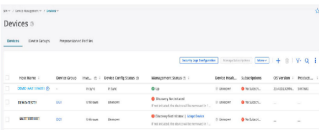**Manuals+** — User Manuals Simplified.

JUNIPER
NETWORKS

**Onboard SRX
Series Firewalls
to Juniper
Security
Director Cloud**

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

Contents

JUNIPER
NETWORKS®

Juniper NETWORKS Onboard SRX Series Firewalls to Juniper Security Director Cloud

Product Usage Instructions

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

1. Install the rack and power on your cloud-ready SRX Series Firewall.
2. Decide on the needed subscriptions and purchase them or use the 30-day trial subscription.
3. Go to **https://sdcloud.juniperclouds.net**/ and create an organization account.
4. Add the purchased subscriptions by logging into the Juniper Security Director Cloud portal.
5. Scan the QR code on the cloud-ready SRX Series Firewall with your mobile phone.
6. Follow the on-screen instructions to sign in and add your device to the organization.
7. Power on your cloud-ready SRX Series Firewall and log in to the Juniper Security Director Cloud portal from your laptop or desktop to view the added device.

FAQ

Q: How do I know if my firewall is cloud-ready?

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

Q: How can I view my added subscriptions?

A: You can view your added subscriptions by navigating to Subscriptions > SRX Management Subscriptions in the Juniper Security Director Cloud portal.

Q: What should I do if I cannot see my subscriptions?

A: If you do not see your subscriptions, go to the Administration > Jobs page to view the status.

Q: How long does it take to approve my organization account?

A: It may take up to 7 working days to approve your account after following the on-screen instructions to activate your account.

Quick Start

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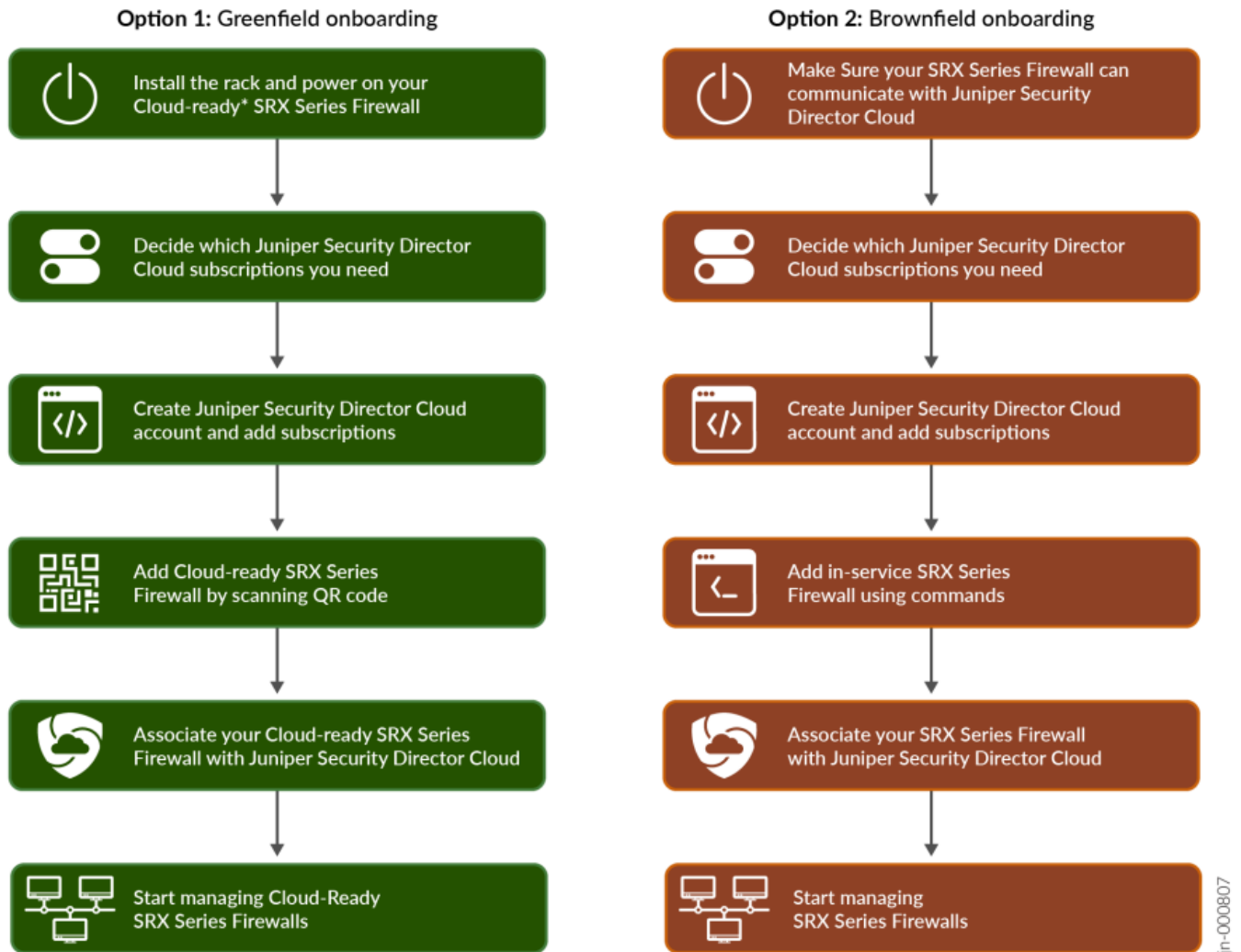
*Your firewall is cloud-ready if it has a QR claim code on the front or back panel.

- **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 the 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**
SRX4300	**SRX4300 Firewall 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 and 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. To add the purchased subscriptions, log in to the Juniper Security Director Cloud portal, click Add Subscriptions, enter details, and click OK.
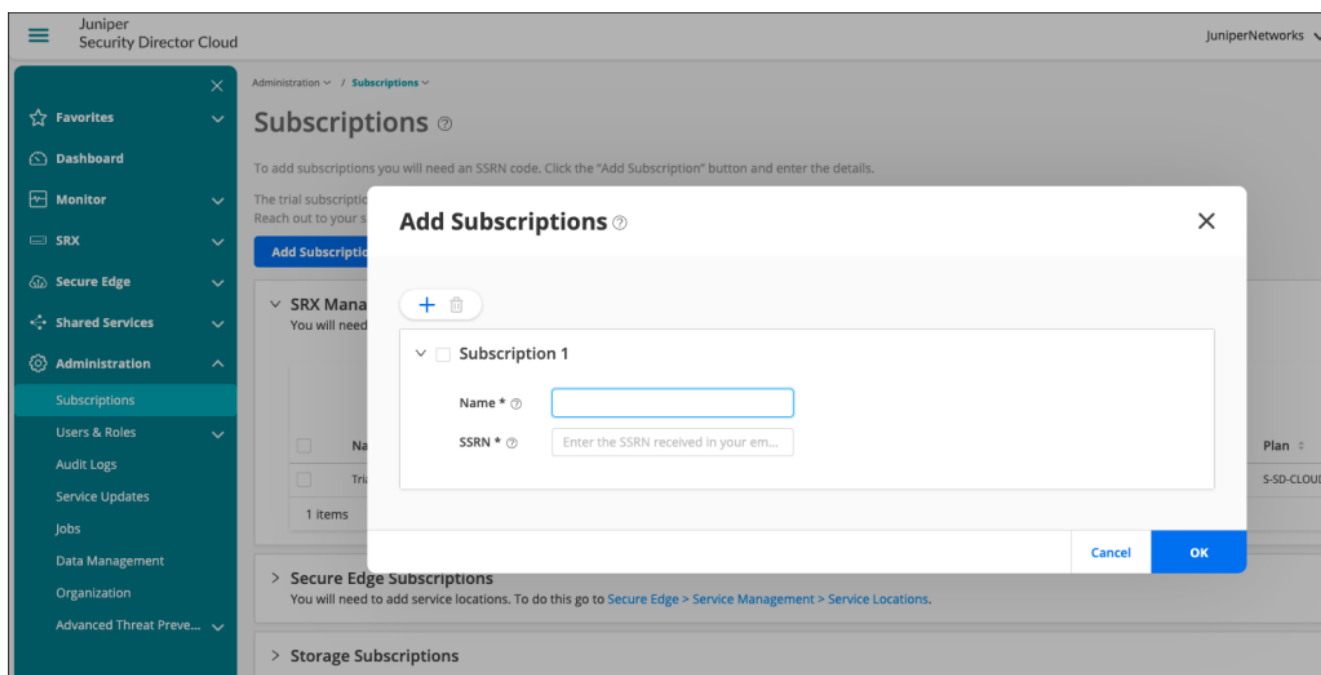
   - View your added subscriptions from Subscriptions>SRX Management Subscriptions. If you do not see your subscriptions, go to Administration > Jobs page to view the status.
4. Use your mobile phone to scan the QR code on the cloud-ready SRX Series Firewall. Click the displayed link and select Claim to SD Cloud to go to the Juniper Security Director Cloud login page.

JUNIPER NETWORKS

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.

Juniper
Security Director Cloud

Email

Next

📋 **View Prerequisites**

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

Juniper
Security Director Cloud

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.

Juniper
Security Director Cloud

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. Log out from the page on your mobile phone.

8. Power on your cloud-ready SRX Series Firewall and log in to the 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:

- **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.
- **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

Region	Purpose	Port	FQDN
North Virginia, US	ZTP	443	**jsec2-virginia.juniperclouds.net**
	Outbound SSH	7804	**srx.sdcloud.juniperclouds.net**

| Region	Purpose	Port	FQDN
	Syslog TLS	6514	**srx.sdcloud.juniperclouds.net**
Ohio, US	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 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.
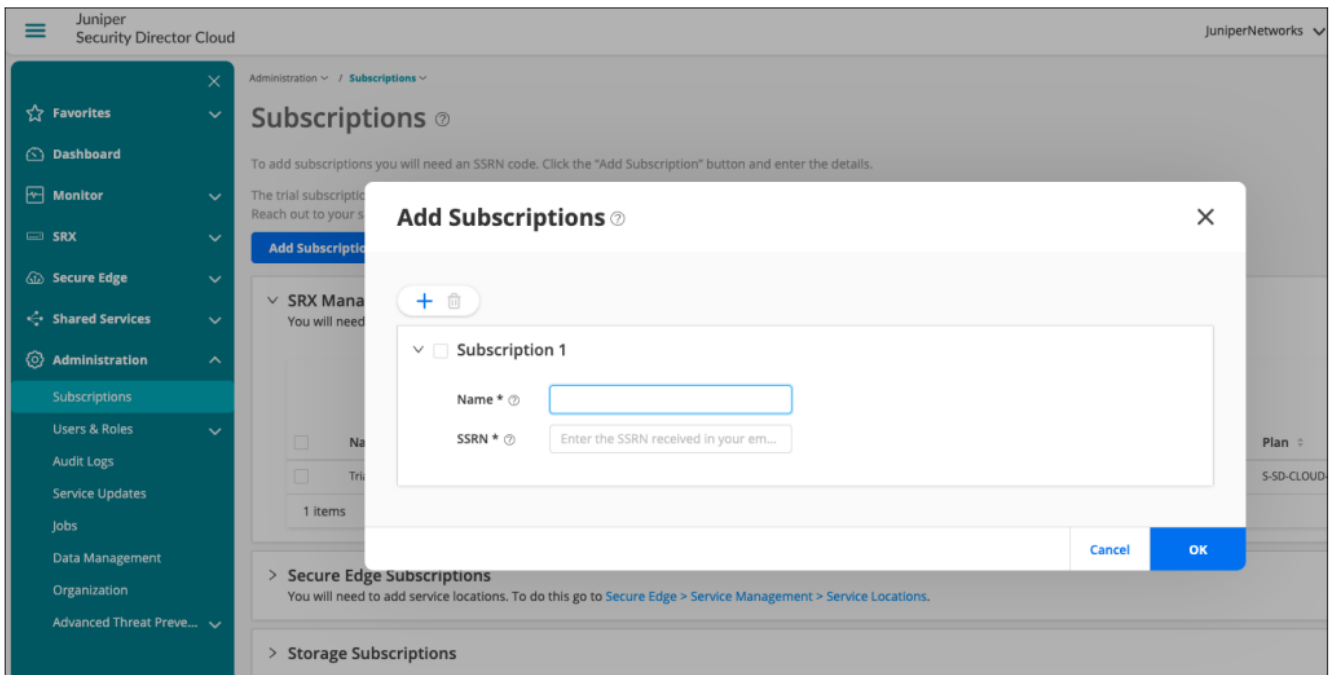
    - View your added subscriptions from Subscriptions>SRX Management Subscriptions. If you do not see your subscriptions, go to Administration > Jobs page to view the status.
4. Go to **Juniper Security Director Cloud**, select SRX > Device Management > Devices, and click the + icon to add your devices.
5. Click Adopt SRX Devices and select one of the following:
    - SRX Devices
    - SRX Clusters
    - SRX Multinode High Availability (MNHA) Pairs
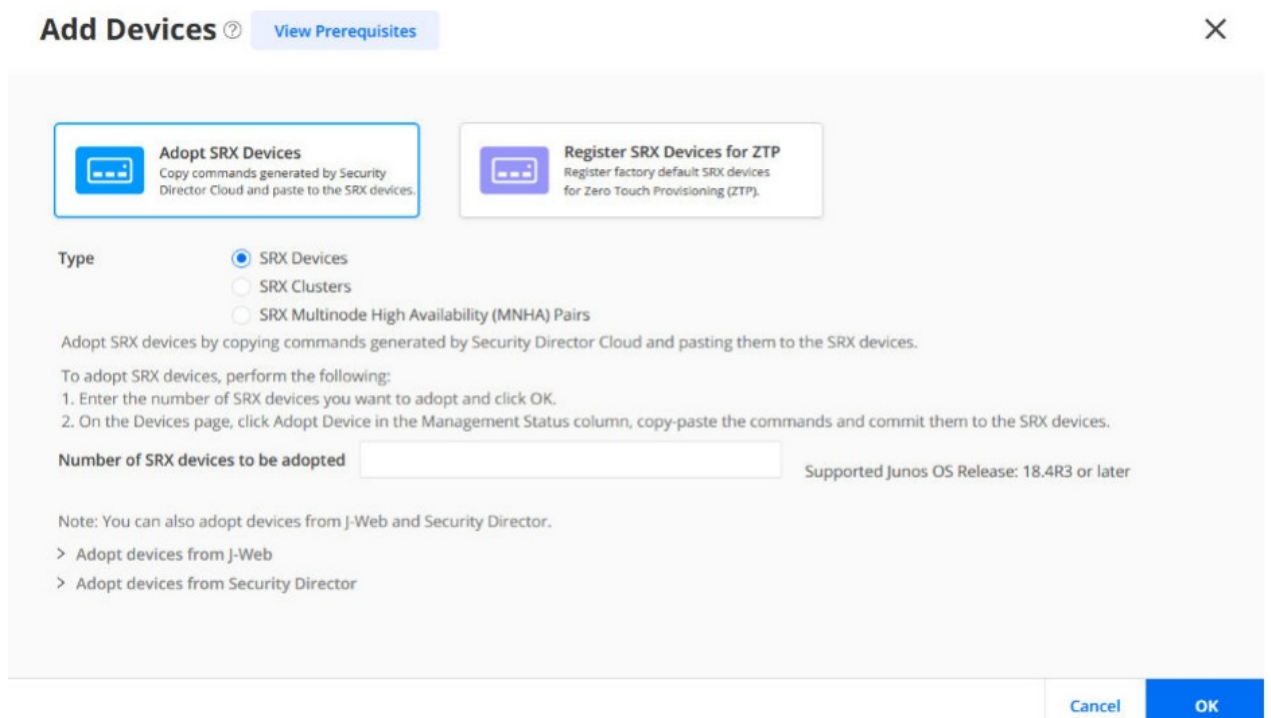
    - Follow the on-screen instructions to continue.
6. Copy and paste the commands from the devices page to the SRX Series Firewall or the primary cluster device

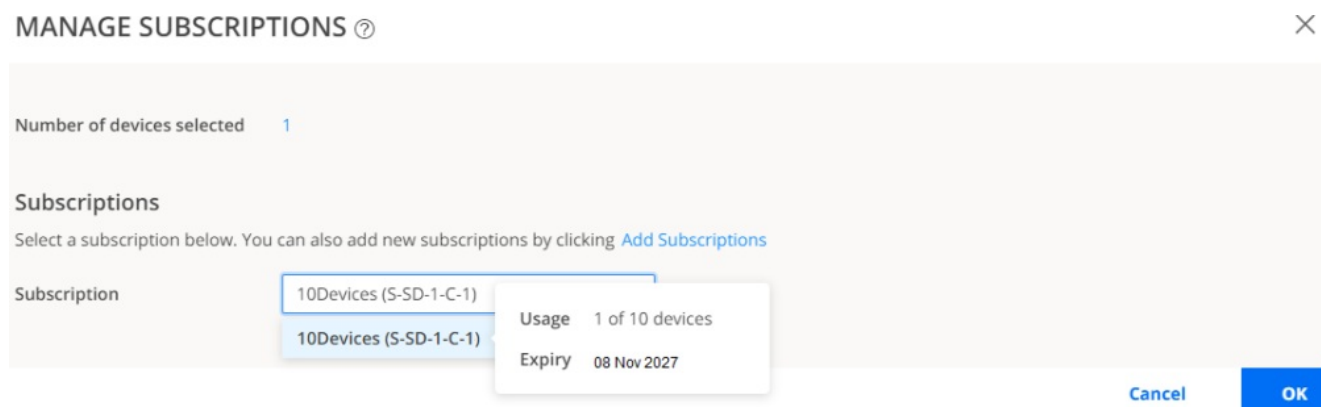console or each device in the MNHA pair, and commit the changes.
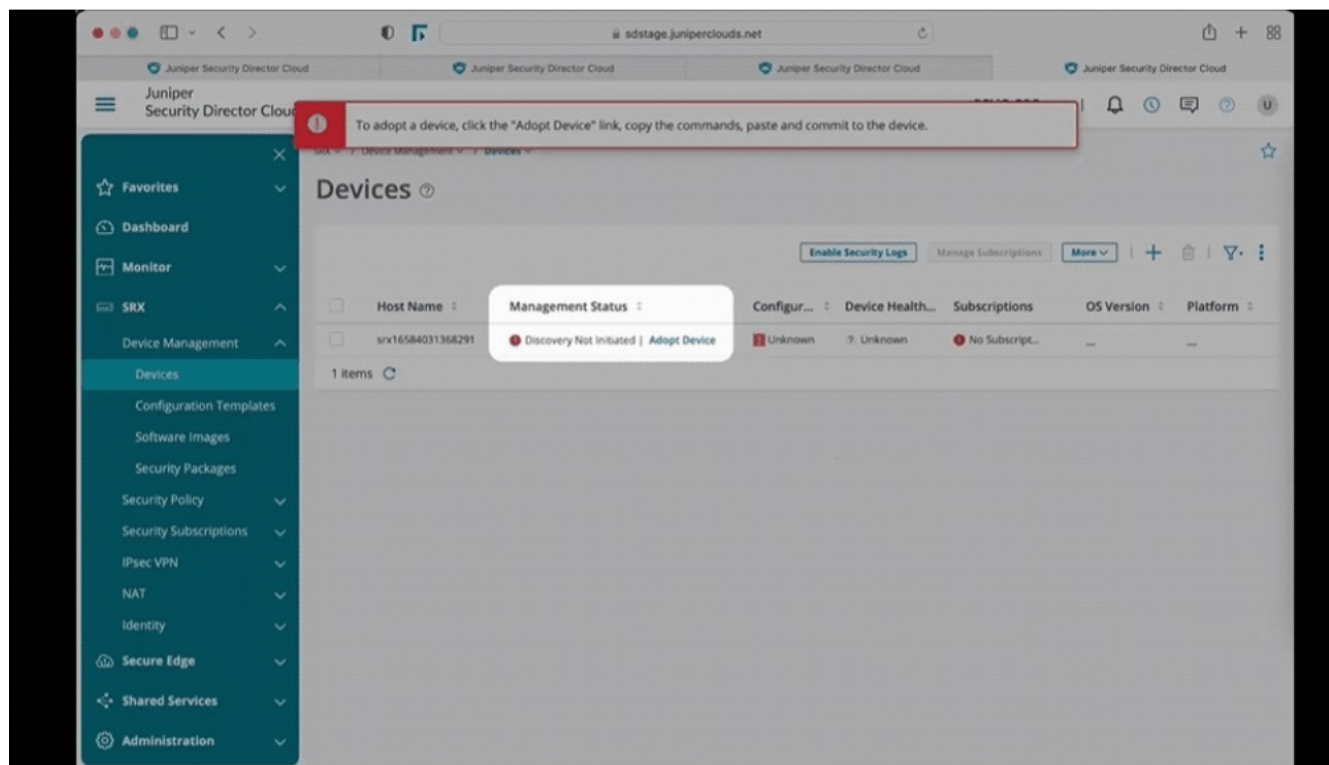
- It will take a few seconds for the device discovered. After device discovery is successful, verify the following fields on the Devices page.
- Management Status changes from Discovery in progress to Up.
- Inventory Status and Device Config Status changes from Out of Sync to In Sync.
- **NOTE:** In case of discovery failure, go to the 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.

Up and Running

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.

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

- **Congratulations!** You have successfully associated your device with Juniper Security Director Cloud.

Keep Going

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](#)**

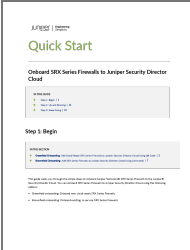| If You Want To	Then
View the traffic logs and network events including viruses found, interfaces that are down, number of attacks, CPU spikes, system reboots, and sessions	See **[About the Session Page](#) and [About the All Security Events Page](#)**

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 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](#)**

Documents / Resources

	[Juniper NETWORKS Onboard SRX Series Firewalls to Juniper Security Director Cloud](#) [pdf] User Guide SRX1600, SRX2300, SRX4300, Onboard SRX Series Firewalls to Juniper Security Director Cloud, Onboard SRX Series, Firewalls to Juniper Security Director Cloud, Juniper Security Director Cloud, Security Director Cloud, Director Cloud, Cloud

References

- [sdcloud.juniperclouds.net/](#)
- [SRX1600 Firewall Hardware Guide | Juniper Networks](#)
- [SRX2300 Firewall Hardware Guide | Juniper Networks](#)
- [SRX4300 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](#)
- [Security Policies Overview | SD Cloud | Juniper Networks](#)
- [About the Session Page | SD Cloud | Juniper Networks](#)

- 🍃 **[Content Security Profiles Overview | SD Cloud | Juniper Networks](#)**
- 🍃 **[Add Devices | SD Cloud | Juniper Networks](#)**
- ⁖ **[SRX Adoption - Mist](#)**
- **[User Manual](#)**