JUNIPer | Engineering
NETWORKS | Simplicity

Security Director

Junos Space Security Director Installation and Upgrade Guide

Published
2025-09-18

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

Table of Contents

About This Guide

Use this guide to install and upgrade Security Director application, set up Log Collector, add Log Collector to Security Director, and upgrade Log Collector.

1
CHAPTER

Installing and Upgrading Security Director

IN THIS CHAPTER

Security Director Installation Overview

IN THIS SECTION

Security Director is a Junos Space management application designed to enable quick, consistent, and accurate creation, maintenance, and application of network security policies. It is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.

Before you install Security Director, you must configure the Junos Space Appliance as a Junos Space node.

You can install Security Director on Junos Space Virtual Appliance. The Junos Space virtual appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. You must deploy the virtual appliance on a VMware ESX server, VMware ESXi server, or a KVM server which provides a CPU, hard disk, RAM, and a network controller, but requires installation of an operating system and applications to become fully functional.

For information about installing Junos Space virtual appliances on a VMware ESX server, VMware ESXi server, or KVM server, see the Junos Space Virtual Appliance Installation and Configuration Guide.

shows the Security Director installation and upgrade flow.

Figure 1: Security Director Installation and Upgrade Flow
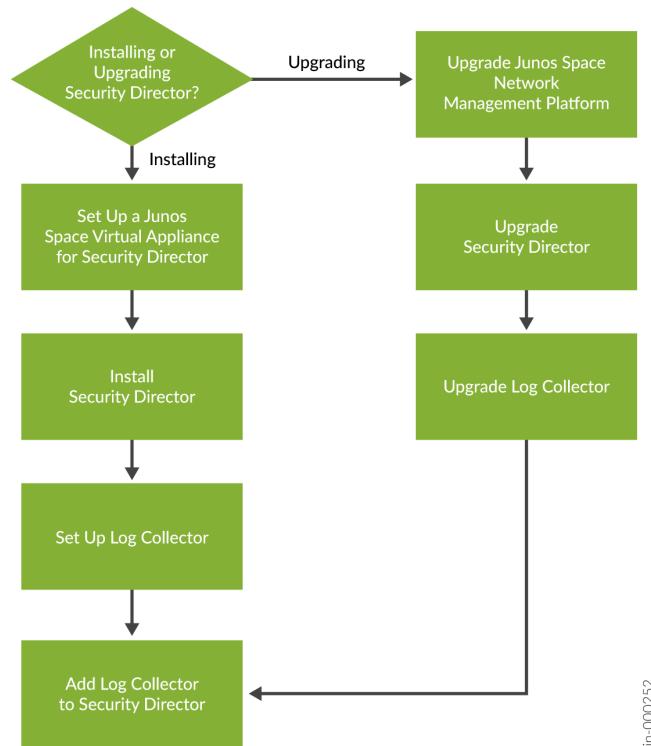
Intended Audience

This document is intended for network operators and administrators who install, configure, and manage the network security infrastructure.

RELATED DOCUMENTATION

Set Up a Junos Space Virtual Appliance for Security Director | 4

Set Up a Junos Space Virtual Appliance for Security Director

The Junos Space virtual appliance consists of preconfigured Junos Space Network Management Platform software with a built-in operating system and application stack that is easy to deploy, manage, and maintain. For more information on installing Junos Space virtual appliance, see Junos Space Virtual Appliance Installation and Configuration Guide.

You must set up the Junos Space virtual appliance to run as a Junos Space node. After you deploy a Junos Space virtual appliance, you must enter basic network and machine information to make your Junos Space virtual appliance accessible on the network. For complete configuration steps, see Configuring a Junos Space Virtual Appliance as a Junos Space Node.

RELATED DOCUMENTATION

Security Director Installation Overview | 2

Upgrade Junos Space Network Management Platform

Junos Space Security Director Release can be installed or upgraded only on the supported Junos Space Network Management Platform Release. For example, Security Director Release 24.1R1 is supported only on Junos Space Network Management Platform Release 24.1R1. If your appliance is running the supported version of Junos Space, you can skip this procedure and begin installation of Security Director. For information on supported version of Junos Space Network Management Platform for Security Director, see "Upgrade Security Director" on page 6.

If your appliance is running a Junos Space Network Management Platform release that is earlier than the supported release, you need to upgrade Junos Space Network Management Platform before upgrading Security Director.

To upgrade your Junos Space Network Management Platform:

1. Determine the installed Junos Space Network Management Platform version:

    a. Log in to Junos Space. The default username is super and password is juniper123. The Dashboard is displayed.

Change the default credentials, when prompted.

b. Click the **+** icon next to Administration to expand the Administration menu.

c. Click **Applications** to list all of the applications installed.

d. Note the version of the Junos Space Network Management Platform or the Network Application Platform. (Some earlier versions of the Network Management Platform were named Network Application Platform.) If the currently installed release is a supported one, you can skip the upgrade procedure; if not, you must upgrade the Junos Space Network Management Platform to the supported release.

2. Upgrade Junos Space Network Management Platform using the procedure at Upgrading to Junos Space Network Management Platform Release 24.1R1.

> ⓘ **NOTE**: For more information about application compatibility, see the Knowledge Base article KB27572 at Junos Space Application Compatibility .

Install Security Director

In Junos Space Security Director, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. You must deploy the Log Collector and then add it to the Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

> ⓘ **NOTE**: Both JSA as Log Collector and Security Director Insights as Log Collector cannot be added together.

> ⓘ **NOTE**: Upgrade to the supported release of Junos Space Network Management Platform Release. See "Upgrade Junos Space Network Management Platform" on page 4.

To install the Junos Space Security Director:

> ⚠️ **CAUTION**: You must install the Junos Space 24.1R1 hot patch v1 before installing or upgrading Junos Space Security Director application.

1. Download the Junos Space Security Director Release image from the download site.

2. Install the Security Director application using the procedure at Adding a Junos Space Application.

> ℹ️ **NOTE**: The applogic service restarts after the application installation job is successful.

RELATED DOCUMENTATION

Upgrade Security Director

Before You Begin

- If you are upgrading from a previous version of Security Director, clear your browser cache before accessing the Security Director user interface.

- Back up Junos Space Security Director Release that you want to upgrade. You must take the backup before upgrading Junos Space Network Management Platform. Backing up the Junos Space Network Management Platform database before the upgrade helps you to recover the data if the upgrade fails. See Backing Up the Junos Space Network Management Platform Database.

- You must upgrade to the supported Junos Space Network Management Platform Release, before you upgrade the Security Director, Log Director, and Security Director Logging and Reporting modules. See "Upgrade Junos Space Network Management Platform" on page 4.

- The Junos Space Network Management Platform should be active and functioning.

You can upgrade from a previous Security Director release to the latest Security Director release.

> **NOTE**: The Required Platform Version column in Table 1 on page 7 indicates the supported Junos Space Network Management Platform version. Before upgrading Security Director, ensure that the system is running the supported Junos Space Network Management Platform version. See "Upgrade Junos Space Network Management Platform" on page 4.

Table 1: Upgrade Path

CAUTION: You must install the Junos Space 24.1R1 hot patch v1 before installing or upgrading Junos Space Security Director application.

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 24.1R2	24.1R1	• 23.1R1 > 24.1R2 • 24.1R1 > 24.1R2	You can upgrade from the following releases: • Junos Space Network Management Platform Release 24.1R1 and Security Director Release 23.1R1 and 24.1R1.
Security Director 24.1R1	24.1R1	• 23.1R1 > 24.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 23.1R1 and Security Director Release 23.1R1
Security Director 23.1R1	23.1R1	• 22.3R1 > 23.1R1 • 22.2R1 > 23.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 22.3R1 and Security Director Release 22.3R1 • Junos Space Network Management Platform Release 22.2R1 and Security Director Release 22.2R1

Table 1: Upgrade Path *(Continued)*

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 22.3R1	22.3R1	• 22.2R1 > 22.3R1 • 22.1R1 > 22.3R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 22.2R1 and Security Director Release 22.2R1 • Junos Space Network Management Platform Release 22.1R1 and Security Director Release 22.1R1
Security Director 22.2R1	22.2R1	• 22.1R1 > 22.2R1 • 21.3R1 > 22.2R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 22.1R1 and Security Director Release 22.1R1 • Junos Space Network Management Platform Release 21.3R1 and Security Director Release 21.3R1
Security Director 22.1R1	22.1R1	• 21.2R1 > 22.1R1 • 21.3R1 > 22.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 21.2R1 and Security Director Release 21.2R1 • Junos Space Network Management Platform Release 21.3R1 and Security Director Release 21.3R1

Table 1: Upgrade Path *(Continued)*

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 21.3R1	21.3R1	• 21.1R1 > 21.3R1 • 21.2R1 > 21.3R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 21.1R1 and Security Director Release 21.1R1 • Junos Space Network Management Platform Release 21.2R1 and Security Director Release 21.2R1
Security Director 21.2R1	21.2R1	• 21.1R1 > 21.2R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 21.1R1 and Security Director Release 21.1R1
Security Director 21.1R1	21.1R1	• 20.3R1 > 21.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 20.3R1 and Security Director Release 20.3R1
Security Director 20.3R1	20.3R1	• 19.3R1 > 20.3R1 • 19.4R1 > 20.3R1 • 20.1R1 > 20.3R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1 • Junos Space Network Management Platform Release 20.1R1 and Security Director Release 20.1R1

Table 1: Upgrade Path *(Continued)*

Upgrading to Release	Required Platform Version	Upgrade Path	Description
Security Director 20.1R1	20.1R1	• 19.3R1 > 20.1R1 • 19.4R1 > 20.1R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1 • Junos Space Network Management Platform Release 19.4R1 and Security Director Release 19.4R1
		You can now perform direct upgrade to 20.1R1 from earlier versions of Junos Space Security Director Release 19.1R1 and 19.2R1. • 19.1R1 > 20.1R1 • 19.2R1 > 20.1R1 **NOTE**: You can perform direct upgrade only for Junos Space Security Director. However, you must follow all the supported upgrade paths for Junos Space Network Management Platform and Log Collector to upgrade to 20.1R1.	
Security Director 19.4R1	19.4R1	• 19.2R1 > 19.4R1 • 19.3R1 > 19.4R1	You can upgrade from the following releases: • Junos Space Network Management Platform Release 19.2R1 and Security Director Release 19.2R1 • Junos Space Network Management Platform Release 19.3R1 and Security Director Release 19.3R1

To upgrade from a previous version of Junos Space Security Director:

1. Download the Junos Space Security Director Release image to which you want to upgrade from the download site.

2. Upgrade the Junos Space Security Director application using the procedure at Upgrading a Junos Space Application.

> *i* **NOTE**:
>
> - If you try to upload Junos Space Security Director image of a lower version, an error message `Can only upgrade to newer version` appears. Click **OK** and upload compatible version of Junos Space Security Director.
>
> - If you try to upload incompatible version of Junos Space Security Director image, an error message `Current platform version does not support this software version` appears . Click **OK** and upload compatible version of Junos Space Security Director.

> *i* **NOTE**: The applogic service restarts after the application upgrade job is successful.

RELATED DOCUMENTATION

Junos Space Store Overview

The Junos Space store displays the latest compatible versions of the Junos Space applications, which can be installed or upgraded on the current version of Junos Space Network Management Platform. Starting in Junos Space Security Director Release 18.2R1, you can install or upgrade Junos space Security Director application from the Junos Space store on the Network Management Platform.

You must configure the Juniper Networks Software download credentials to connect to Junos Space store. The Junos Space store lists the latest available applications.

The Junos Space Network Management Platform accesses the metadata repository hosted by Juniper Networks to discover the available applications and published versions. When you initiate an install or upgrade for Security Director application or its components, the package path is identified from the metadata file and package is downloaded. This reduces the manual effort of downloading the application package from the download site and then uploading it to the Junos Space Network Management Platform server, thereby enhancing the installation and upgrade process.

You can view whether a Security Director application version is supported on the current Junos Space Network Management Platform version, even before initiating install or upgrade. Junos Space store allows the component configuration while installing Security Director. It limits the component configuration when you try to upgrade Security Director.

> **NOTE**: The earlier method of installing and Upgrading Security Director application documented in "Install Security Director" on page 5 and "Upgrade Security Director" on page 6 are still applicable. You can choose to install using the existing method or through the Junos Space store.

RELATED DOCUMENTATION

Install and Upgrade Security Director from the Junos Space Store

The Junos Space store displays a list of applications, which can be installed on the Junos Space Network Management Platform. This topic describes the Security Director installation and upgrade procedure using the Junos Space store.

Before You Begin

- Configure Junos Space Store in Junos Space Network Management Platform. For details on configuring and modifying the Junos Space settings, see Configuring and Managing Junos Space Store.

- Ensure the HDD size (>500GB) of Junos Space Platform before configuring integrated Log Collector. OpenNMS should be in the disabled state.

For configuring Log Collector component in Junos Space store:

- Deploy and configure Junos Space Security Director Insights as the Log Collector. See Deploy and Configure Security Director Insights and Add Security Director Insights as a Log Collector.

- Deploy and configure JSA for using JSA as Log Collector. See, "JSA Log Collector Overview" on page 32.

For configuring Policy Enforcer component in Junos Space Store:

- Configure Policy Enforcer. See, Security Director Insights as Policy Enforcer.

To install and upgrade Security Director from the Junos Space Store:

1. Log in to Junos Space Network Management Platform.
2. Select **Administration** > **Applications** > **Junos Space Store**.

   The Junos Space Store page appears.

   > **NOTE**: Click **Get Latest** to refresh the list of applications in Junos Space store.

   The Junos Space store with all the applications are displayed as shown in Figure 2 on page 13.

Figure 2: Junos Space Store

3. Select **Security Director**.

   The details of the application such as the compatible versions, version release date, and release highlights are displayed.

   > **NOTE**: Click **Show only compatible version** option to display only the Security Director versions supported on the current platform version.
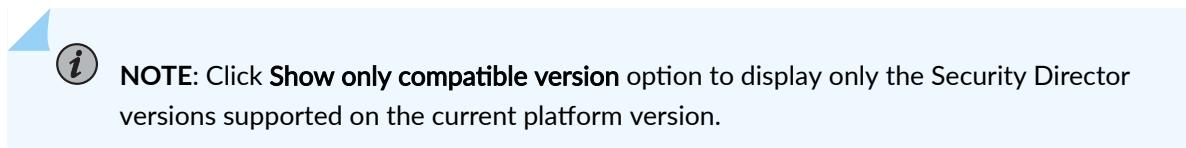
4. Select a version to be installed or upgraded and click **Next**.

   > **NOTE**: If the selected version is not compatible with the Junos Space Network Management Platform version, a warning message is displayed.

5. Select the components, which you want to configure and complete the configuration according to the guidelines given in Table 2 on page 15.

> ⓘ **NOTE**: Junos Space store allows the component configuration while installing Security Director. Upgrade of components is not handled by Junos Space Store.

6. Click **Next**.

The Security Director terms and conditions and the license agreement are displayed. Review the license agreement.

7. Click **Accept and Install**.

The job status is displayed as shown in Figure 3 on page 14.

Figure 3: Job Status
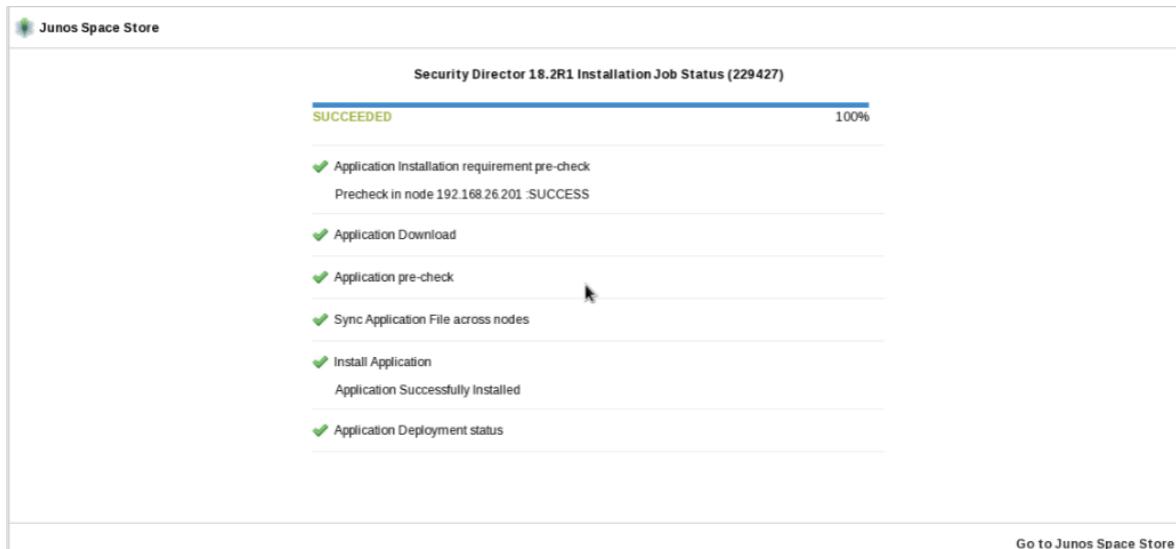
8. Click **Go to Junos Space Store**.

The installed or upgraded version of Security Director is displayed in the Junos Space store as shown in Figure 4 on page 15.

Figure 4: Verifying the Installed or Upgraded Version

Table 2: Security Director Components Description

Fields	Description
Log Collector	
Deployment Mode	• Integrated—The integrated Log Collector is installed on Junos Space node (virtual appliance). Integrated Log Collector on a Junos Space virtual appliance supports only 500 eps. **NOTE**: For Integrated Log Collector, OpenNMS must be disabled. On the Junos Space Network Management Platform, the disk space must be greater than 500GB.
Node Type	Select one of the following: • Security Director Log Collector • Juniper Secure Analytics
Node Name	Enter the Node name.
IP Address	Enter the IPv4 or IPv6 address.

Table 2: Security Director Components Description *(Continued)*

Fields	Description
Username and Password	For Security Director Log Collector, provide the default credentials; username is admin and password is juniper123. Change the default password using the Log Collector CLI `configureNode.sh` command. For JSA, provide the admin credentials that is used to login to the JSA console.
Policy Enforcer	
Deployment Mode	Select Standalone. **NOTE**: For Policy Enforcer, only Standalone option is available.
IP Address	Specify the IP address of the Policy Enforcer virtual machine.
Password	Enter the password to login to the virtual machine with the root credentials.
ATP Cloud Configuration Type	Select one of the following configuration types: • ATP Cloud—Includes all threat prevention types, but does not include the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer. All enforcement is done through SRX Series Firewall policies. • Cloud Feeds Only—The prevention types available are command and control server, infections hosts, and Geo IP feeds. Policy Enforcer Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies are also available. All enforcement is done through SRX Series Firewall policies. • ATP Cloud with Juniper Connected Security —A full version of the product. All Policy Enforcer features and threat prevention types are available. • None—There are no feeds available from ATP Cloud, but the benefits of Secure Fabric, Policy Enforcement Groups, and Threat Prevention policies provided by Policy Enforcer are available. Infected hosts is the only prevention type available.
Network End Point	Polling timers affect how often the system polls to discover endpoints. The timer polls infected endpoints moving within the sites that are a part of Secure fabric. You can set this range from 2 minutes to 60 minutes. The default is 5 minutes.

Table 2: Security Director Components Description *(Continued)*

Fields	Description
PollSite End Point	Polling timers affect how often the system polls to discover endpoints. The timer polls all endpoints added to the secure fabric. You can set this range between 1 to 48 hours. The default is 24 hours.

RELATED DOCUMENTATION

2
CHAPTER

Setting Up and Upgrading Log Collector

IN THIS CHAPTER

Log Collector 24.1 Overview

You can use the Security Director Insights OVA file to install Security Director Insights and use the Security Director Insights VM as a log collector (Log Collector 23.1) and as an integrated Policy Enforcer.

In this chapter, you'll learn how to configure Security Director Insights as a log collector.

Table 3 on page 19 below lists the required specifications for deploying Security Director Insights as a log collector for various events per second (eps) rates.

Table 3: Specifications

EPS	CPU	Memory	CPU/Memory Reservation
5k	6	16	13.2 GHz /16Gb
10k	8	16	17.6 GHz/16Gb
25k	24	80	50 GHz/80Gb

The log retention policies are:

- 365 days

- 80% storage size (This has higher priority)

Benefits

- A single Security Director Insights VM provides up to 25K eps making it easier for you to scale up with less virtual resources.

- Security Director Insights and Policy Enforcer capability are readily available for users of Log Collector 23.1, which is bundled with the Log Collector.

- It is the best long-term solution against vulnerabilities.

Log Collector 24.1 — Architecture

Security Director UI
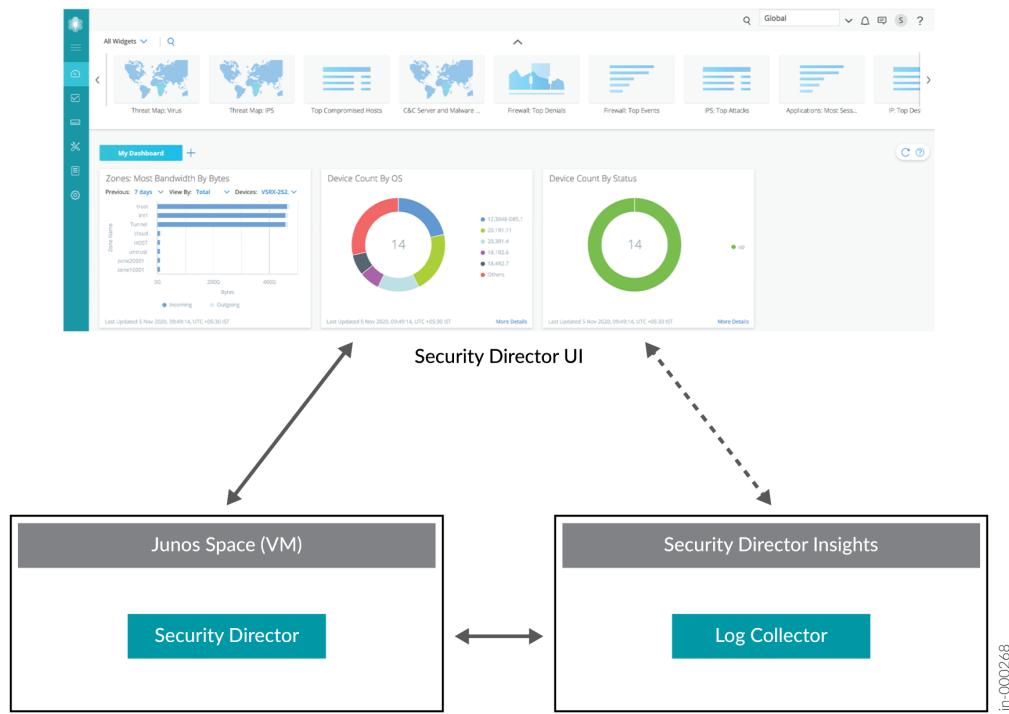
RELATED DOCUMENTATION

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files

Deploy and Configure Security Director Insights with Open Virtualization Appliance (OVA) Files

Security Director Insights requires VMware ESXi server version 6.5 or later to support a virtual machine (VM) with the following configuration:

- 12 CPUs

- 24-GB RAM

- 1.2-TB disk space

If you are not familiar with using VMware ESXi servers, see VMware Documentation and select the appropriate VMware vSphere version.

To deploy and configure the Security Director Insights with OVA files, perform the following tasks:

1. Download the Security Director Insights VM OVA image from the Juniper Networks software download page.

   NOTE: Do not change the name of the Security Director Insights VM image file that you download from the Juniper Networks support site. If you change the name of the image file, the creation of the Security Director Insights VM may fail.

2. Launch the vSphere Client that is connected to the ESXi server, where the Security Director Insights VM is to be deployed.

3. Select **File** > **Deploy OVF Template**.

   The Deploy OVF Template page appears, as shown in Figure 5 on page 22.

Figure 5: Select an OVF Template Page
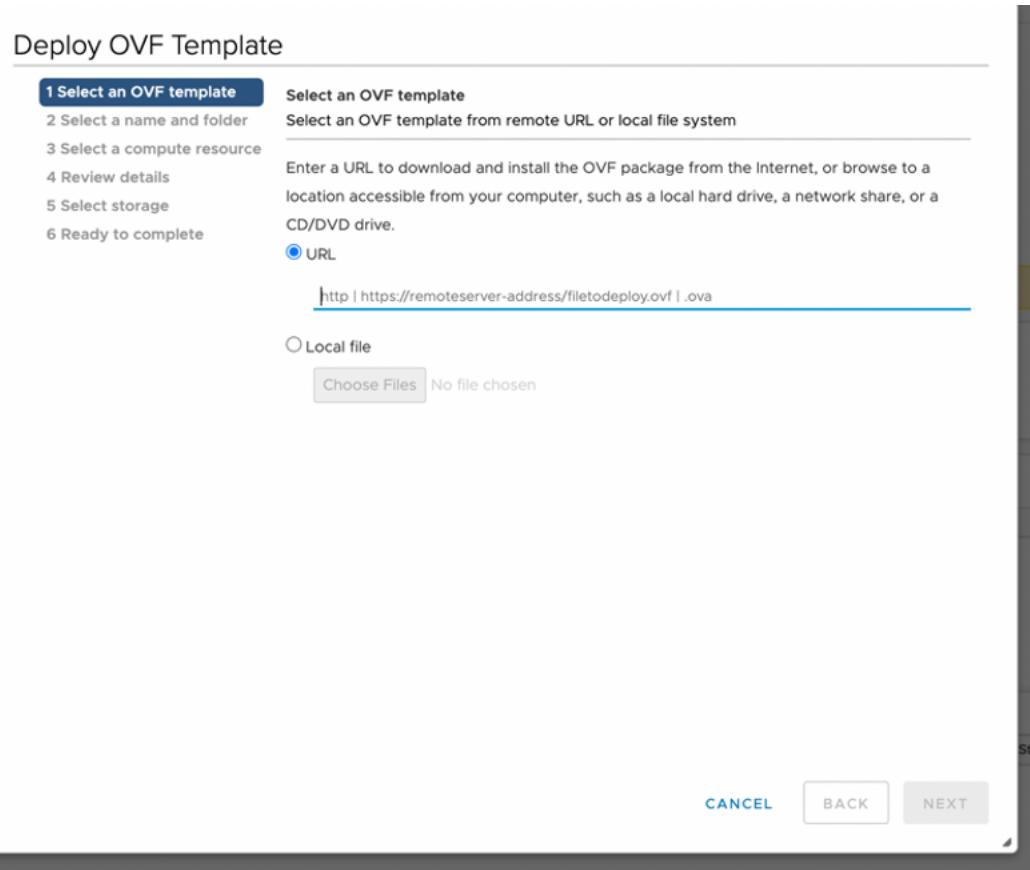
4. In the Select an OVF template page, select the **URL** option if you want to download the OVA image from the internet or select **Local file** to browse the local drive and upload the OVA image.

5. Click **Next**.

    The Select a name and folder page appears.

6. Specify the OVA name, installation location for the VM, and click **Next**.

    The Select a compute resource page appears.

7. Select the destination compute resource for the VM, and click **Next**.

    The Review details page appears.

8. Verify the OVA details and click **Next**.

    The License agreements page appears, as shown in .

Figure 6: License Agreements Page
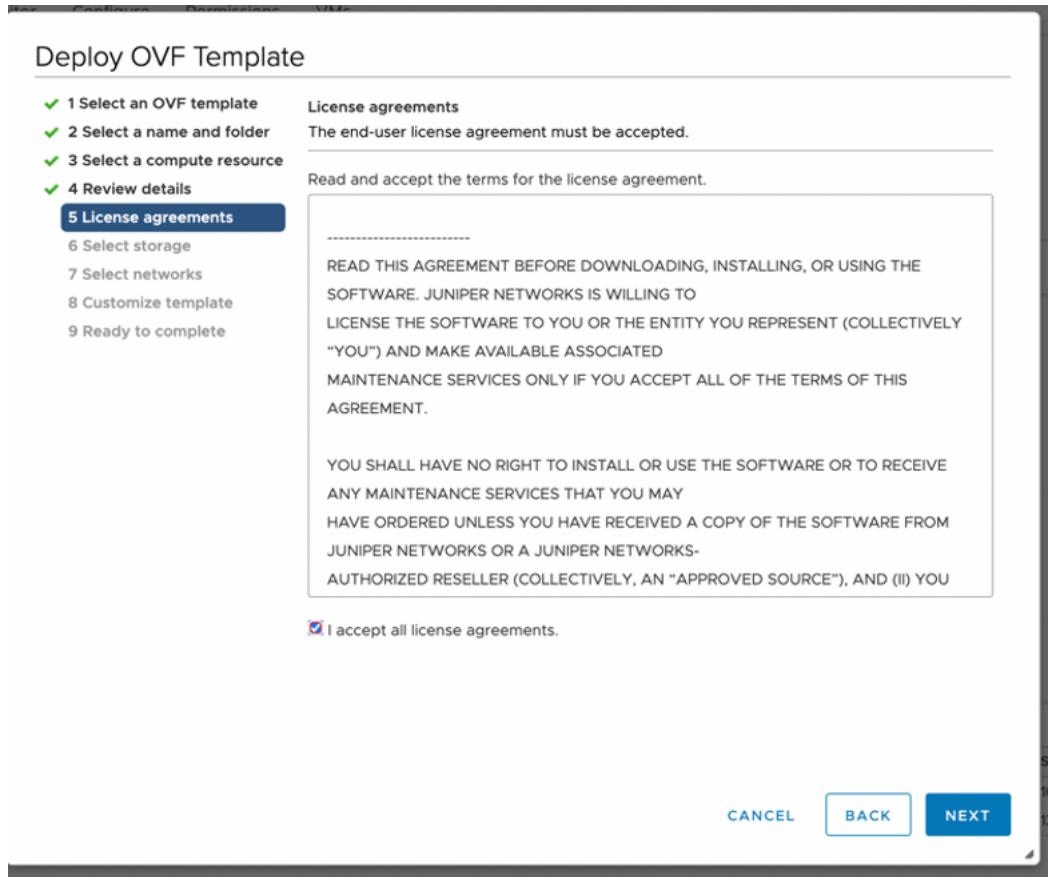
9. Accept the EULA and click **Next**.

   The Select storage page appears.

10. Select the destination file storage for the VM configuration files and the disk format. (Thin Provision is for smaller disks and Thick Provision is for larger disks.)

    Click **Next**. The Select networks page appears.

11. Select the network interfaces that will be used by the VM.

    IP allocation can be configured for DHCP or Static addressing. We recommend using Static IP Allocation Policy.

    Click **Next**. The Customize template page appears. For DHCP instructions, see to Step 13.

12. For IP allocation as Static, configure the following parameters for the virtual machine:

    - IP address—Enter the Security Director Insights VM IP address.

    - Netmask—Enter the netmask.

    - Gateway—Enter the gateway address.

    - DNS Address 1—Enter the primary DNS address.

- DNS Address 2—Enter the secondary DNS address.

Figure 7: Customize Template Page

13. For IP allocation as DHCP, enter the search domain, hostname, device name, and device description for the virtual machine.

    This option is recommended only for the Proof of Concept type of short-term deployments. Do not use this option.

    Click **Next**. The Ready to complete page appears, as shown in .

Figure 8: Ready to Complete Page
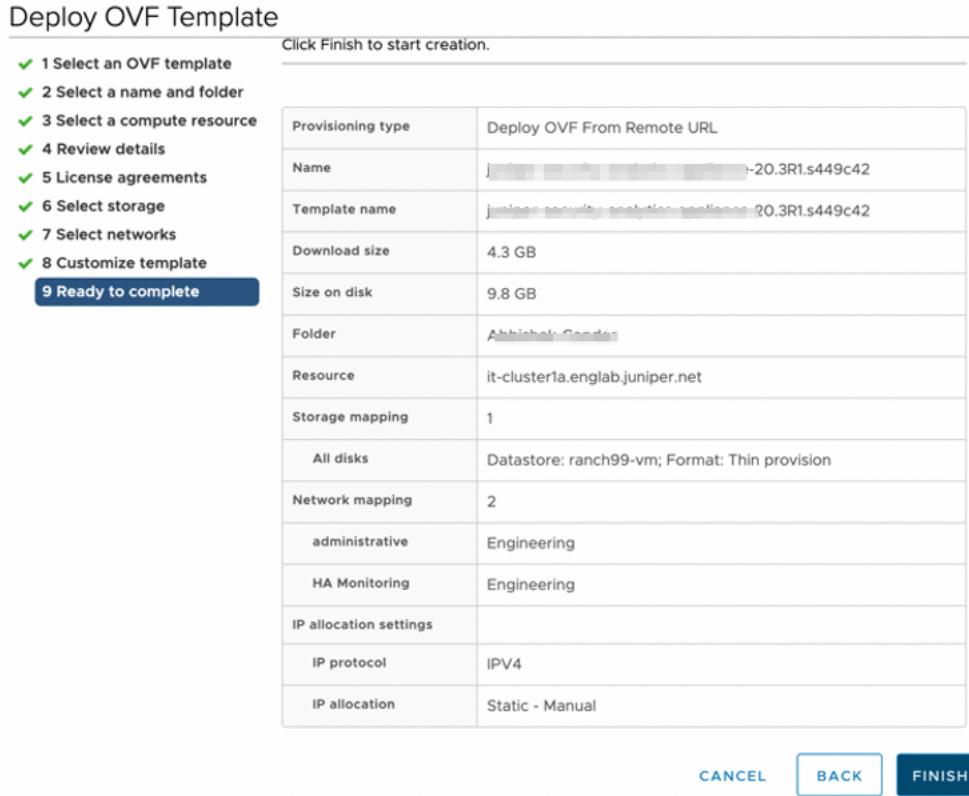
14. Verify all the details and click **Finish** to begin the OVA installation.

15. After the OVA is installed successfully, power on the VM and wait for the boot-up to complete.

16. Once the VM powers on, in the CLI terminal, log in as administrator with the default username as "admin" and password as "abc123".

After you log in, you will be prompted to change the default admin password. Enter a new password to change the default password, as shown in Figure 9 on page 25.

Figure 9: Default Admin Password Reset

The Security Director Insights deployment is now complete.

Add Security Director Insights as a Log Collector

Add Security Director Insights as a Log Collector

To use the log collector functionality that comes along with the Security Director Insights installation, add the IP address of the Security Director Insights virtual machine (VM) as a log collector.

Before you add the log collector node in the GUI, you must set the administrator password. By default, the Security Director log collector is disabled. You must first enable it and then set the administrator password.

To enable the log collector and configure the administrator password:

1. Go to the Security Director Insights CLI.

   ```
   # ssh admin@${security-director-insights_ip}
   ```

2. Enter the application configuration mode.

   ```
   user:Core# applications
   ```

3. Enable Security Director log collector.

   ```
   user:Core#(applications)# set log-collector enable on
   ```

4. Configure the administrator password.

   ```
   user:Core#(applications)# set log-collector password

   Enter the new password for SD Log Collector access:

   Retype the new password:

   Successfully changed password for SD Log Collector database access
   ```

To add the Security Director Insights VM IP address as a log collector node:

1. From the Security Director user interface, select **Administration** > **Logging Management** > **Logging Nodes**, and click the plus sign (+).

   The Add Logging Node page appears.

2. Choose the Log Collector type as **Security Director Log Collector**.

3. Click **Next**.

   The Add Collector Node page appears.

4. In the Node Name field, enter a unique name for the log collector.

5. In the IP Address field, enter the IP address of the Security Director Insights VM.

   The IP address used in the Deploy OVF Template page must be used in the Add Collector Node page, as shown in Figure 10 on page 27 and Figure 11 on page 28.

Figure 10: Deploy OVF Template Page

Figure 11: Add Logging Node Page

6. In the User Name field, enter the username of the Security Director Insights VM.

7. In the Password field, enter the password when you set "user:Core#(applications)# set log-collector password" above.

8. Click **Next**.

The certificate details are displayed.

9. Click **Finish** and then click **OK** to add the newly created Logging Node.

> **(i)** **NOTE**: Starting in Security Director Release 21.3R1 Hot Patch V1, you can add both the legacy log collector node and the Security Director Insights VM on the Logging Nodes page in Security Director. We've added the legacy log collector support for read-only purpose to view existing data in the event viewer. You cannot add same type of log collector nodes on the Logging Nodes page.

10. After you add Security Director Insights as a log collector, enable the following options in Junos Space:

a. Log in to Junos Space.

b. Select **Administration** > **Applications**.

c. Right-click **Log Director** and select **Modify Application Settings**.

d. Enable the following options:

- Enable SDI Log Collector Query Format

- Integrated Log Collector on Space Server

Performance Matrix

shows the performance matrix for various events per second (eps) rates.

Table 4: Performance Matrix for EPS

CPU	Memory	EPS	CPU/Memory Reservation
6	16	5K	13.2 GHz / 16Gb
12	24	10K	26.4 GHz / 24Gb
24	80	25K	50 GHz / 80Gb

> **NOTE**: CPU and Memory values must be reserved according to the performance matrix, to achieve the correlating EPS.

RELATED DOCUMENTATION

Configure Security Director Insights High Availability

Security Director Insights High Availability Deployment Architecture

Configure Policy Enforcer for Security Director Insights Mitigation

Upgrade Security Director Insights

Table 5 on page 30 shows Security Director Insights upgrade path.

Table 5: Upgrade Path

Upgrading to Release	Upgrade Path
Security Director Insights 23.1R1	22.3R1 > 23.1R1
Security Director Insights 22.3R1	22.2R1 > 22.3R1
Security Director Insights 22.2R1	22.1R1 > 22.2R1
Security Director Insights 22.1R1	21.3R1 > 22.1R1
Security Director Insights 21.3R1	21.2R1 > 21.3R1

To upgrade from a previous version of Security Director Insights:

1. Download the release image from the download site to a location (virtual machine) that is accessible from Security Director Insights.

2. Type `server` to switch to the server mode of CLI.

3. Copy the upgrade package to Security Director Insights:

   `set system-update copy user@ip_addr:/location`.

Figure 12: Copy the Upgrade Package

> **NOTE:** You can host the upgrade file to any location that is accessible by secure copy protocol (scp).

4. Check the copy progress:

   `show system-update copy.`

Figure 13: Check Copy Progress

5. Check the available upgrade versions:

   `show system-update versions.`

Figure 14: Available Upgrade Versions

6. Start the upgrade process:

   `set system-update start software <version-number>.`

   Use the <tab> key to select the software version number.

Figure 15: Start Upgrade Process

7. Monitor the status of upgrade:

   `show system-update status`.

Figure 16: Monitor Upgrade Status

JSA Log Collector Overview

You can use Juniper Secure Analytics (JSA) as a Log Collector to view log data in Security Director. From the JSA console, Security Director queries logs from SRX Series devices. Security Director can use either JSA3800, JSA5800, JSA7500, or virtual JSA for log collection. You must add JSA as a logging node in Security Director to view log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

> **NOTE**: The JSA version supported by Security Director to be added as log collector node is JSA Release 2014.8.R4 or later.

After JSA is deployed, you can configure network devices to send system logs to JSA. It collects the logs in a standalone or clustered setup. For more details on deploying and configuring JSA, see Juniper Secure Analytics documentation.

Figure 17 on page 33 shows the deployment example using the JSA All-in-One or JSA Dedicated Console.

Figure 17: Using JSA All-in-One or JSA Dedicated Console
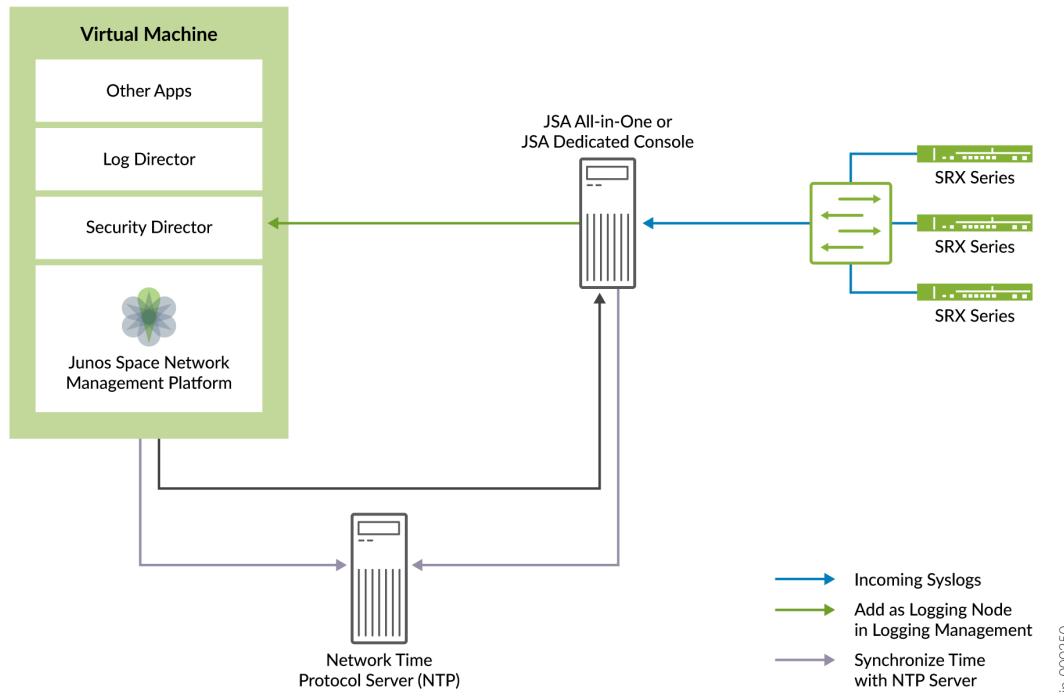
To add JSA as a logging node in Security Director, see "Add JSA Log Collector Node to Security Director" on page 33.

Add JSA Log Collector Node to Security Director

Before You Begin

- Deploy JSA as a Log Collector.

- Configure system log and security logging for the devices managed by Junos Space Security Director from **Devices** > **Security Devices** > **Modify Configuration**.

- While adding SRX firewall as a log source in JSA or QRadar, set the log source type to Juniper Junos Platform and not Juniper SRX Series Services Gateway.

- You must have the recent version of Juniper Junos Device Support Module (DSM) installed on JSA or QRadar.

- After upgrading Log Collector, database password will reset to default credentials, that is, admin/abc123. You must re-configure the database password after Log Collector upgrade before adding the Log Collector node to Security Director.

You must deploy Juniper Secure Analytics (JSA) as a log collector and then add it to Security Director to view the log data in the Dashboard, Events and Logs, Reports, and Alerts pages.

To add Log Collector to Security Director:

1. From the Security Director user interface, select **Administration** > **Logging Management** > **Logging Nodes**, and click the plus sign (+).

   The Add Logging Node page appears.

2. Choose the Log Collector type as **Juniper Secure Analytics**.

3. Click **Next**.

4. Complete the configuration for JSA Node.

   > ⚠️ **CAUTION**: For JSA, provide the admin credentials that is used to log in to the JSA console.

5. Click **Next**.

   The certificate details are displayed.

6. Click **Finish**.

7. Review the summary of configuration changes from the summary page and click **Edit** to modify the details, if required.

8. Click **OK** to add the node.

   A new logging node with your configuration is added. To verify that the node is configured correctly, click **Logging Management** to check the status of the node.

To remove an existing Security Director Log Collector and add JSA as a Log Collector:

1. Select **Administration** > **Logging Management** > **Logging Nodes**.

2. Select the existing Security Director Log Collector and click the delete icon to delete Security Director Log Collector node.

3. Click the **+** icon to add JSA as a Log Collector.

4. Configure the SRX Series devices to stop sending logs to Security Director Log Collector, and ensure that logs are sent to the JSA node.

RELATED DOCUMENTATION

3

CHAPTER

Migrate Standalone Policy Enforcer

IN THIS CHAPTER

Migrate Policy Enforcer Release 23.1R1 to Policy Enforcer Release 24.1R1.

Starting in Junos Space Security Director Release 24.1R1, you cannot use standalone Policy Enforcer. You'll need to migrate to Policy Enforcer running on Security Director Insights 24.1R1.

You must migrate the standalone Policy Enforcer Release 23.1R1 data to Security Director Insights 24.1R1.

Policy Enforcer migration procedure is based on the existing backup and restore functionality.

> **NOTE**: You must migrate the standalone Policy Enforcer Release 23.1R1 data to Security Director Insights 24.1R1.

Before migrating Standalone Policy Enforcer to Security Director Insights Policy Enforcer, you must first upgrade from Junos Space Network Management Platform 23.1R1 or Security Director 23.1R1 to Junos Space Network Management Platform 24.1R1 or Security Director 24.1R1 respectively.

For more details on the upgrade procedure, see Upgrade to Junos Space Network Management Platform Release 24.1R1.

To migrate Standalone Policy Enforcer to Security Director Insights Policy Enforcer:

1. Take a backup of the changes in Security Director Release 23.1R1 and store in a remote server. Follow the instructions mentioned in Policy Enforcer Backup and Restore

   Before initiating the backup, you must upgrade Standalone Policy Enforcer Release 23.1R1 V2 or Security Director Insights Policy Enforcer to the latest hot patch version available.

2. Shut down the Policy Enforcer from which the back up has been taken.

3. Add Security Director Insights 24.1 Policy Enforcer to Security Director.

4. Initiate the restore process as shown in .

Figure 18: Backup and Restore

5. When the restore process is complete as shown in Figure 19 on page 38, re-add Policy Enforcer.

Figure 19: Restore Status

6. Go to **Administration** > **Policy Enforcer** > **Settings** and enter the required details on the settings window and click **OK**. See Figure 20 on page 39 for more details.

Figure 20: Re-add Policy Enforcer

7. After Policy Enforcer is configured, a prompt appears to confirm if you want to setup the Threat Policies in a guided setup as shown in . Click **OK** but ignore the guided setup for Threat Policies, as it is redundant.

Figure 21: Threat Policy Prevention
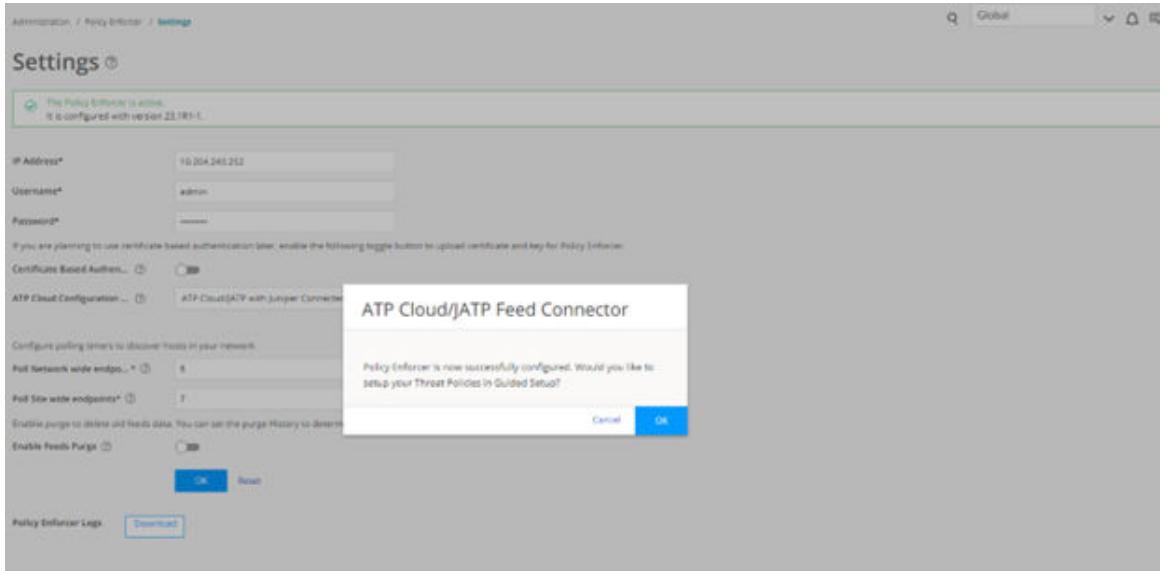
8. Navigate to **Configure** > **Threat Prevention** > **Feed Sources** and re-add the realm and assign a site to the realm. This is to sync the feed and device with the realm and Policy Enforcer.

9. Make sure the realm comes to sync in sometime and feed status is **OK** as shown in Figure 22 on page 40.

Figure 22: Feed Sources

10. Ensure that the security intelligence URL and the IP address is displayed for the device. Here is an example:

```
Iroot@vS1RX-23.2R1.13> show configuration services security—intelligence url | display set
set services security—intelligence url https://10.204.243.201:444/api/v1/manifest.xml
```

11. Navigate to **Secure Fabric** > **Sites** and verify if the **Feed Source Status** shows **Success**. For more details see, Figure 23 on page 41

Figure 23: Secure Fabric

12. Navigate to **Configure** > **Threat Prevention** > **Policies** > **Threat Prevention Policies** and verify the status of the policy recovered from backup. For details, see .

Figure 24: Threat Prevention Policies

13. Click **Update required** under the status tab for Threat Prevention Policies and proceed with the update.

Older policies gets replaced by the newer ones as shown in .

Figure 25: Policy Change List

14. Go to **Configure** > **Shared Objects** > **Geo IP** and perform the Geo IP analysis and update the generated policies to the device. For details see .

Figure 26: Geo IP

15. Go to **Administration** > **Policy Enforcer** > **Connectors** as shown in Figure 27 on page 44.

Figure 27: Connectors
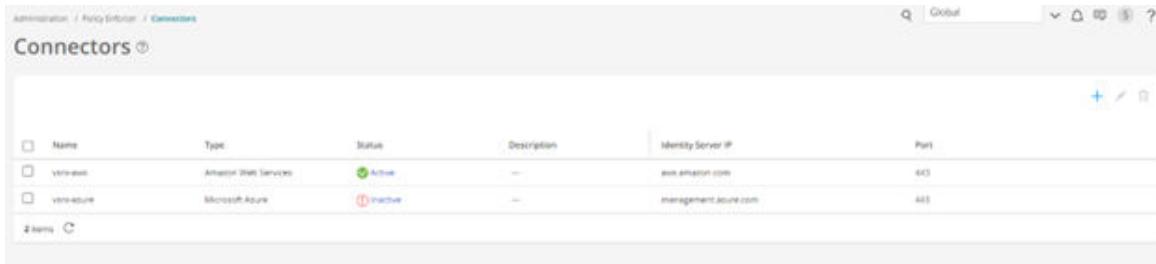
The status of the connector shows **Inactive** by default.

16. Modify or delete and re-add the failed connectors to make them active.

   If you re-add the connector by editing the existing connector, you must perform the following:

   - Re-add the credentials and `pem` file again.

   - Ensure that you have selected the other values for tags correctly.

   Migration of Standalone Policy Enforcer to Security Director Insights Policy Enforcer is complete.

   > **NOTE**: The migrated custom feed may take approximately 10 mins to sync due to internal activities involved in schema versioning, manifest generation for the feeds to be available for consumption to SRX devices. The time consumed depends on the feed type and feed volume.