

# Junos Space Security Director Release 21.3R1

Published  
2024-07-31

RELEASE

# Table of Contents

[Introduction](#)

[New and Changed Features](#)

[Supported Managed Devices](#)

[Supported Log Collection Systems](#)

[Supported Junos OS Releases](#)

[Supported Policy Enforcer and Juniper® Advanced Threat Prevention \(ATP\) Cloud Releases](#)

[Supported Browsers](#)

[Installation and Upgrade Instructions](#)

[Loading Junos OS Schema for SRX Series Devices](#)

[DMI Schema Compatibility for Junos OS Service Releases](#)

[Management Scalability](#)

[Known Behavior](#)

[Known Issues](#)

[Resolved Issues](#)

[Hot Patch Releases](#)

[Finding More Information](#)

[Revision History](#)

# Introduction

The Junos Space® Security Director application is a powerful and easy-to-use solution that enables you to secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, intrusion prevention system (IPS) policies, and application firewalls.

**NOTE:** You need IPS and application firewall licenses to push IPS policies and application firewall signatures to a device.

## New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 21.3R1.

- **Onboard devices to Juniper® Security Director Cloud**—Starting in Security Director Release 21.3R1, you can add Security Director managed devices to Juniper Security Director Cloud. You can add only root devices or the primary root device in a cluster device. Juniper Security Director Cloud automatically discovers the secondary device in a cluster. You cannot add MX Series, cSRX, logical system, and tenant system devices to Juniper Security Director Cloud.
- **Root certificates**—Starting in Security Director Release 21.3R1, you can configure multiple certificates in the SSL proxy profile.
- **Action for out-of-band policy changes**—Starting in Security Director Release 21.3R1, during automatic synchronization of out-of-band firewall, intrusion prevention system (IPS), and NAT policy changes from a device to Security Director, you can choose from rename object, keep existing value, or overwrite with imported value. By default, Rename Object is selected.
- **RT\_FLOW\_SESSION logs support**—Security Director does not use AppTrack logs, instead it retrieves the data from RT\_FLOW\_SESSION logs. For application visibility feature to function and to view application data in Security Director, session-close log should be enabled at rule level.

For example: set security policies from-zone untrustZone to-zone trustZone policy policy13 then log session-close

For new features and enhancements in Policy Enforcer, see [Policy Enforcer Release Notes](#).

# Supported Managed Devices

You can use Security Director Release 21.3R1 to manage the following devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX240H
- SRX300
- SRX320
- SRX320-POE
- SRX340
- SRX345
- SRX380
- SRX550
- SRX550M
- SRX650
- SRX1400
- SRX1500
- SRX3400
- SRX3600
- SRX4100
- SRX4200
- SRX5400
- SRX5600

- SRX5800
- SRX4600
- vSRX
- MX240
- MX480
- MX960
- MX2010
- MX2020
- LN1000-V
- LN2600

## Supported Log Collection Systems

The following log collection systems are supported:

- Log Collector 21.3 (Security Director Insights VM)
- Integrated Log Collector 20.1R1
- Juniper Networks® Secure Analytics (JSA) Series Virtual Appliance as Log Collector on JSA Release 2014.8.R4 and later
- QRadar as Log Collector on QRadar Release 7.2.8 and later

**NOTE:** Starting in Security Director Release 20.2R1 onward, we're not supporting standalone Log Collector.

## Supported Junos OS Releases

Security Director Release 21.3R1 supports the following Junos OS releases:

- 10.4
- 11.4
- 12.1
- 12.1X44
- 12.1X45
- 12.1X46
- 12.1X47
- 12.3X48
- 15.1X49
- vSRX 15.1X49
- 16.1R3-S1.3
- 15.1X49-D110
- 17.3
- 17.4
- 18.1
- 18.1R2.6
- 18.2
- 18.2R3.4
- 18.3
- 18.4
- 18.4R3.3
- 19.1
- 19.2
- 19.3
- 19.4
- 20.1

- 20.2
- 20.3
- 20.4
- 21.1
- 21.2

SRX Series devices require Junos OS Release 12.1 or later to synchronize the Security Director description field with the device.

The logical systems feature is supported only on devices running Junos OS Release 11.4 or later.

**NOTE:** To manage an SRX Series device by using Security Director, we recommend that you install the matching Junos OS schema on the Junos Space Network Management Platform. If the Junos OS schemas do not match, a warning message is displayed during the publish preview workflow.

## Supported Policy Enforcer and Juniper® Advanced Threat Prevention (ATP) Cloud Releases

[Table 1 on page 5](#) shows the supported Policy Enforcer and Juniper ATP Cloud releases.

**Table 1: Supported Policy Enforcer and Juniper ATP Cloud Releases**

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud supported devices)
16.1R1	16.1R1	Junos OS Release 15.1X49-D60 and later
16.2R1	16.2R1	Junos OS Release 15.1X49-D80 and later

**Table 1: Supported Policy Enforcer and Juniper ATP Cloud Releases (Continued)**

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud supported devices)
17.1R1	17.1R1	Junos OS Release 15.1X49-D80 and later
17.1R2	17.1R2	Junos OS Release 15.1X49-D80 and later
17.2R1	17.2R1	Junos OS Release 15.1X49-D110 and later
17.2R2	17.2R2	Junos OS Release 15.1X49-D110 and later
18.1R1	18.1R1	Junos OS Release 15.1X49-D110 and later
18.1R2	18.1R2	Junos OS Release 15.1X49-D110 and later
18.2R1	18.2R1	Junos OS Release 15.1X49-D110 and later
18.3R1	18.3R1	Junos OS Release 15.1X49-D110 and later
18.4R1	18.4R1	Junos OS Release 15.1X49-D110 and later
19.1R1	19.1R1	Junos OS Release 15.1X49-D110 and later
19.2R1	19.2R1	Junos OS Release 15.1X49-D120 and later



**Table 1: Supported Policy Enforcer and Juniper ATP Cloud Releases (*Continued*)**

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud supported devices)
19.3R1	19.3R1	Junos OS Release 15.1X49-D120 and later
19.4R1	19.4R1	Junos OS Release 15.1X49-D120 and later
20.1R1	20.1R1	Junos OS Release 15.1X49-D120 and later
20.3R1	20.3R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
21.1R1	21.1R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
21.2R1	21.2R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
21.3R1	21.3R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later

**NOTE:** For Policy Enforcer details, see [Policy Enforcer Release Notes](#).

## Supported Browsers

Security Director Release 21.3R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

## Installation and Upgrade Instructions

### IN THIS SECTION

- [Installing and Upgrading Security Director Release 21.3R1 | 8](#)

This section describes how you can install and upgrade Junos Space Security Director and Log Collector.

### Installing and Upgrading Security Director Release 21.3R1

Junos Space Security Director Release 21.3R1 is supported only on Junos Space Network Management Platform Release 21.3R1 that can run on the following devices:

- Juniper Networks® JA2500 Junos Space® Appliance
- Junos Space virtual appliance
- Kernel-based virtual machine (KVM) server installed on CentOS Release 7.2.1511

For more information about installing and upgrading Security Director and Log Collector 21.3 (Security Director Insights VM), see [Security Director Installation and Upgrade Guide](#).

# Loading Junos OS Schema for SRX Series Devices

You must download and install correct Junos OS schema to manage SRX Series devices. To download the correct schema, from the Network Management Platform list, select **Administration > DMI Schema**, and click **Update Schema**. See [Updating a DMI Schema](#).

## DMI Schema Compatibility for Junos OS Service Releases

The following tables explain how the Junos Space Network Management Platform chooses Device Management Interface (DMI) schemas for devices running Junos OS Service Releases.

If a Junos OS Service Release is installed on your device with a major release version of a DMI schema installed on Junos Space Network Management Platform, then Junos Space chooses the latest corresponding major release of DMI schemas, as shown in [Table 2 on page 9](#).

**Table 2: Device with Service Release and Junos Space with FRS Release**

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.4R1.8 18.3R1.1 18.2R1.1	18.2R1.1	18.4R1.8
If 18.4R1.8 version is not available, then Junos Space chooses the nearest lower version of DMI schema installed.			
18.4R1-S1	18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If a Junos OS Service Release is installed on your device without a matching DMI schema version in Junos Space Network Management Platform, then Junos Space chooses the nearest lower version of DMI schema installed, as shown in [Table 3 on page 10](#).

**Table 3: Device with Service Release and Junos Space without matching DMI Schema**

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.5R1.1 18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If more than one version of the DMI schemas are installed in Junos Space Platform for a single Junos OS Service Release version, Junos Space chooses the latest version of the DMI schema, as shown in [Table 4 on page 10](#).

**Table 4: Device with Service Release and Junos Space with more than one DMI Schemas**

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.4R1.8 18.4R1.7 18.4R1.6 18.3R1.1	18.3R1.1	18.4R1.8
If 18.4R1.x versions are not available, then Junos Space chooses the nearest lower version of DMI schema installed.			
18.4R1-S1	18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If a Junos OS Service Release is installed on your device without a corresponding DMI schema version in Junos Space Network Management Platform, then Junos Space chooses the nearest lower version of DMI schema installed, as shown in [Table 5 on page 11](#).

Table 5: Device with Service Release and Junos Space without more DMI Schemas

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1.1	18.5R1.1 18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

For information about Junos OS compatibility, see [Junos OS Releases Supported in Junos Space Network Management Platform](#).

## Management Scalability

The following management scalability features are supported in Junos Space Security Director:

- By default, monitor polling is set to 15 minutes and resource usage polling is set to 10 minutes. This polling time changes to 30 minutes for a large-scale data center setup such as one for 200 SRX Series devices managed in Security Director.

**NOTE:** You can manually configure the monitor polling on the **Administration>Monitor Settings** page.

- Security Director supports up to 15,000 SRX Series devices with a six-node Junos Space fabric. In a setup with 15,000 SRX Series devices, all settings for monitor polling must be set to 60 minutes. If monitoring is not required, disable it to improve the performance of your publish and update jobs.
- To enhance the performance further, increase the number of update subjobs thread in the database. To increase the update subjobs thread in the database, run the following command:

```
#mysql -u <mysql-username> -p <mysql-password> sm_db;
mysql> update RuntimePreferencesEntity SET value=20 where name='UPDATE_MAX_SUBJOBS_PER_NODE';
mysql> exit
```

**NOTE:** For MySQL username and password, contact Juniper Support.

**NOTE:** If you use a database dedicated setup (SSD hard disk VMs), the performance of publish and update is better compared to the performance in a normal two-node Junos Space fabric setup.

## Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 21.3R1.

- You can generate a temporary password in Security Director under **Administration > Users & Roles > Users** by either creating a new user or editing an existing user.

Make sure you check the **Generate** checkbox on the **Create User** or the **Edit User** window to create a temporary password.

After you generate the temporary password in Security Director, you must first log in through Junos Space Network Management Platform GUI and not Security Director GUI.

- To discover the tenant devices in Security Director Release 21.2R1, we recommend the schema to be greater than or equal to 20.1R1. You must install the schema before Security Director discovers a tenant device.
- If you configure VPN in Security Director Release earlier to 19.4R1 and upgrade Security Director to Release 20.1R1 and later, IKE ID is displayed blank if IKE ID is defined as Default.
- Security Director does not generate CLIs for deletion if a VPN is already configured in the device and the same device is used for creating another VPN from Security Director.
- In Security Director Release 20.1R1 and later, you must configure a tunnel IP address for dynamic routing protocols. In Security Director Release 19.4R1 and earlier, if you configure VPN as unnumbered with a dynamic routing protocol, you are prompted to provide a tunnel IP address while editing the VPN after upgrading to Security Director Release 20.1R1 and later.
- After upgrade, you cannot edit profiles with predefined proposals because the profiles in Security Director Release 20.1R1 and later support only custom proposals.

- In Security Director Release 19.4R1 and earlier, if you configure a VPN with static routing or a traffic selector with protected network as the zone or interface, you must perform the following tasks:
  1. Before you upgrade to Security Director Release 20.1R1 and later, update the configuration on the device, and delete the VPN policy from Security Director.
  2. After you upgrade, import the VPN configuration.

**NOTE:** In Security Director Release 20.1R1 and later, we support only address objects in protected networks for static routing and traffic selector.

- You must enable the **Enable preview and import device change** option, which is disabled by default:
  1. Select **Network Management Platform > Administration > Applications**.
  2. Right-click **Security Director**, and select **Modify Application Settings**.
  3. From Update Device, select the **Enable preview and import device change** option.
- If you restart the JBoss application servers manually in a six-node setup one by one, the Junos Space Network Management Platform and Security Director user interfaces are launched within 20 minutes, and the devices reconnect to Junos Space Network Management Platform. You can then edit and publish the policies. When the connection status and the configuration status of all devices are UP and IN SYNC, respectively, click **Update Changes** to update all security-specific configurations or pending services on SRX Series devices.
- To generate reports in the local time zone of the server, you must modify `/etc/sysconfig/clock` to configure the time zone. Changing the time zone on the server by modifying `/etc/localtime` does not generate reports in the local time zone.
- If the vSRX VMs in NSX Manager are managed in Security Director Release 17.1R1 and Policy Enforcer Release 17.1R1, then after upgrading to Security Director Release 20.3R1 and Policy Enforcer Release 20.3R1, we recommend that you migrate the existing vSRX VMs in NSX Manager from Policy Enforcer Release 17.1R1 to Release 20.3R1.

To migrate the existing vSRX VMs:

1. Log in to the Policy Enforcer server by using SSH.
2. Run the following commands:

```
cd /var/lib/nsxmicro
./migrate_devices.sh
```

- If the NSX Server SSL certificate has expired or changed, communication between Security Director and NSX Manager fails, thereby impacting the functionality of NSX Manager, such as sync NSX inventory and security group update.

To refresh the NSX SSL certificate:

1. Log in to Policy Enforcer by using SSH.
2. Run the following command:

```
nsxmicro_refresh_ssl --server <<NSX IP ADDRESS>>--port 443
```

This script fetches the latest NSX SSL certificate and stores it for communication between Security Director and NSX Manager.

- In a setup where other applications are installed in Junos Space Network Management Platform along with Security Director, the JBoss PermSize must be increased from 512m to 1024m in the `/usr/local/jboss/domain/configuration/host.xml.slave` file. Under `<jvm name="platform">`, change the following values in the `<jvm-options>` tag:

```
<option value="-XX:PermSize=1024m"/>
```

```
<option value="-XX:MaxPermSize=1024m"/>
```

- When you import addresses through CSV, a new address object is created by appending `a_1` to the address object name if the address object already exists in Security Director.

## Known Issues

This section lists the known issues in Junos Space Security Director Release 21.3R1.

For the most complete and latest information about known Security Director defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

- A policy analysis report with more than 20000 rules cannot be generated. [PR1708393](#)
- SSL certificate error is displayed while analyzing threat prevention policy. [PR1648734](#)
- In a multi node setup, user is unable to push license from Security Director to an SRX Series device. <https://prsearch.juniper.net/PR1636657>
- When you use Security Director Insights as a log collector, device selection on Monitor page does not work when a logical system or a tenant system device is selected. [PR1621052](#)
- Security Director displays device lookup failed error during preview. [PR1617742](#)



Workaround:

1. Move the device to RMA state. Navigate to Junos Space Network Management Platform. Select **Devices > Device Management**. Select a device, right-click and select **Device Operations** and then select **Put in RMA State**.
  2. Reactivate the device from RMA state. Navigate to Junos Space Network Management Platform. Select **Devices > Device Management**. Select a device, right-click and select **Device Operations** and then select **Reactivate from RMA**.
- Primary cluster displays the status as DOWN while both devices in the device cluster displays the status as UP. [PR1616993](#)

Workaround:

1. Move the device to RMA state. Navigate to Junos Space Network Management Platform. Select **Devices > Device Management**. Select a device, right-click and select **Device Operations** and then select **Put in RMA State**.
  2. Reactivate the device from RMA state. Navigate to Junos Space Network Management Platform. Select **Devices > Device Management**. Select a device, right-click and select **Device Operations** and then select **Reactivate from RMA**.
- Security Director does not clear uncommitted logical system or tenant system device management configuration in case of job failure, which causes subsequent updates to fail. You must clear the configuration from space node before proceeding with next update. [PR1603146](#)

Workaround: Navigate to **Junos Space Network Management Platform > Devices > Device Management > Modify Configuration > Deploy > Reject Changes**.

- Security Director fails to import policies when custom dynamic-applications are configured at root-level and referred in logical system or tenant system policies. <https://prsearch.juniper.net/PR1602677>
- An icon showing out-of-band changes is seen for firewall and IPS policies, although the corresponding policy changes are not made on the device. [PR1484953](#)

Workaround: Clear the out-of-band icon on the policies when changes are not made on the device. Navigate to the corresponding policy, and right-click the policy. Select **View Device Policy Changes** and reject all changes, and then click **OK**.

- Deployment of cipher list CLI works only when you perform Save, or Save and Deploy. [PR1485949](#)

Workaround: You must save or deploy the selected Cipher list before you view the preview changes.

- An object conflict occurs when you import Web filter profiles with duplicate names, although the values are the same. [PR1420341](#)

Workaround: Select either **Overwrite with Imported Value** or **Keep Existing Object** to avoid duplicate objects.

- Junos Space Security Director does not support routing instances and proxy profiles in an antivirus pattern update for the unified threat management (UTM) default configuration. [PR1462331](#)
- When you import out-of-band changes to a logical system device, a job is created for the root device along with the logical system device, although changes are made only in the logical system device. [PR1448667](#)
- Import fails when a device is imported only with UTM custom objects without a UTM policy. [PR1447779](#)

Workaround: Delete the UTM custom objects if they are not used in a policy, or assign a UTM policy.

- Update fails for unified policies when an SSL proxy profile that is set as global in a device is not used in any policy for that device. [PR1407389](#)
- A policy analysis report with a large number of rules cannot be generated. [PR1418125](#)
- When a column filter is used, the **Deselect all** and **Clear all** options do not clear selected items occasionally. [PR1424112](#)
- The Show Unused option is not available for URL categories. [PR1431345](#)
- Restart of a single JBoss node does not recover the system even if the issue is present on a single node. [PR1478804](#)

Workaround: Restart all JBoss nodes.

For known issues in Policy Enforcer, see [Policy Enforcer Release Notes](#).

## Resolved Issues

This section lists the issues fixed in Junos Space Security Director 21.3R1:

For the most complete and latest information about resolved issues, use the Juniper Networks online [Junos Problem Report Search](#) application.

- There are issues with top-talker and top source IPs by bandwidth reports. [PR1587200](#)
- Proxy ARP delete commands are generated though the proxy ARP setting is enabled. [PR1598341](#)
- There are issues with policy update after you rename objects. [PR1601704](#)

- Policy update to cluster devices fails without any error message. [PR1602370](#)
- When the application name is Any, there is a dynamic application name mismatch between SRX Series device and Security Director. [PR1603010](#)
- There is an issue with the SRX Series device packet capture timestamp. [PR1603617](#)
- Network Management Platform causes MySQL packet.db tables to increase over 17 GB and create issues on node replication. [PR1607509](#)
- There is an error while calculating rules to publish. [PR1608285](#)
- The SRX Series device import fails. [PR1609767](#)
- VPN monitoring does not work as expected. [PR1611051](#)
- Multiple auto policy sync jobs are generated for a single commit. [PR1613144](#)
- Deletion of all devices from the top check box in Security Director does not work. [PR1618523](#)
- Security Director does not import addresses from a CSV file. [PR1623570](#)
- Security Director sets antispam and web-filtering CLIs after import. [PR1619077](#)
- Address object import from a CSV file fails. [PR1623265](#)
- Security Director does not fetch user details from Juniper® Identity Management Service (JIMS). [PR1621785](#)
- If you are using a device running Junos OS Release 21.1R1 and later, due to apptrack changes, you are unable to view application data in Security Director. [PR1502587](#)

## Hot Patch Releases

### IN THIS SECTION

- [Installation Instructions | 18](#)
- [New and Enhanced Features in the Hot Patch | 19](#)
- [Known Issues in Hot Patches | 21](#)
- [Resolved Issues in Hot Patches | 21](#)

This section describes the installation procedure, features, and resolved issues in Junos Space Security Director Release 21.3R1 hot patch.

During hot patch installation, the script performs the following operations:

- Blocks the device communication.
- Stops JBoss, JBoss Domain Controller (JBoss-dc), and jmp-watchdog services.
- Backs up existing configuration files and EAR files.
- Updates the Red Hat Package Manager (RPM) files.
- Restarts the watchdog process, which restarts JBoss and JBoss-dc services.
- Unblocks device communication after restarting the watchdog process for device load balancing.

**NOTE:** You must install the hot patch on Security Director Release 21.3R1 or on any previously installed hot patch. The hot patch installer backs up all the files which are modified or replaced during hot patch installation.

## Installation Instructions

**NOTE:** You must install the latest Junos Space Network Management Platform Release 21.3 hot patch v2 and above, before installing the latest Security Director hot patch.

Perform the following steps in the CLI of the JBoss-VIP node only:

1. Download the Security Director 21.3R1 Patch vX from the [download site](#).

Here, X is the hot patch version. For example, v1, v2, and so on.

2. Copy the **SD-21.3R1-hotpatch-vX.tgz** file to the **/home/admin** location of the VIP node.
3. Verify the checksum of the hot patch for data integrity:

```
md5sum SD-21.3R1-hotpatch-vX.tgz.
```

4. Extract the **SD-21.3R1-hotpatch-vX.tgz** file:

```
tar -zxvf SD-21.3R1-hotpatch-vX.tgz
```

5. Change the directory to **SD-21.3R1-hotpatch-vX**.

```
cd SD-21.3R1-hotpatch-vX
```

6. Execute the `patchme.sh` script from the **SD-21.3R1-hotpatch-vX** folder:

```
sh patchme.sh
```

The script detects whether the deployment is a standalone deployment or a cluster deployment and installs the patch accordingly.

A marker file, `/etc/.SD-21.3R1-hotpatch-vX`, is created with the list of Red-hat Package Manager (RPM) details in the hot patch.

**NOTE:** We recommend that you install the latest available hot-patch version, which is the cumulative patch.

## New and Enhanced Features in the Hot Patch

Junos Space Security Director Release 21.3R1 hot patch includes the following enhancements:

- **Manage threat prevention policy without Policy Enforcer**—Starting in Junos Space Security Director Release 21.3R1 Hot Patch V1, you can manage threat prevention policies even if you haven't configured Policy Enforcer. If you create and associate a threat prevention policy or profile with the firewall policy using the device CLI or J-Web without configuring Policy Enforcer, then Security Director doesn't delete the threat prevention policy or profile when you preview or update the firewall policy. Therefore, you don't have to reconfigure the threat prevention policy or profile, and reassociate it with the firewall policies in the device.

**NOTE:** This feature is applicable only when you create a threat prevention policy and associate it to existing rules using the device CLI or J-Web.

- **Legacy log collector and Security Director Insights log collector support for event viewer**—Starting in Junos Space 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 read-only log collector support to enable you to view existing data. This support provides a smooth transition from the legacy log collector to the Security Director Insights VM as the log collector.

**NOTE:** You cannot add same type of log collector nodes on the Logging Nodes page.

The Legacy Node check box appears on all the Events & Logs pages after you add the legacy log collector node. Select the Legacy Node check box to view only the existing log collector data. New logs should point to Security Director Insights VM as the log collector. You see the Security Director Insights log collector data after you clear the Legacy Node check box.

- **Polymorphic address support in source and destination address for NAT rules—** Starting in Security Director Release 21.3R1 hot patch V3, while creating NAT rules for group policies you can select polymorphic addresses as source or destination address. The rule points to default address if the device IP address does not match any of the context values in the polymorphic address. If there is a match, the address corresponding to the context value is considered in the source or destination address of the rule.

**NOTE:** Polymorphic address is not supported for static NAT destination address.

- **Support for disabling service offload in Security Director—** Starting in Security Director Release 21.3R1 hot patch V3, we've provided an option to disable service offload on the Edit Profile page of a rule for standard and unified firewall policies. This feature is supported both on logical systems and tenant systems. You can select from the following options:
  - **None:** Select to delete the configured service on the device.
  - **Enable:** Select to enable service offload. When services-offload is enabled, only the first packets of a session go to the Services Processing Unit (SPU), rest of packets in services-offload mode does not go to SPU, therefore some security features such as stateful screen are not supported. Only TCP and UDP packets can be services offloaded.
  - **Disable:** Select to disable service offload.
- **Support to terminate CLI/J-Web edit mode user session—** Starting in Security Director Release 21.3R1 hot patch V3, when you retry the update job on failed devices caused due to device lock failures, you can log the user (edit mode user) out who locked the configuration database, from the device CLI.

Navigate to **Monitor > Job Management**. Select the job, and then from the More list select **Retry on Failed Devices**. On the Retry Update Failed Devices page, enable **Evict CLI/J-Web edit mode users** option.

## Known Issues in Hot Patches

This section lists the known issue in Security Director Release 21.3R1 hot patch.

- The report for the root device event displays Logical System (LSYS) and Tenant System (TSYS) events instead of root device events. [PR1712069](#)

## Resolved Issues in Hot Patches

lists the resolved issues in Security Director Release 21.3R1 hot patches.

**Table 6: Resolved Issues in Hot Patches**

PR	Description	Hot Patch Version
<a href="#">PR1751227</a>	Security director is unable to get the policy hit count using the rest API.	v13
<a href="#">PR1765982</a>	Security Director API fails to prevent creation of duplicate addresses.	v13
<a href="#">PR1754290</a>	VPN publishing jobs fail.	v13
<a href="#">PR1760414</a>	When you perform GET request for <code>/api/juniper/sd/policy-management/firewall/policies/detailedPolicy/{Policy-ID}</code> for a device having LSYS, it shows 500 internal server error.	v13
<a href="#">PR1762610</a>	The <b>Service</b> search functionality in Security Director fails to obtain the required result.	v13

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1728629</a>	User is unable to sort the columns on the <b>Logging Devices</b> page in Security Director.	v12
<a href="#">PR1748252</a>	Unable to import firewall rule in Security Director if the rule has DAG with missing category.	v12
<a href="#">PR1681255</a>	After upgrading to Security Director Release 21.3R1, the user is unable to add a device to the VPN profile.	v12
<a href="#">PR1744649</a>	Security Director displays the device names instead of device IPs under the <b>Device IP</b> column on the <b>Logging Devices</b> page.	v12
<a href="#">PR1653054</a>	The Auto Policy Sync in Security Director does not work.	v11
<a href="#">PR1659212</a>	The service search by port number does not work.	v11
<a href="#">PR1698920</a>	Security Director shows invalid configuration in the update configuration preview.	v11
<a href="#">PR1613930</a>	The user is unable to edit the Policy-based VPN name or description in Security Director.	v11
<a href="#">PR1681035</a>	There are issues with VPN profiles authentication algorithm after you upgrade Security Director.	v11



Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1683173</a>	When the user configures a new IPsec VPN profile for route-based Hub and Spoke using the manual pre-shared key option, the output is set to multiple security IKE policies instead of only one security IKE policy.	v11
<a href="#">PR1689638</a>	When you view device changes, Security Director displays the Managed status as Device Changed for several devices.	v11
<a href="#">PR1694161</a>	Security Director updates multiple policies even when you select only one policy for update.	v11
<a href="#">PR1736563</a>	Security Director modifies the device setup by adding an additional set of VPN configurations.	v11
<a href="#">PR1653687</a>	Security Director does not display the correct time-zone when you change the time-zone using modify configuration.	v11
<a href="#">PR1689302</a>	Address object import from a CSV file fails.	v11
<a href="#">PR1698572</a>	Security director displays An error occurred while requesting the data error message while importing configuration from SRX4100 device.	v11

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1707744</a>	When you try to preview, publish, or update configuration in Security Director, it fails with an error.	v11
<a href="#">PR1709345</a>	The Maximum Transmission Unit (MTU) is not visible during the edit workflow, when provided as default.	v11
<a href="#">PR1722324</a>	Security Director is unable to import Firewall policy in SRX4200.	v11
<a href="#">PR1723715</a>	Save Comments does not work after upgrade to Security Director 22.3.	v11
<a href="#">PR1731271</a>	Security Director API displays internal server error during policy edit if the policy is locked.	v11
<a href="#">PR1734133</a>	When user performs snapshot rollback policy, Security Director creates a duplicate default IPS policy.	v11
<a href="#">PR1735089</a>	Security Director deletes the configurations for the policy-based VPNs that do not get imported to Security Director.	v11
<a href="#">PR1742002</a>	When you try to preview the changes done to a policy before publishing, it fails with Calculating XML Edit Config error message.	v11

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1723625</a>	User is unable to modify the zone with more than hundred interface units.	v10
<a href="#">PR1728651</a>	User is unable to import the group policies through zip file and snapshot roll back policy feature in Security Director.	v10
<a href="#">PR1664682</a>	Geographical location report shows incorrect data in Security Director.	v10
<a href="#">PR1687371</a>	Security Director deletes device configuration due to SRX DMI schema 22.1R1.10.	v10
<a href="#">PR1709403</a>	Security Director fails to import the policy zip files with more than 20000 rules.	v10
<a href="#">PR1710418</a>	Security Director fails to publish the SRX Series cluster policy with UTM is not available in the device error message.	v10
<a href="#">PR1659212</a>	The search functionality in Security Director does not work properly when you search by port number.	v10
<a href="#">PR1718065</a>	User is unable to search for the policies after publishing the new device configuration.	v10
<a href="#">PR1719283</a>	The <b>Application visibility</b> feature fails with errors.	v10

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1701645</a>	SRX series devices do not show any data in the Intrusion Prevention System (IPS) report with log event <i>IDP_ATTACK_LOG_EVENT_LS</i> .	v9
<a href="#">PR1568417</a>	In Security Director, Security Director Insights shows the log source as 127.0.0.1 for all logs rather than the SRX IP address or the actual source from where the logs are originated.	v8
<a href="#">PR1689483</a>	The search functionality in Security Director does not work for newly created address objects.	v8
<a href="#">PR1700163</a>	User is unable to change the destination address for static NAT rules in Security Director.	v8
<a href="#">PR1705221</a>	Security Director displays the following error message while saving IPS/NAT policy rule: <code>java.lang.NullPointerException</code>	v8
<a href="#">PR1679106</a>	Security Director updates the database with incorrect cyclic service group.	v8
<a href="#">PR1703135</a>	User is unable to search for an object in Security Director even when the objects exist in Shared Objects.	v8

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1701008</a>	When you change the sequence of three or more set of rules in the Security Director, the changed order does not appear correctly after saving the changes.	v7
<a href="#">PR1683144</a>	The search and find usage functionality does not work properly in Security Director.	v7
<a href="#">PR1698840</a>	Update to the LSYS fail at times in Security Director.	v7
<a href="#">PR1676755</a>	Security Director fails to import the security policies with the object address 0.0.0.0/0.	v6
<a href="#">PR1695528</a>	Intrusion Detection and Prevention (IDP) signature continues to install the updates on SRX series devices from IDP files even when the file transfer fails.	v6
<a href="#">PR1662267</a>	The search functionality in Security Director does not work for newly configured rules.	v6
<a href="#">PR1684862</a>	Address objects fails to update properly in Security Director.	v5
<a href="#">PR1638491</a>	The maximum transmission unit (MTU) is set to 1500 by default when the size of MTU is not predefined.	v4

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1665789</a>	In Security Director, the value of security log transport TLS-profile is incorrectly set to NONE.	v4
<a href="#">PR1666574</a>	Security Director alarms fail to show up after upgrading to 22.1R1.	v4
<a href="#">PR1666710</a>	Security Director pushes invalid configurations for IKE gateway fragmentation size.	v4
<a href="#">PR1669804</a>	Automatic firewall policy in Junos Space Network Management Platform wrongly imports firewall policy rules.	v4
<a href="#">PR1672405</a>	Unable to add Security Director Insights under <b>Security Director &gt; Administration &gt; Insight Management &gt; Insights Node</b> .	v4
<a href="#">PR1675551</a>	User is unable to delete files under <b>SD_Device_Config</b> .	v4
<a href="#">PR1669807</a>	During auto policy sync, unused objects are stuck in firewall/NAT policy updates.	v4
<a href="#">PR1665842</a>	User is automatically logged out from Security Director despite activity.	v4
<a href="#">PR1669805</a>	When you update policies, re-synchronize the Security Director with the managed device.	v3

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1666924</a>	When the user rollbacks firewall policy, the associated IPS policy is created with _1 in the policy name.	v3
<a href="#">PR1664637</a>	References do not work for dynamic address objects in Security Director.	v3
<a href="#">PR1662493</a>	Unified Threat Management (UTM) custom categories are deleted from SSL proxy profile whitelist.	v3
<a href="#">PR1660892</a>	Security Director fails to export the filtered search for a rule to .pdf format.	v3
<a href="#">PR1660583</a>	Security Director fails to display the latest device configuration in the preview, and displays the following error message: Statement creation failed.	v3
<a href="#">PR1654639</a>	Search functionality does not work as expected.	v3
<a href="#">PR1654241</a>	Select and save functionalities in Intrusion Prevention System (IPS) policy fails in the firewall rule.	v3
<a href="#">PR1653847</a>	The user is unable to disable Network Address Translation (NAT) policies on devices.	v3
<a href="#">PR1653543</a>	The IPS signature update fails with an error.	v3

Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1655473</a>	The logical system device update fails.	v2
<a href="#">PR1651792</a>	The user is unable to import URL patterns and categories.	v2
<a href="#">PR1650817</a>	There are issues with the VPN delete API call.	v2
<a href="#">PR1655401</a>	The user is unable to delete unused dynamic objects created as a result of import.	v2
<a href="#">PR1647300</a>	When Security Director Insights is unreachable, the status is not displayed on the Logging Node page.	v2
<a href="#">PR1644063</a>	The Security Director Insights log collector does not display logging devices.	v2
<a href="#">PR1656449</a>	Security Director is unreachable when node 2 is the VIP node.	v2
<a href="#">PR1636657</a>	Unable to push license from Security Director in multi node setup.	v1
<a href="#">PR1637747</a>	Security Director deletes the threat Prevention Policy that is added via J-Web or device CLI on root and logical system.	v1



Table 6: Resolved Issues in Hot Patches *(Continued)*

PR	Description	Hot Patch Version
<a href="#">PR1638876</a>	There are auto policy sync job issues.	v1
<a href="#">PR1644157</a>	User is unable to add devices to Juniper Security Director Cloud after on-prem Security Director upgrade.	v1
<a href="#">PR1644238</a>	User is unable to create or modify variable objects in Security Director.	v1
<a href="#">PR1644736</a>	IPsec VPN update fails from Security Director due to incorrect CLI for IKE and IPsec VPN profiles.	v1
<a href="#">PR1644737</a>	Unable to view data on the VPN Monitoring page.	v1
<a href="#">PR1644877</a>	Packet capture functionality does not work as expected.	v1
<a href="#">PR1646550</a>	Update firewall policy fails.	v1
<a href="#">PR1647181</a>	Unable to create polymorphic object in Security Director.	v1
<a href="#">PR1648031</a>	The NAT rule Disable option does not work as expected.	v1
<a href="#">PR1648126</a>	User is unable to view packet capture data for IDP policy.	v1

## Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: <http://prsearch.juniper.net>.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <http://pathfinder.juniper.net/feature-explorer/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

## Revision History

29 December, 2021—Revision 1—Junos Space Security Director Release 21.3R1

1 March, 2022—Revision 2—Junos Space Security Director Release 21.3R1 Hot Patch V1

11 April, 2022—Revision 3—Junos Space Security Director Release 21.3R1 Hot Patch V2

22 June, 2022—Revision 4—Junos Space Security Director Release 21.3R1 Hot Patch V3

16 August, 2022—Revision 5—Junos Space Security Director Release 21.3R1 Hot Patch V4

19 September, 2022—Revision 6—Junos Space Security Director Release 21.3R1 Hot Patch V5

8 November, 2022—Revision 7—Junos Space Security Director Release 21.3R1 Hot Patch V6

7 December, 2022—Revision 8—Junos Space Security Director Release 21.3R1 Hot Patch V7

29 December, 2022—Revision 9—Junos Space Security Director Release 21.3R1 Hot Patch V8

14 February, 2023—Revision 10—Junos Space Security Director Release 21.3R1 Hot Patch V9

20 April, 2023—Revision 11—Junos Space Security Director Release 21.3R1 Hot Patch V10

29 June, 2023—Revision 12—Junos Space Security Director Release 21.3R1 Hot Patch V11

14 August, 2023—Revision 13—Junos Space Security Director Release 21.3R1 Hot Patch V12

21 December, 2023—Revision 14—Junos Space Security Director Release 21.3R1 Hot Patch V13

---

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.