JUNIPER NETWORKS | Engineering Simplicity

Quick Start

Onboard SRX Series Firewalls to Juniper Security Director

IN THIS GUIDE

- Step 1: Begin | 1
- Step 2: Up and Running | 7
- Step 3: Keep Going | 11

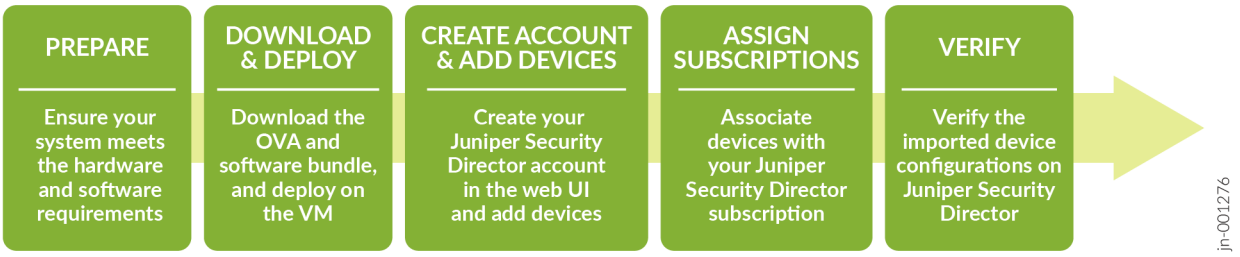
Step 1: Begin

IN THIS SECTION

- Prepare to Install Juniper Security Director | 2
- Download the OVA and Software Bundle | 3
- Deploy the VM | 3

Juniper Security Director brings powerful security management, installed on-premises. This guide walks you through installing Juniper Security Director, onboarding your devices, and configuring Juniper Security Director to manage your devices. Use this guide if you need to manage SRX Series Firewalls using Juniper Security Director.

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



Prepare to Install Juniper Security Director

Hardware Requirements

Table 1: Hardware Requirements for ESXi Server

VM Configuration	Device Management Capability	Log Analytics and Storage Capability
16 vCPU, 80 GB RAM, 2.1 TB storage	• Up to 1000 devices • Up to 10000 policy rules per device • Up to 6000 NAT rules per device • Up to 1000 VPNs per device/system	• Up to 17000 logs per second • Out of the 2.1 TB storage, 1.5 TB is dedicated for log analytics.
40 vCPU, 208 GB RAM, 4.2 TB storage	• Up to 3000 devices • Up to 20000 policy rules per device • Up to 10000 NAT rules per device • Up to 1500 VPNs per device/system	• Up to 40000 logs per second • Out of the 4.2 TB storage, 3.5 TB is dedicated for log analytics.

NOTE: We do not recommend hyperthreading on VMware hypervisor (ESXi) Server. You must use dedicated resources for CPU, RAM, and disk as per the hardware requirement. We do not recommend oversubscription or sharing resources.

Software Requirements

- Juniper Security Director runs on a VMware hypervisor (ESXi) Server. Use vCenter and vSphere version 7.0 and later. You must deploy the OVA through vCenter Server only. We do not support OVA deployment on ESXi directly.
- You must have the following dedicated IP addresses in the same subnet:
  - **Management IP address**—IP address for the VM that provides access to the Juniper Security Director CLI.
  - **UI virtual IP address**—Virtual IP address to access the Juniper Security Director GUI.
  - **Device connection virtual IP address**—Virtual IP address to establish connection between the managed devices and Juniper Security Director.
  - **Log collector virtual IP address**—Virtual IP address to receive logs from devices.
- Ensure that you have access to SMTP, NTP, and DNS servers from the VM network (Juniper Security Director).

> **NOTE**: We support NTP server with IPv4 address only.

Download the OVA and Software Bundle

1. Download the **Juniper Security Director OVA** (.ova file) from https://support.juniper.net/support/downloads/?p=security-director-on-prem to a Web server or your local machine.
2. Download the **Juniper Security Director Software Bundle** (.tgz file) to your local machine from https://support.juniper.net/support/downloads/?p=security-director-on-prem and then transfer the file to your staging server.
   A staging server is an intermediate server where the software bundle is downloaded and is accessible from the VM.

   The staging server must support software bundle download from the Juniper Security Director VM through Secure Copy Protocol (SCP). Before you deploy the VM, you must have the details of the staging server, including the SCP username and password.

Deploy the VM

1. Open the vSphere Client.
2. Right-click the inventory object that is a valid parent object of a VM and select **Deploy OVF Template**.
3. On the Select an OVF template page:

- Enter the webserver OVA URL, where you have downloaded the OVA. The system might warn you about source verification. Click **Yes**.

  NOTE: Ensure that firewall rules do not block image access from the vSphere cluster.

  OR

- Select the **Local file** option and click **UPLOAD FILES** to choose the OVA file from your local machine.

4. On the Select a name and folder page, enter the VM name and the location.
5. On the Select a compute resource page, select the compute resource for the host on which the VM will be deployed.
6. On the Review details page, review the details of the resources to be provisioned.
7. On the Select storage page, select the storage for the configuration and the virtual disk format. We recommend you to use virtual disk format as Thick provision.

   NOTE: We do not recommend thin provisioning. If you choose thin provisioning and the actual disk space available is low, the system might encounter problems once the disk is full.

8. On the Select networks page, select the network to configure IP allocation for static addressing.
9. On the Customize template page, configure Juniper Security Director on-premise OVA parameters.

   NOTE: Prepare all details for the Custom template page in advance. The OVF template will timeout after 6 to 7 minutes.

Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Customize template
8 Ready to complete

Customize template

Customize the deployment properties of this software solution.

Juniper Security Director On-Premises OVA Settings 15 settings

Hostname	
cliadmin user password	Min Length 8, Max length 32, required at least 3 types: digit, uppercase alphabet, lower case alphabet, special character (~!@#$%^&*( )_-+={ }[ ];:" '<,>.?/|\) Password Confirm Password
Management IP address	Enter the IP address in CIDR format. For example, 10.2.4.5/24. Do not use /32 netmask to indicate the address. Netmask must be at least /29.
Default gateway	Gateway IP address of the network.
DNS servers	Enter the server addresses, each separated by a space.
Search domains	Enter multiple search domains, each separated by a space.
UI virtual IP address	The virtual IP address must be in the same subnet of the management IP address.
UI FQDN	Fully Qualified Domain Name that resolves to UI virtual IP address
Device connection virtual IP address	The virtual IP address must be in the same subnet of the management IP address
Device Connection FQDN	Fully Qualified Domain Name that resolves to Device Connection virtual IP address
Log collector virtual IP address	The virtual IP address must be in the same subnet of the management IP address
Log Collector FQDN	Fully Qualified Domain Name that resolves to LOG Collector virtual IP address
Software bundle SCP path	Format with port - user@server:port/relative-path or user@server:port//absolute-path. For example, root@10.0.0.1:22//var/www/html/sdop-24.1-898.tgz Format without port - user@server:relative-path or user@server:/absolute-path. For example, root@10.0.0.1:/root/sdop-24.1-898.tgz
SCP password	Password Enter a password to enable authentication. Confirm Password
NTP server	

CANCEL BACK NEXT

NOTE:

- The **cliadmin user password** field does not strictly validate password requirements. However, during the installation process, the system enforces strict validations and rejects the password that does not meet the specified requirements, causing installation failure. To avoid issues during installation, ensure that the password meets these criteria:
  - Must be at least 8 characters long and not more than 32 characters.
  - Must not be dictionary words.
  - Must include at least three of the following:
    - Numbers (0-9)
    - Uppercase letters (A-Z)
    - Lowercase letters (a-z)
    - Special characters (~!@#$%^&*()_-+={}[];:"'<,>.?/|\)
- We recommend you to use FQDN.

10. On the Ready to complete page, review all the details and if required, go back and edit the VM parameters. These network parameters cannot be changed from the VM configuration after successful installation. However, network parameters can be changed from the CLI. Click **Finish** to begin the OVA deployment.

    You can monitor the OVA deployment progress status in the Recent Tasks window at the bottom of your screen till it is 100% complete. The Status column shows the deployment complete percentage.

    Congratulations! Now the OVA deployment is complete.

11. Click the triangle icon to power on the VM.

NOTE:

- By default, the VM is deployed with the smallest resource configuration mentioned in "Hardware Requirements" on page 2. Adjust the resources to match other resource configurations using the VMWare Edit VM settings.
- The resource allocation must match "Hardware Requirements" on page 2. Incorrect allocation will result in VM installation to fail.

Once the VM powers on, navigate to the **Summary** tab and click **LAUNCH WEB CONSOLE** to monitor the software bundle installation status.

NOTE: Avoid performing any operation on the console until the installation is complete.

A successful installation requires approximately 30 minutes. If the installation lasts longer, check the Web console for potential errors. You can ssh to the VM IP using the **cliadmin** user and the password you configured during the OVA deployment. Then, use the **show bundle install status** command to check the installation status.

You can view the installation progress on the console. After the installation is complete, the console displays *Successfully installed software bundle on the cluster*.

Congratulations! The software bundle installation is now complete.

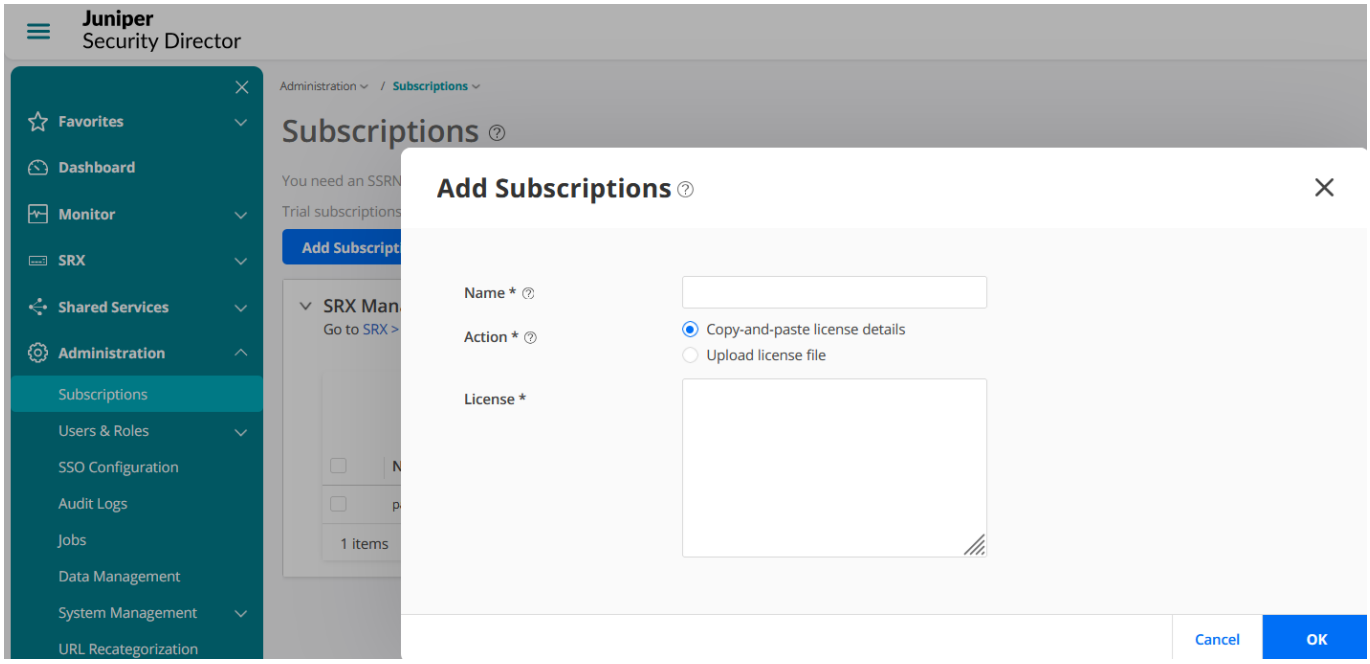
Step 2: Up and Running

IN THIS SECTION

- Create Organization Account and Add Devices | **7**
- Associate Devices with Your Juniper Security Director Subscription | **9**
- Verify Configuration on Adopted Devices | **10**

Create Organization Account and Add Devices

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**, enter details, and click **OK**. You can also use a 60-day trial subscription that is available by default.



NOTE: Ensure that your license details or uploaded license file includes the following fields and their values to avoid validation failure:

Issue Date:

Expiry Date:

HW Serial Number:

SSRN:

Feature:

Quantity:

License Type:

License Key:

Any discrepancies, such as mismatched field names, incomplete details, or invalid file extension might prevent you from adding the subscription.

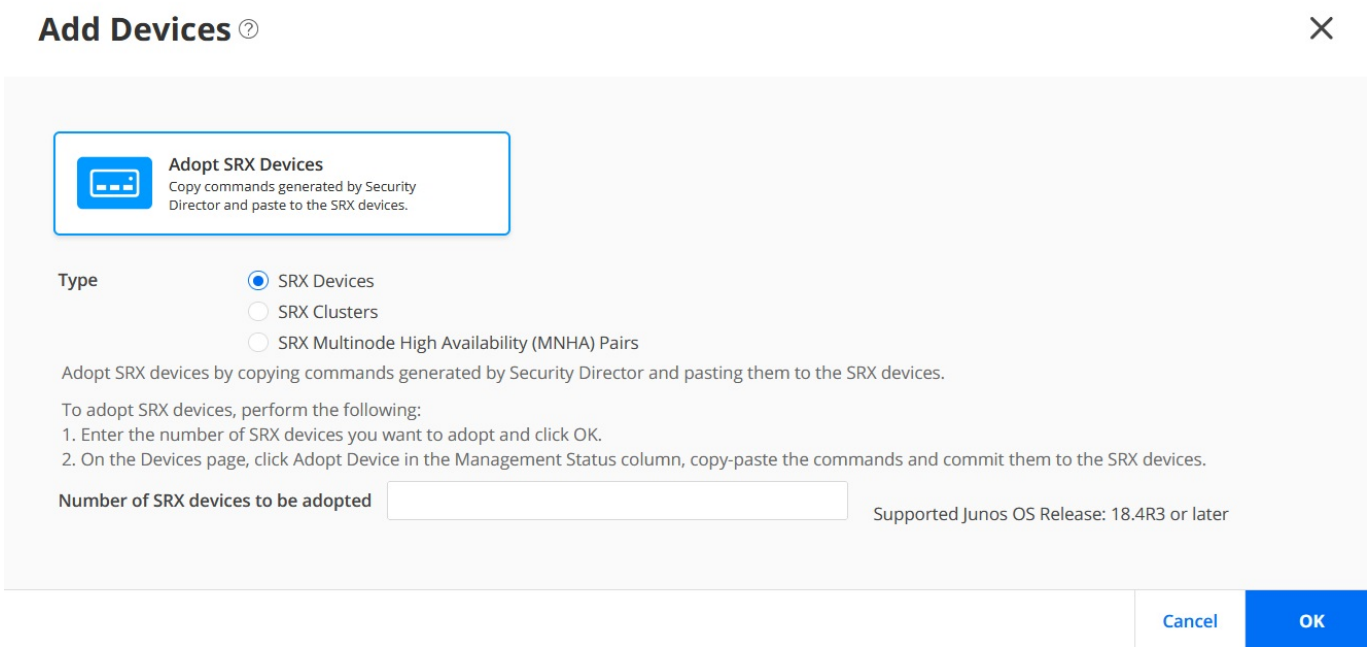
3. View your added subscriptions from **Subscriptions** > **SRX Management Subscriptions**. If you do not see your subscriptions, go to **Administration** > **Jobs** page to view the status.

4. 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.

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. For details, see Add Devices.

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

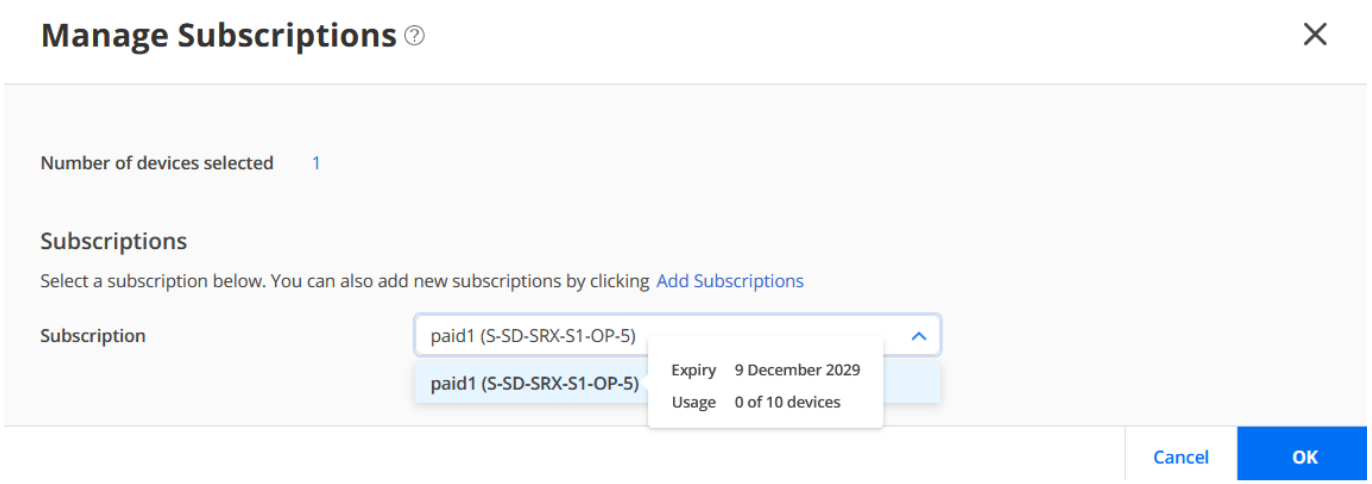
   It will take few seconds for device discovery. After device discovery is successful, verify the following fields on the **Devices** page:

   - **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.

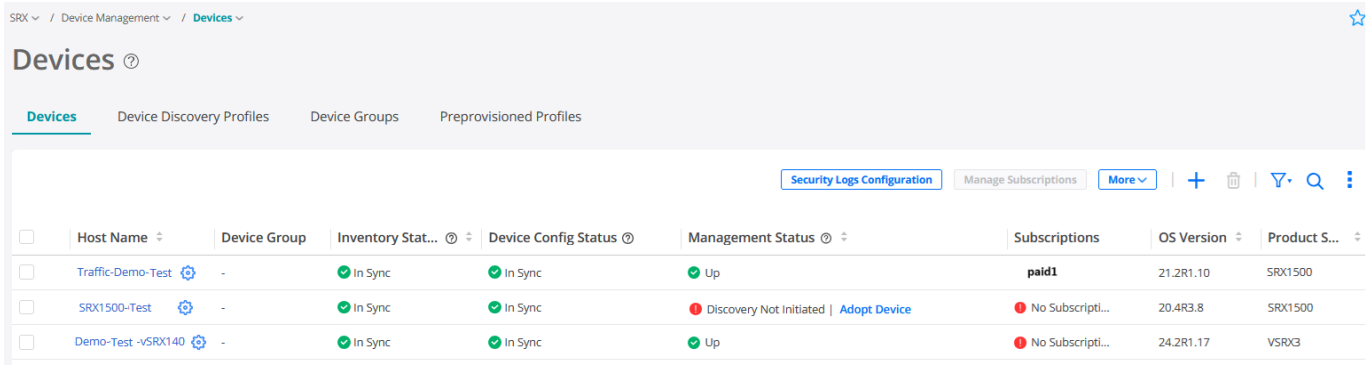
Associate Devices with Your Juniper Security Director Subscription

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

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

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.

Step 3: Keep Going

IN THIS SECTION

- What's Next? | 11
- General Information | 11

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