JUNIPER NETWORKS | Engineering Simplicity

Quick Start

Juniper Security Director 25.2.2 Quick Start

IN THIS GUIDE

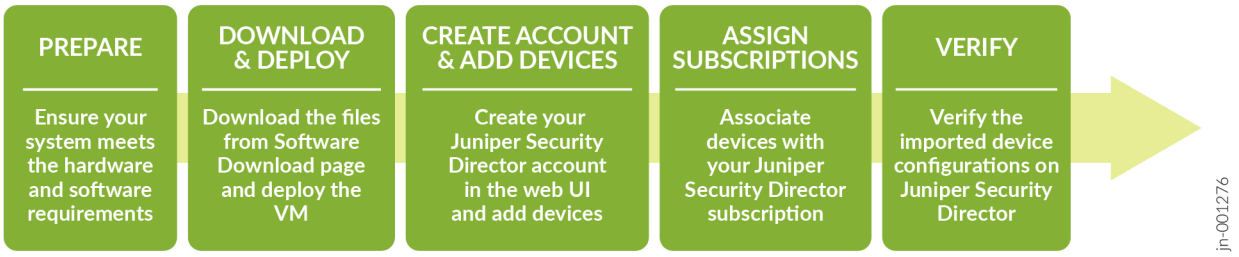
Step 1: Begin

IN THIS SECTION

You can install Juniper Security Director on-premises and manage SRX Series Firewalls and vSRX Virtual Firewalls through a centralized web interface. This guide walks you through installing Juniper Security Director, onboarding your devices, and configuring Juniper Security Director to manage your devices.

NOTE: This Quick Start is for Juniper Security Director 25.2.2 release. To access earlier versions, use the drop-down selector menu on the Juniper Security Director Documentation page.

Here's the high-level order of installation and device onboarding workflow.



Deploy Juniper Security Director VM

Table 1 on page 2 provides the deployment options for Juniper Security Director VM.

Table 1: Supported Deployment Options

Deployment option	Refer
Deploy Juniper Security Director Using VMware vSphere	Juniper Security Director Installation and Upgrade Guide
Deploy Juniper Security Director Using KVM	Juniper Security Director Installation and Upgrade Guide

Step 2: Up and Running

IN THIS SECTION

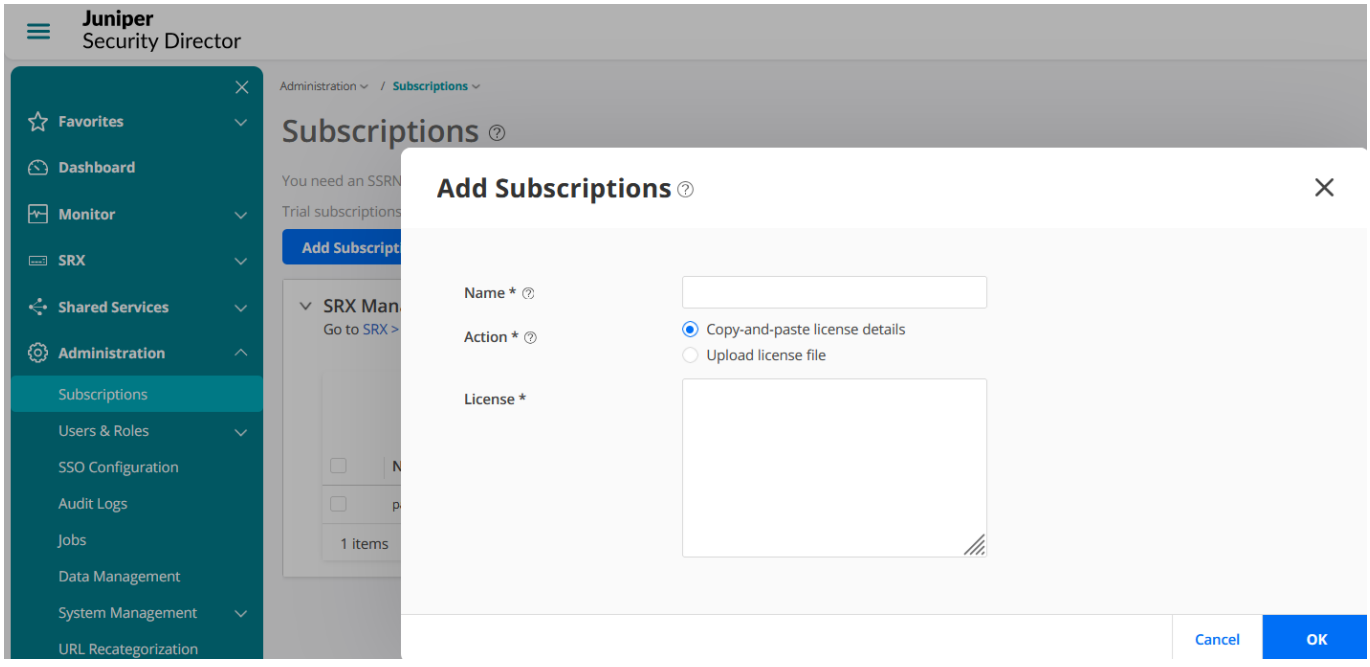
Create Organization Account and Add Devices

Before You Begin

The following ports must be opened:

- Inbound port 443 for users' connection to Web is associated to the UI virtual IP address.
- Outbound port 25 for outbound to configured mail server is associated to the Management IP address.
- Inbound port 7804 from all managed devices is associated to the device connection virtual IP address.
- Outbound port 443 for signature download URL is associated to the Management IP address.
- Inbound port 6514 for inbound connection for traffic log is associated to the log collector virtual IP address.

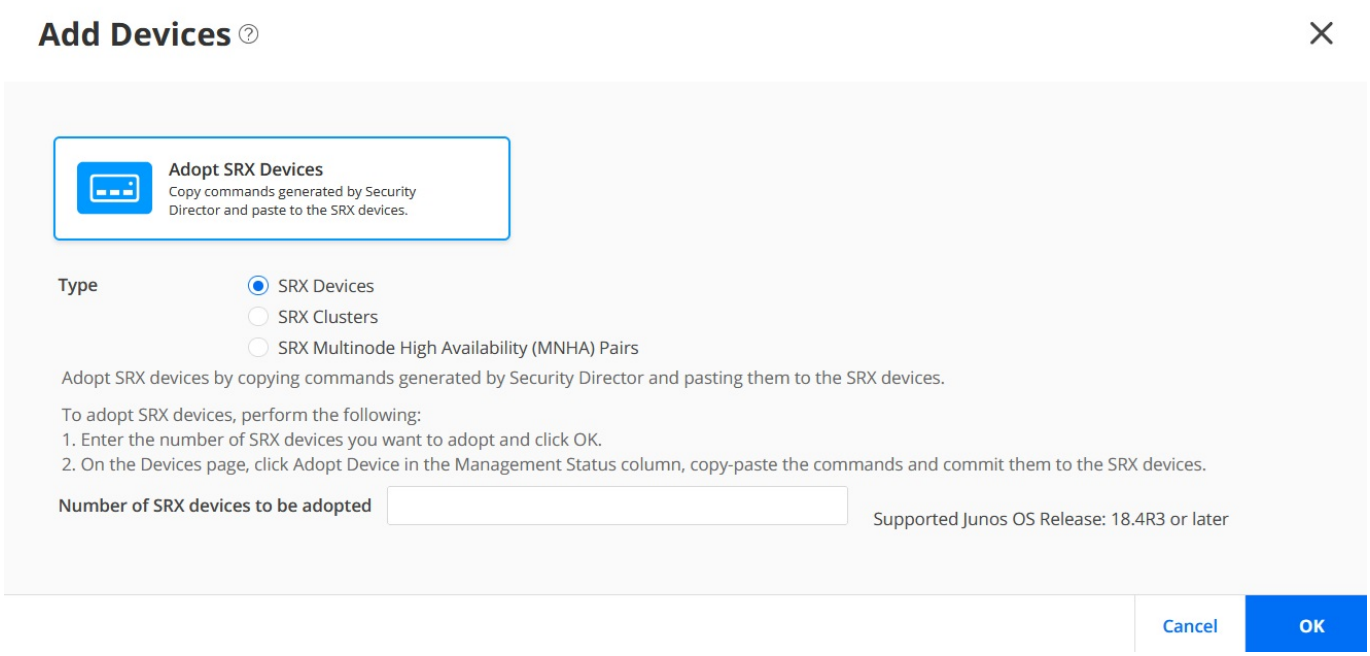
1. Enter the UI virtual IP address or FQDN (domain name) in a browser to access the Juniper Security Director login page. Follow on-screen instructions to create and activate your account. For details, see Log In to the Juniper Security Director Web UI.
2. Login to Juniper Security Director, click **Add Subscriptions**. You can also use a 60-day trial subscription that is available by default.



3. Enter a name for the subscription and select either of the following options:
   a. **Copy-and-paste license details**—Copy license key and paste in the **License** field.
   b. **Upload license file**—Click **Browse** and navigate to the license.txt file. Click **Open**. Please note you can upload only .txt file.
4. Click **OK**. You can 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.
5. Select **SRX** > **Device Management** > **Devices**, and click the + icon to add your devices.

NOTE: To know about supported devices, see Juniper Security Director Supported Firewalls.

6. Click **Adopt SRX Devices** and select one of the following:
   - **SRX Devices**
   - **SRX Clusters**
   - **SRX Multinode High Availability (MNHA) Pairs**



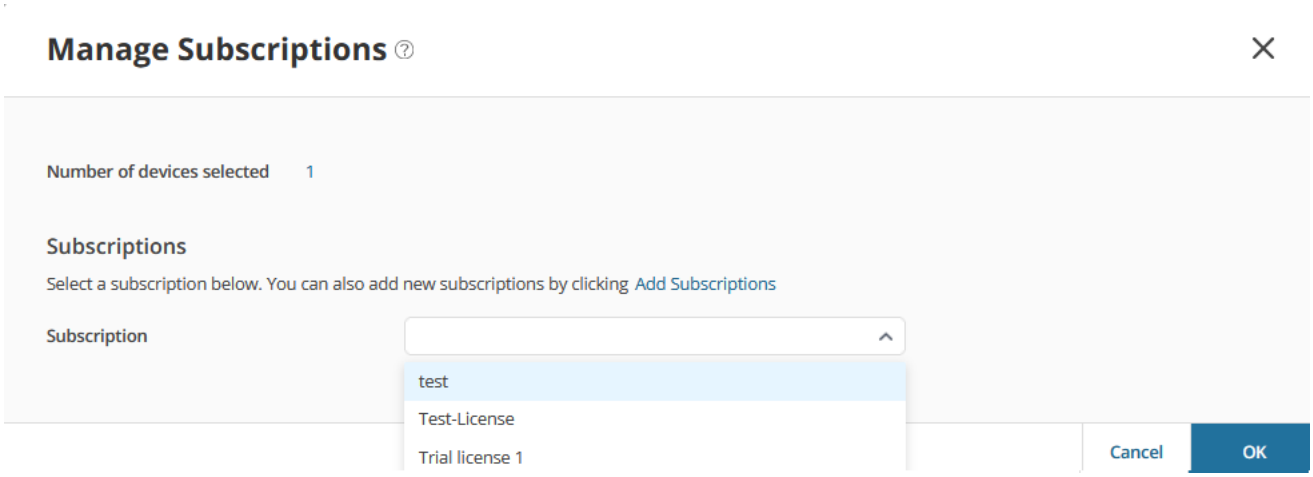
   Follow the on-screen instructions to continue. For details, see Add Devices.

7. Copy and paste commands from the devices page to the SRX Series Firewall or the primary cluster device console. Then commit the changes. It will take few seconds for 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**.

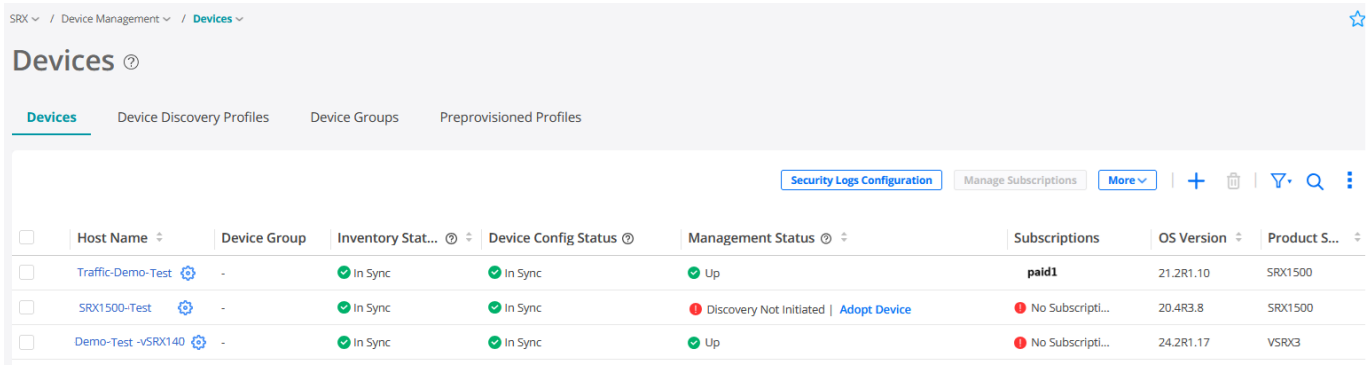
NOTE: In case of discovery failure, go to the **Administration** > **Jobs** page and view the status.

Associate Devices with Your Juniper Security Director Subscription

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



2. Verify that **Subscriptions** column displays the subscription name for your device. Congratulations! You have successfully associated your device to Juniper Security Director.



Verify Configuration on Adopted Devices

Verify your device configurations in Juniper Security Director.

- Go to **SRX** > **Security Policy** > **SRX Policy** and verify the imported security policies.
- Go to **SRX** > **NAT Policy** > **NAT** and verify the imported NAT policies.
- Go to **SRX** > **Device Management** > **Devices**, click **Security Logs Configuration**, and verify the security log configurations.

If you've set up security policy, NAT, IPSec VPN, and logs on the device, these configurations will be imported into Juniper Security Director.

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 Security Policies Overview
Create a NAT policy, add a rule to the NAT policy, and deploy the NAT policy on the devices.	See NAT Policies Overview
Set up the Content Security profiles to secure your network from multiple security threat types.	See Content Security Overview
View the traffic logs and network events including viruses found, interfaces that are down, number of attacks, and sessions.	See About the Session Page and About the All Security Events Page
Monitor the status of the CPU, disk space, storage database, and services running on the Juniper Security Director VM.	System Overview
Configure log level settings, generate and download system logs to troubleshoot the issues related to Juniper Security Director.	See About System Logs Page

General Information

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