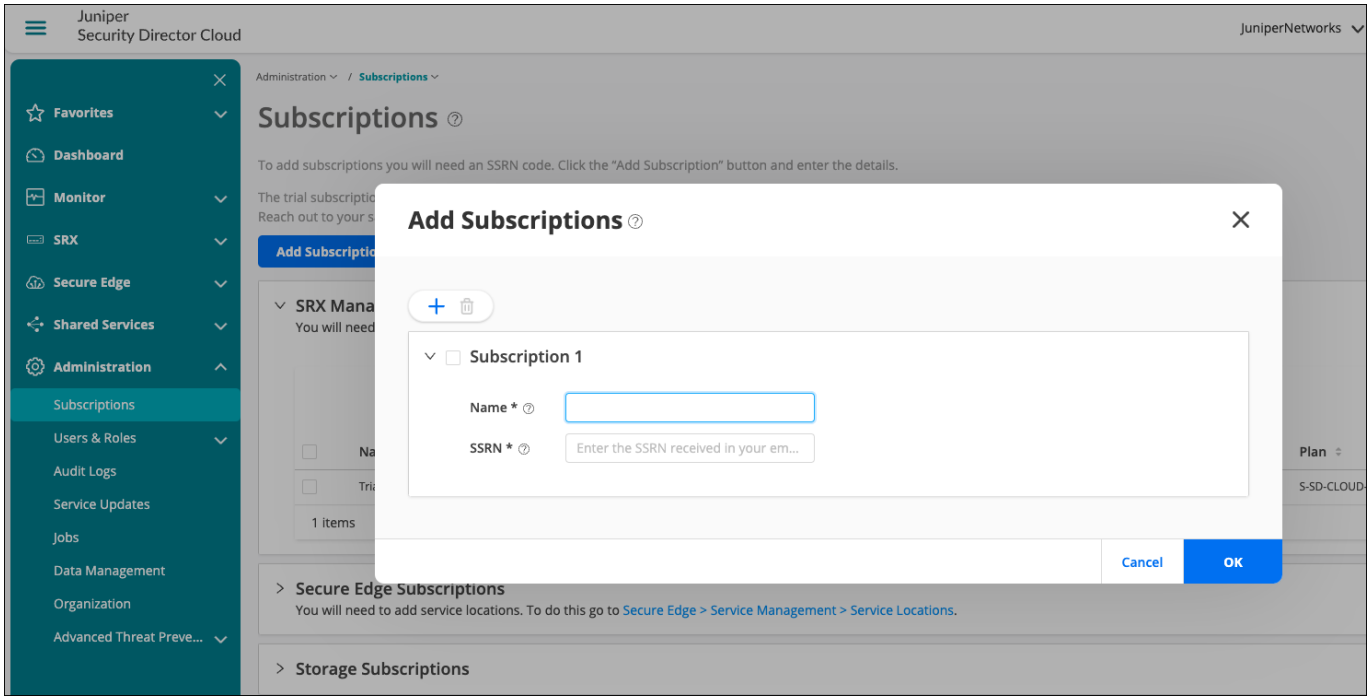
Home Region	Purpose	Port	FQDN
North Virginia	ZTP Outbound SSH System Log messages over TLS	443 7804 6514	jsec-virginia.juniperclouds.net srx.sdcloud.juniperclouds.net srx.sdcloud.juniperclouds.net
Ohio	ZTP Outbound SSH System log messages over TLS	443 7804 6514	jsec-ohio.juniperclouds.net srx.jsec-ohio.juniperclouds.net srx.jsec-ohio.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 and contact your sales representative or account manager to purchase subscriptions.
2. Go to https://sdcloud.juniperclouds.net/ and click **Create an organization account**.

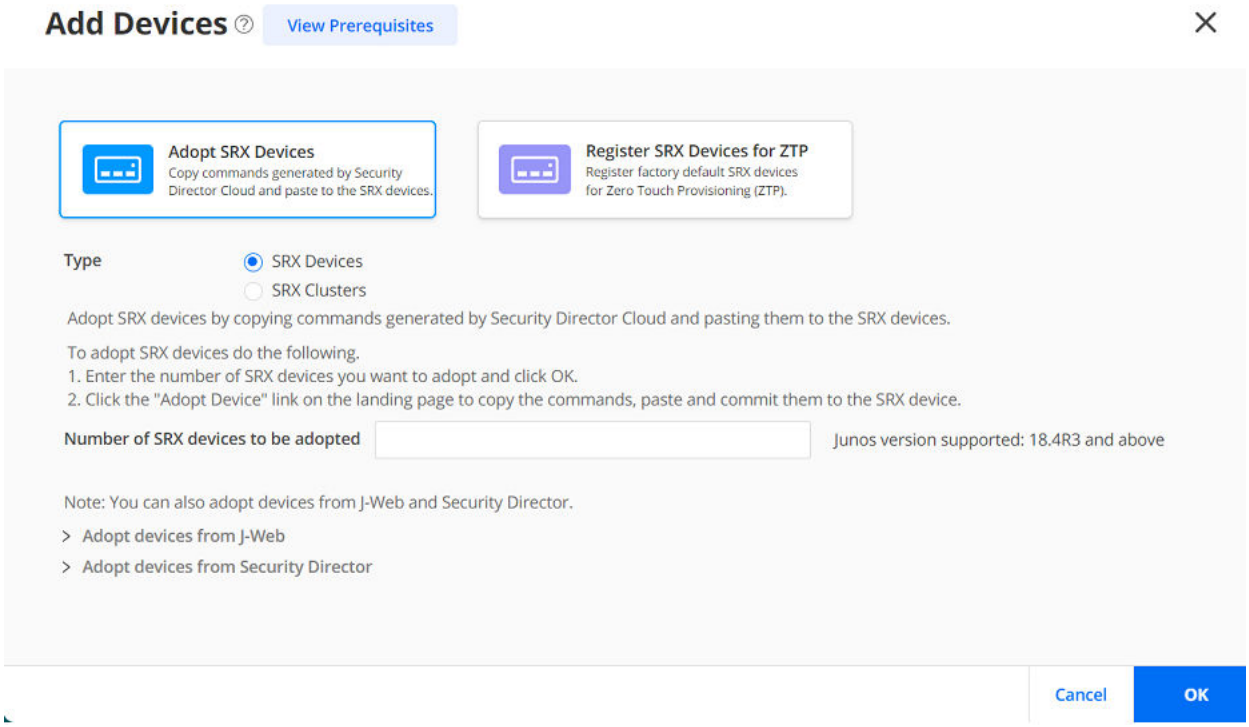
   Follow the on-screen instructions to activate your account. It takes up to 7 working days to approve your account activation request.

3. Log in to the Juniper Security Director Cloud portal, click **Add Subscriptions**, enter details, and click **OK**



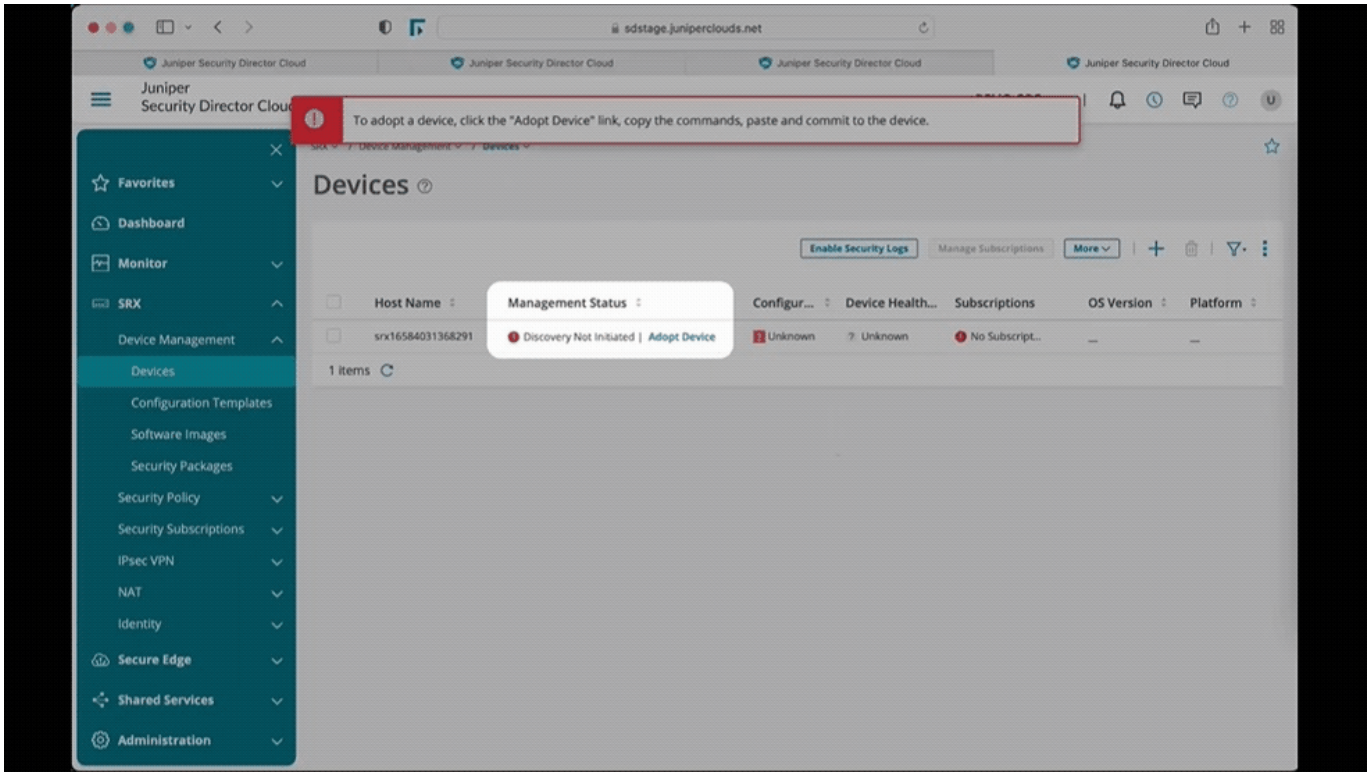
View your added subscriptions from **Subscriptions**>**SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

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.

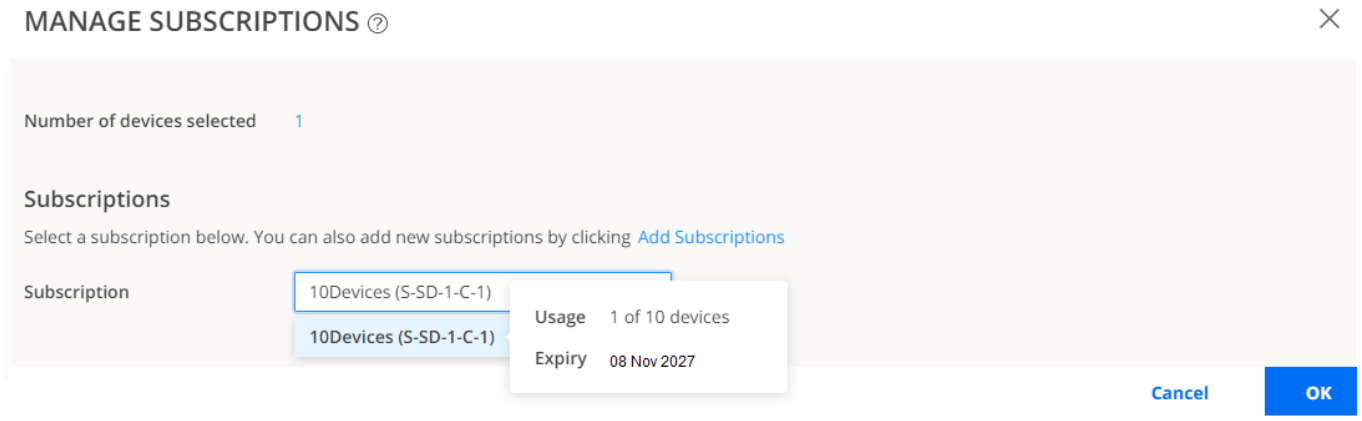
You're ready to associate devices to your Juniper Security Director Cloud subscription. To continue, proceed to "Step 2: Up and Running" on page 10 .

Step 2: Up and Running

IN THIS SECTION

Associate Devices with Your Juniper Security Director Cloud Subscription

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

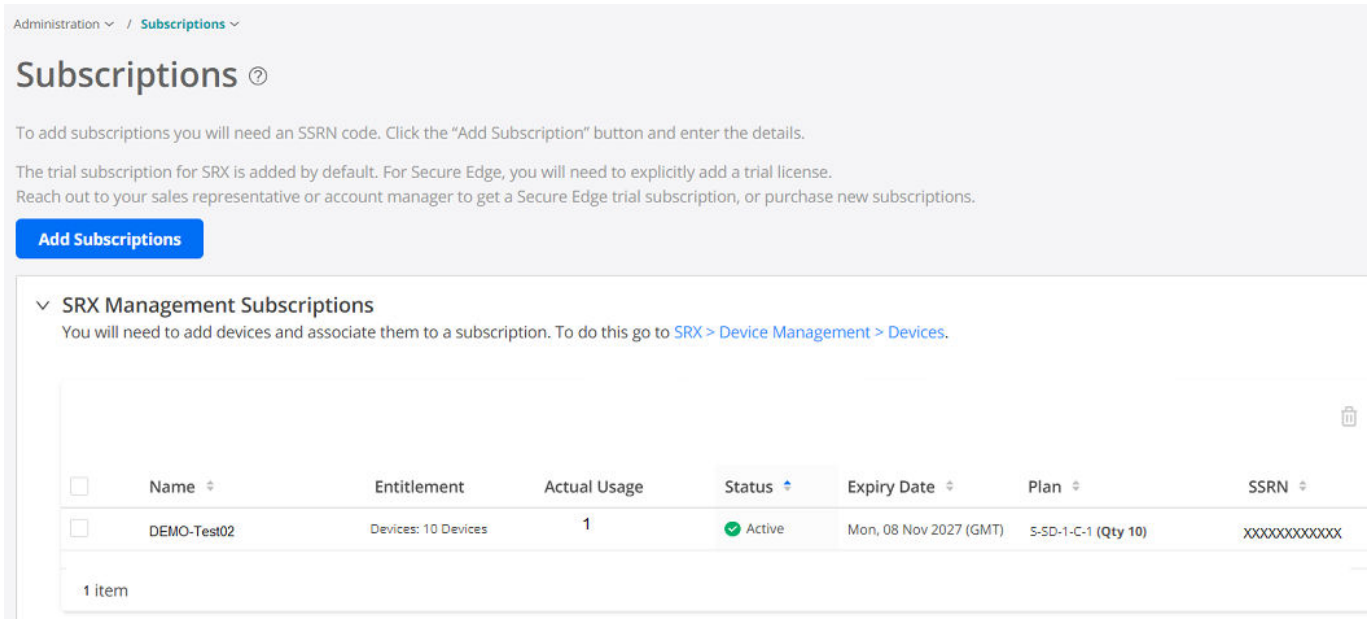


2. Verify the subscription from **Administration** > **Subscriptions** > **SRX Management Subscriptions**.

   The subscription status changes to

   Active

   .



   Congratulations! You have successfully added devices 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
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