

# Release Notes: Junos Space Security Director Release 21.2R1

1 June 2022  
Revision 4

<b>Contents</b>	<b>Introduction   3</b>
	<b>Release Notes for Junos Space Security Director   3</b>
	<b>New and Changed Features   4</b>
	<b>Supported Managed Devices   5</b>
	<b>Supported Log Collection Systems   6</b>
	<b>Supported Junos OS Releases   6</b>
	<b>Supported Policy Enforcer and Juniper® Advanced Threat Prevention (ATP) Cloud         Releases   8</b>
	<b>Supported Browsers   9</b>
	<b>Installation and Upgrade Instructions   10</b>
	<b>Installing and Upgrading Security Director Release 21.2R1   10</b>
	<b>Loading Junos OS Schema for SRX Series Devices   10</b>
	<b>DMI Schema Compatibility for Junos OS Service Releases   10</b>
	<b>Management Scalability   13</b>
	<b>Known Behavior   13</b>
	<b>Known Issues   16</b>
	<b>Resolved Issues   17</b>
	<b>Hot Patch Releases   18</b>
	<b>Installation Instructions   19</b>
	<b>Resolved Issues in the Hot Patches   19</b>
	<b>Finding More Information   21</b>
	<b>Documentation Feedback   21</b>

Requesting Technical Support | 22

Self-Help Online Tools and Resources | 22

Creating a Service Request with JTAC | 23

Revision History | 23

# Introduction

The Junos Space<sup>®</sup> 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.

## Release Notes for Junos Space Security Director

### IN THIS SECTION

- [New and Changed Features | 4](#)
- [Supported Managed Devices | 5](#)
- [Supported Log Collection Systems | 6](#)
- [Supported Junos OS Releases | 6](#)
- [Supported Policy Enforcer and Juniper<sup>®</sup> Advanced Threat Prevention \(ATP\) Cloud Releases | 8](#)
- [Supported Browsers | 9](#)
- [Installation and Upgrade Instructions | 10](#)
- [Loading Junos OS Schema for SRX Series Devices | 10](#)
- [DMI Schema Compatibility for Junos OS Service Releases | 10](#)
- [Management Scalability | 13](#)
- [Known Behavior | 13](#)
- [Known Issues | 16](#)
- [Resolved Issues | 17](#)
- [Hot Patch Releases | 18](#)

## New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director and Policy Enforcer Release 21.2R1.

- **Support for tenant systems**—Starting in Security Director Release 21.2R1, we provide support for tenant systems. When you discover a device in Security Director, you can:
  - View the details of the tenant system that the user created on the root device.
  - Create a tenant system in Security Director.

Tenant system is supported on devices running Junos OS Release 18.3 and later for SRX Series devices and Junos OS Release 20.1 and later for vSRX Series devices.

**NOTE:** When there is a job failure in Security Director, you can discard the uncommitted changes on the root device from Junos Space<sup>®</sup> Network Management Platform. Navigate to **Devices > Device Management > Modify Configuration** and then click **Deploy** and delete the configuration changes.

- **Threat profiling**—Starting in Security Director Release 21.2R1, you can configure a firewall policy with source and destination feed as threat types. The policy then injects the source IP feed and destination IP feed into the selected threat type when traffic matches the rule. Other devices can also leverage the threat feed as a dynamic address group.
- **IPS policy enhancements**—Starting in Security Director Release 21.2R1, while creating a firewall policy rule, you can configure an IPS Policy value irrespective of IPS value (On or Off).
  - In Junos OS Release 18.1 and earlier, if you configure a policy with both IPS as On or Off and an IPS policy, Security Director ignores the IPS policy and sends only the IPS On CLI command to the device.
  - In Junos OS Release 18.2 and later, if you configure a policy with both IPS as On or Off and an IPS policy, Security Director ignores the IPS On CLI and sends only the IPS policy CLI command to device.
- **Log Collector 21.2 (Security Director Insights VM)**—Starting in Security Director Release 21.2R1, you must use Security Director Insights VM as the Log Collector. For details, see [Security Director Installation and Upgrade Guide](#).
- **Inclusion and Diversity changes**—Starting in Security Director Release 21.2R1, we've implemented the Inclusion and Diversity language changes in the GUI.
- **Purge feature**—Starting in Policy Enforcer Release 21.2R1, we provide support to purge the feeds which are older than a specified number of days.

## Supported Managed Devices

Security Director Release 21.2R1 manages 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 21.2 (Security Director Insights VM)
- Integrated Log Collector 20.1R1
- Juniper Networks<sup>®</sup> 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 21.2R1 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
- 19.2R3.5
- 19.3
- 19.4
- 19.4R3.11
- 20.1R1.11
- 20.2R2.11
- 20.3R1.8
- 20.4
- 21.1R1
- 21.2R1

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<sup>®</sup> Advanced Threat Prevention (ATP) Cloud Releases

Table 1 on page 8 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
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



**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)
19.2R1	19.2R1	Junos OS Release 15.1X49-D120 and later
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

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

## Supported Browsers

Security Director Release 21.2R1 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 21.2R1](#) | 10

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

### Installing and Upgrading Security Director Release 21.2R1

Junos Space Security Director Release 21.2R1 is supported only on Junos Space Network Management Platform Release 21.2R1 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

#### NOTE:

For more information about installing and upgrading Security Director and Log Collector Release 21.2R1, 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 11](#).

**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.

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
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 11](#).

**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 12](#).

**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.

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
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 12](#).

**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 21.2R1.

- 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 21.2R1.

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

- 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. [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 and Policy Enforcer Release 21.2R1:

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

- Column filter does not work for source address with IP address and address object. [PR1570439](#)
- Security Director deletes all address books and applications during the publish preview. [PR1571801](#)
- Service object search does not work as expected. [PR1573475](#)
- The user is unable to enter fully qualified domain name (FQDN) in the hostname field of extranet devices. [PR1579535](#)
- Security Director API does not return the service object if the user does not select the same domain. [PR1579808](#)
- The user is unable to switch between domains. [PR1581109](#)
- When the user updates the policy on the device, the rules are deleted incorrectly. [PR1581760](#)
- Policy hit-count does not work as expected. [PR1584206](#)
- IKE and IPsec proposal name get modified after you change the routing topology in the VPN profile. [PR1585730](#)
- Policy hit-count does not work as expected. [PR1586274](#)
- IPv6 search does not work in Security Director. [PR1586900](#)
- Commit check job fails in Security Director. [PR1590596](#)
- While user creates address objects, Security Director REST API allows invalid entries. [PR1592806](#)
- The user is unable to upload the IDP signature file. [PR1593312](#)
- Update fails when Security Director tries to set address-set (range) and address with the same name. [PR1593706](#)
- Search does not work in Security Director installed using the QCOW2 image on a KVM. [PR1594473](#)
- The user is unable to import the variables CSV file into Security Director. [PR1594864](#)

- Security Director sends additional unified threat management (UTM) commands after the user upgrades the firewall from Junos OS Release 15.x to a later version. [PR1597074](#)
- There are issues with IPsec VPN extranet device IP deployment. [PR1597978](#)
- The user is unable to change interface binding for IPsec VPN. [PR1598301](#)
- The configure Rules Sets option does not show all the rules. [PR1599595](#)
- There is an error when user updates the VPN on a device. [PR1579779](#)
- Device update job fails in Security Director. [PR1585013](#)
- There is disk space issue on Policy Enforcer. [PR1513703](#)
- The user is unable to add Policy Enforcer after restoring Junos Space Network Management Platform. [PR1588186](#)

## Hot Patch Releases

This section describes the installation procedure, features, and resolved issues in Junos Space Security Director Release 21.2R1 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 21.2R1 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

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

1. Download the Security Director 21.2R1 Patch vX from the [download site](#).

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

2. Copy the **SD21.2R1-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-21.2R1-hotpatch-vX.tgz.
```

4. Extract the **SD-21.2R1-hotpatch-vX.tgz** file:

```
tar -zxvf SD21.2R1-hotpatch-vX.tgz
```

5. Change the directory to **SD21.2R1-hotpatch-vX**.

```
cd SD-21.2R1-hotpatch-vX
```

6. Execute the **patchme.sh** script from the **SD-21.2R1-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/.SD21.2R1-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.

## Resolved Issues in the Hot Patches

[Table 6 on page 20](#) lists the resolved issues in Security Director Release 21.2R1 hot patches.

**NOTE:** Log4j vulnerabilities are addressed in the Junos Space Security Director Release 21.2R1 V2 hot patch.

Table 6: Resolved Issues in Hot Patches

PR	Description	Hot Patch Version
<a href="#">PR1653543</a>	The Intrusion Prevention System (IPS) signature update fails with an error.	V3
<a href="#">PR1665789</a>	Deployment of SRX series device fails because Security Director sets TLS profile value as “none”.	V3
<a href="#">PR1626403</a>	Logging devices do not show Security Director Insights information.	V3
<a href="#">PR1649267</a>	The firewall policy update fails on the SRX Series device.	V3
<a href="#">PR1651838</a>	Incorrect fabric and control link status are shown for logical systems.	V3
<a href="#">PR1655401</a>	The user is unable to delete unused dynamic objects created as a result of import.	V3
<a href="#">PR1655473</a>	The logical system device update fails.	V3
<a href="#">PR1656449</a>	Security Director is unreachable when node 2 is the VIP node.	V3
<a href="#">PR1652573</a>	The user is unable to edit the logical interfaces of devices through Security Director.	V3
<a href="#">PR1664941</a>	Security Director API call fails for NAT policies with 300 rules.	V3
<a href="#">PR1623570</a>	Security Director does not import addresses from a CSV file.	V2
<a href="#">PR1628535</a>	The import of NAT policy with the compressed IPv6 format fails.	V2
<a href="#">PR1623265</a>	The address object import from a CSV file fails.	V2
<a href="#">PR1636132</a>	There is an issue with search operation for multiple IPs in firewall rules.	V2
<a href="#">PR1502587</a>	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. Security Director does not use AppTrack logs, instead it retrieves the data from RT_FLOW_SESSION logs.	V1

**NOTE:** If the hot patch contains a UI fix, then you must clear the Web browser's cache to reflect the latest changes.

## 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>.

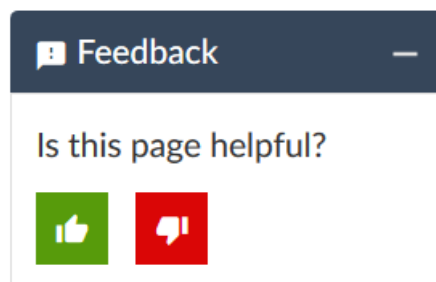
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable).

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:  
<https://entitlementsearch.juniper.net/entitlementsearch/>

## Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see  
<https://support.juniper.net/support/requesting-support/>.

## Revision History

27 July 2021—Revision 1—Junos Space Security Director Release 21.2R1

29 September 2021—Revision 2—Junos Space Security Director Hot Patch Release 21.2R1 V1

10 January 2022—Revision 3—Junos Space Security Director Hot Patch Release 21.2R1 V2

1 June 2022—Revision 4—Junos Space Security Director Hot Patch Release 21.2R1 V3

Copyright © 2023 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.