

# Release Notes: Junos Space Security Director Release 20.1R1

13 January 2022  
Revision 6

<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   6</b>
	<b>Supported Line Cards   7</b>
	<b>Supported Junos OS Releases   8</b>
	<b>Supported Policy Enforcer and Juniper Sky ATP Releases   9</b>
	<b>Supported Browsers   10</b>
	<b>Installation and Upgrade Instructions   10</b>
	<b>Installing and Upgrading Security Director Release 20.1R1   11</b>
	<b>Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later   11</b>
	<b>Loading Junos OS Schema for SRX Series Devices   12</b>
	<b>DMI Schema Compatibility for Junos OS Service Releases   12</b>
	<b>Management Scalability   14</b>
	<b>Known Behavior   15</b>
	<b>Known Issues   18</b>
	<b>Resolved Issues   19</b>
	<b>Hot Patch Releases   21</b>
	<b>Installation Instructions   22</b>
	<b>Supported Junos OS Releases   23</b>
	<b>New and Enhanced Features in the Hot Patch   23</b>
	<b>Resolved Issues in the Hot Patches   23</b>

Finding More Information | 28

Documentation Feedback | 29

Requesting Technical Support | 29

Self-Help Online Tools and Resources | 30

Creating a Service Request with JTAC | 30

Revision History | 30

# 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, Network Address Translation (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 | 6](#)
- [Supported Line Cards | 7](#)
- [Supported Junos OS Releases | 8](#)
- [Supported Policy Enforcer and Juniper Sky ATP Releases | 9](#)
- [Supported Browsers | 10](#)
- [Installation and Upgrade Instructions | 10](#)
- [Loading Junos OS Schema for SRX Series Devices | 12](#)
- [DMI Schema Compatibility for Junos OS Service Releases | 12](#)
- [Management Scalability | 14](#)
- [Known Behavior | 15](#)
- [Known Issues | 18](#)
- [Resolved Issues | 19](#)
- [Hot Patch Releases | 21](#)

## New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director and Policy Enforcer Release 20.1R1.

- **Enhancements in IPsec VPN**—Starting in Junos Space Security Director Release 20.1R1, we've updated the UI options for creating an IPsec VPN. You can view the representations of different VPN topologies. You must click on the icons to configure site to site, hub and spoke, and full mesh topologies.
- **Enhancements in license management**—We've made the following enhancements to license management:
  - You can find the license details under **Devices > Licenses**.
  - You can deploy the license on cluster and chassis devices.
  - After you install the license on a device, the Licenses page is automatically refreshed.
  - You can choose to run a job immediately or schedule the job to run later by using the Schedule Start Time option on the License Schedule Polling page.
- **New IPS policy templates**—We provide predefined policy templates that you can use as a guideline to create policies. Each template contains a set of rules of a specific rule base type. Starting in Junos Space Security Director Release 20.1R1, all the 14 existing predefined IPS policy templates are replaced with 6 new templates, namely, Default, Recommended, Recommended-Client-Protections, Recommended-Enhanced, Recommended-Sever-Protections, and Strict. You can use these predefined IPS policy templates or create custom templates. You can also edit and clone the templates. If your existing templates are associated with IPS policies, then those templates will act as custom rules in Security Director.
- **Synchronize out-of-band changes for NAT policy**—Starting in Junos Space Security Director Release 20.1R1, you can synchronize (that is, import or reject) out-of-band changes for a NAT policy from a device to Security Director manually or automatically. Automatic synchronization is applicable for a device-specific policy, and manual synchronization is applicable for both device-specific and group policies.
- **Additional parameters to manage SRX Series devices**—Starting in Junos Space Security Director Release 20.1R1, you can configure additional device parameters to effectively manage an SRX Series device. We've added SSL Initiation Profile, ICAP Redirect Profile, and Link Aggregation (LAG) Profile sections.
- **IPS policy support for logical system**—Starting in Junos Space Security Director Release 20.1R1, you can use an IPS policy to selectively enforce various attack detection and prevention techniques on network traffic passing through a logical system.  
 Devices running Junos OS Release 18.3 and later support IPS policies for logical system.
- **Convert traditional firewall policies with application firewall to unified firewall policies**—Starting in Junos Space Security Director Release 20.1R1, you can convert a standard policy with application firewall configuration to a unified firewall policy.

- **Enhancements in IPS signature dynamic groups**—Starting in Junos Space Security Director Release 20.1R1, you can configure additional dynamic attack group parameters to create more effective IPS signature dynamic groups. We've added parameters such as CVSS-score, age of attack, file type, and vulnerability type.
- **Competitive reports**—Starting in Junos Space Security Director Release 20.1R1, we've added the predefined URLs Visited Per User report, which displays statistics related to a specific user. You can generate the report using the Run now option, preview the report as PDF, or send the report over an e-mail. You can choose to have a complete record or top ten records for a user. The report displays various statistics for users such as top URLs by session, top high risk URLs visited, total bandwidth used by high risk URL categories, breakdown of URL categories visited, total session used on risky URLs, and so on.
- **Configure parameters for DNS host type**—Starting in Junos Space Security Director Release 20.1R1, you can configure DNS name and DNS type (either IPv4 or IPv6) while creating addresses and address groups with DNS host type.
- **Export service objects to CSV file**—Starting in Junos Space Security Director Release 20.1R1, you can export service objects to a CSV file.
- **Configure parameters to delete unused address objects**—When a device is updated from Security Director, if you want the unused addresses and address groups or NAT pools to be deleted from the device, go to Junos Space Network Management Platform, select **Administration > Application > Modify Application Settings > Update Device**, and select the corresponding **Delete unused addresses and address groups** or **Delete unused NAT pool** check box.
- **Download the Signature Database for vSRX 3.0**—Starting in Junos Space Security Director Release 20.1R1, you can download the Signature Database for vSRX 3.0. The detectors and other signature files specific to vSRX 3.0 in the Security Director database can be pushed to vSRX 3.0 devices.
- **Enhancements in search and filter for advanced security option**—Starting in Junos Space Security Director Release 20.1R1, under the Advanced Security option in firewall policy, you can search and filter policies with IPS On or Off values.
- **Predefined application or services**—Starting in Junos Space Security Director Release 20.1R1, the new set of predefined application or services supported in Junos are added in the Security Director database during installation.
- **TCP-session options**—Starting in Junos Space Security Director Release 20.1R1, you can configure Initial TCP MSS and Reverse TCP MSS options while configuring a firewall policy profile.
- **LSYS and VRF instance support**—Starting in Policy Enforcer Release 20.1R1, you can create a tenant representing an enterprise. On an MX Series device, you can assign a Virtual Routing and Forwarding (VRF) instance to a tenant. The custom feed sends feeds to Policy Enforcer at the logical system (LSYS) and VRF instance levels on the MX Series device. The VRF instance is dedicated to handling traffic within the tenant's private network. You can route the traffic on the tenant's private network from the VRF instance on the MX Series device at one site to the same VRF instance on another MX Series device at

a different site. The MX Series device supports multiple VRF instances, which can be assigned to different tenants. Therefore, a device can be shared with multiple tenants.

**NOTE:**

- In Policy Enforcer Release 20.1R1, only MX Series devices support LSYS and VRF.
- Only root logical system is supported.
- All the sites of a realm are either with tenants or without tenants.
- VRF based feeds such as C&C, allowlist, and blocklist are supported through custom feeds.
- Custom C&C feed (not VRF-based) is supported on SRX Series devices in all modes except the default mode.

- **vSRX 3.0 support**—Policy Enforcer Release 20.1R1 supports vSRX 3.0 running with Junos OS Release 19.4R1 and later.

## Supported Managed Devices

Security Director Release 20.1R1 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

The following log collection systems are supported:

- Security Director Log Collector
- Juniper Secure Analytics (JSA) as Log Collector on JSA Release 2014.8.R4 and later
- QRadar as Log Collector on QRadar Release 7.2.8 and later

## Supported Line Cards

[Table 1 on page 8](#) shows the supported Juniper Networks line cards in Junos Space Security Director Release 20.1R1.

**Table 1: Supported Line Cards**

Device	Line Cards
SRX5800	<ul style="list-style-type: none"> <li>• SRX5K IOC4</li> <li>• SRX5K RE3</li> <li>• SRX5K SCB4</li> </ul>
SRX320	SRX-MP-WLAN-WW

## Supported Junos OS Releases

Security Director Release 20.1R1 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
- 18.2
- 18.3
- 18.4
- 19.1
- 19.2



- 19.3
- 19.4

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 Sky ATP Releases

Table 2 on page 9 shows the supported Policy Enforcer and Juniper Sky Advanced Threat Prevention (Juniper Sky ATP) releases.

**Table 2: Supported Policy Enforcer and Juniper Sky ATP Releases**

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper Sky ATP-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

Table 2: Supported Policy Enforcer and Juniper Sky ATP Releases (*continued*)

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper Sky ATP-supported Devices)
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
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

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

## Supported Browsers

Security Director Release 20.1R1 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 20.1R1 | 11](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later | 11](#)

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

## Installing and Upgrading Security Director Release 20.1R1

Junos Space Security Director Release 20.1R1 is supported only on Junos Space Network Management Platform Release 20.1R1 that can run on the following devices:

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

In Junos Space Security Director Release 20.1R1, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. All three applications are installed when you install the Security Director Release 20.1R1 image.

**NOTE:** Starting in Junos Space Security Director Release 17.2R1 onward, Log Collector version information is stored in the `/etc/juniper-release` file on Log Collector. In previous Junos Space Security Director releases, Log Collector version information is stored in the `/etc/redhat-release` file on Log Collector.

**NOTE:** An integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 events per second (eps).

For more information about installing and upgrading Security Director Release 20.1R1, see [Security Director Installation and Upgrade Guide](#).

## Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later

For distributed Log Collector deployment, you must add only a Log Receiver node. You can add the node directly to Security Director using admin credentials, as in the case of the JSA node. For security reasons, non-root credentials are used to add a node.



**CAUTION:** For Security Director Log Collector, provide the default credentials: username is admin and password is juniper123. You must change the default password by using the Log Collector CLI command `configureNode.sh` as shown in [Figure 1 on page 12](#).

Figure 1: Change Password

```
[root@LOG-COLLECTOR ~]# sh configureNode.sh
#####

Please enter your choice:
1) Configure IP Address
2) Configure Time Zone
3) Configure Name Server Settings
4) Configure NTP Settings
5) Configure eMail Settings for event notification
6) Update Log Collector database password
7) Quit

Please enter your choice: 6

Updating Log Collector database password

Please Enter New Password for db(elasticsearch) user, admin :
```

For JSA, provide the admin credentials that are used to log in to the JSA console.

For information about how to add the Log Collector node to Security Director, 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 3 on page 13](#).

**Table 3: 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 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 default DMI schema version, as shown in [Table 4 on page 13](#).

**Table 4: 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	18.3R1.1 18.2R1.1	18.2R1.1	18.2R1.1

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 5 on page 13](#).

**Table 5: 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 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 a default DMI schema version, as shown in [Table 6 on page 14](#).

Table 6: 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	18.3R1.1 18.2R1.1	18.2R1.1	18.2R1.1

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 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.

Table 7 on page 15 shows the supported firewall rules per policy that are processed concurrently.

Table 7: Supported Firewall Rules per Policy

Number of Device Rules Processed Concurrently	JBoss Node Count	Memory	Platform OpenNMS Function	Log Collector	Hard Disk
5,000–7,000	1	64 GB of RAM	Enabled	Dedicated node	Any
15,000	1	64 GB of RAM	Off or dedicated node	Dedicated node	Any
40,000	2	64 GB of RAM per node	Off or dedicated node	Dedicated node	Any
100,000	2	64 GB of RAM per node	Off or dedicated node	Dedicated node	SSD required

**NOTE:** If you use a database dedicated setup (SSD hard disk VMs) for the deployment mentioned in [Table 7 on page 15](#), 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 20.1R1.

- In Junos Space Security Director Release 20.1R1, you must configure tunnel IP address for dynamic routing protocols. In Junos Space Security Director Release 19.4R1 and earlier, if you have configured VPN as unnumbered with dynamic routing protocol, you will be prompted to provide tunnel IP address while editing the VPN after upgrading to Junos Space Security Director Release 20.1R1.
- After upgrade you will not be allowed to edit profiles with predefined proposals because profiles in Junos Space Security Director Release 20.1R1 supports only custom proposals.
- In Junos Space Security Director Release 19.4R1 and earlier, if you have configured VPN with static routing or traffic selector with protected network as zone or interface, perform the following:
  1. Before you upgrade, update the configuration to device, and delete the VPN Policy from Security Director.
  2. After you upgrade to Junos Space Security Director Release 20.1R1, you must import the VPN configuration.

**NOTE:** In Junos Space Security Director Release 20.1R1, only address objects is supported in protected networks for static routing and traffic selector.

- In Junos Space Security Director Release 19.4R1 and earlier, if you have configured route settings as None, Security Director does not allow you to edit the VPN after you upgrade to Junos Space Security Director Release 20.1R1. This is because , you must select one of the routing protocols for creating a VPN in Junos Space Security Director Release 20.1R1.
- You must disable OpenNMS before installing the integrated Log Collector.

To disable OpenNMS:

1. Select **Network Management Platform > Administration > Applications**.
2. Right-click **Network Management Platform**, and select **Manage Services**.
3. Select **Network Monitoring**, and click the Stop Service icon.

The network monitoring service is stopped, and the status of OpenNMS is changed to Disabled.

**NOTE:** You must ensure that Junos Space Network Management Platform and Security Director are already installed on a JA2500 appliance or Junos Space virtual appliance.

- The **Enable preview and import device change** option is disabled by default.

To enable this option:

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 19.4R1 and Policy Enforcer Release 19.4R1, you must migrate the existing vSRX VMs in NSX Manager from Policy Enforcer Release 17.1R1 to Release 19.4R1.

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 via CSV, a new address object is created by appending **a\_1** to the address object name if the address object is already present in Security Director.

## Known Issues

This section lists the known issues in Security Director Release 20.1R1.

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

- Security Director generates incomplete CLIs for dynamic attack group "vendor\_description", which causes update failure. [PR1502196](#)
- For dynamic attack groups (false positive and performance impact), incorrect CLIs are generated due to the mismatch in the UI options with respect to the device options. [PR1513528](#)
- Security Director deletes only one VPN at a time, though UI allows to delete multiple VPNs of the same device in a single delete attempt. [PR1508265](#)

Workaround: Delete single VPN at a time and update one after the other.

- 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.

Workaround: Clear the out-of-band icon on the policies when changes are not made on the device. Navigate to corresponding policy and right-click the policy. Select **View Device Policy Changes** and reject all changes, and then click **OK**. [PR1484953](#)

- Cipher list CLIs deploy works only when you perform "save" or "save and deploy".

Workaround: You must save or deploy the selected Cipher list before viewing the preview changes. [PR1485949](#)

- An object conflict occurs while you are importing 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.

- Security Director does not support routing instances and proxy profiles in an antivirus pattern update for the UTM default configuration. [PR1462331](#)
- When out-of-band changes are imported to a logical system (LSYS) device, a job is created for the root device along with the LSYS device, although changes are made only in the LSYS 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](#)
- Junos Space Security Director fails to import VPN if a device uses master password encryption because VPN preshared key with \$8\$ format is not supported. [PR1416285](#)

- Junos Space Security Director generates wrong CLI commands for deleting advanced policy-based routing (APBR) rules. [PR1417708](#)
- 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 single node does not recover system issue only present on 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 20.1R1.

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

- When you import multiple devices with default IPS policies simultaneously, only one default IPS policy is imported. The default IPS policies of other devices are not imported. [PR1470335](#)
- Unified IPS support for a logical system (LSYS) device is not provided. [PR1465554](#)
- The newly created first rule of a rule group always moves to the previous rule group when out-of-band changes are imported. [PR1451550](#)
- Security Director does not push the correct detector version or signature database for vSRX 3.0. [PR1468161](#)
- An unexpected behavior is seen when you enable the Policy Sync Settings option. [PR1472215](#)
- Logs from JSA to Security Director show wrong subdomain. [PR1472468](#)
- When an SRX Series cluster fails over, Security Director device updates fail. [PR1479795](#)
- There is inconsistency in grid view of application visibility data. [PR1479934](#)
- VPN is not up as Security Director does not generate unique IKE policy. [PR1480647](#)
- Search does not work for user IDs in security policies. [PR1483279](#)
- Security Director does not push the pre-shared key (PSK) to the VPNs because the PSKs are encrypted twice. [PR1484611](#)
- Device-related jobs on Security Director fail. [PR1485485](#)
- Users are unable to export the filtered PDF. [PR1485780](#)

- Multiple IKE policy pre-shared-key statements are pushed to the firewall. [PR1486055](#)
- After you configure a VPN, the traffic selector information does not get saved. [PR1486200](#)
- Transaction rolled back for device update job. [PR1486311](#)
- Search does not work for objects in the firewall, IPS, or NAT policies. [PR1486740](#)
- The policy sync job fails. [PR1487675](#)
- The pre-shared keys for the VPNs in Security Director do not get updated on the devices correctly. [PR1488781](#)
- VPN edit generates delete CLI, which causes update failure from Security Director. [PR1488858](#)
- IPS signature installation fails from Junos Space on a vSRX instance installed on KVM. [PR1490851](#)
- When a rule is cloned in firewall policies, the cloned rule does not contain the tunnel information. [PR1490998](#)
- You cannot create a usable custom role name to be used in the source-identity field of the policy. [PR1491008](#)
- Data is not displayed in the application-related widgets when a specific device is selected. [PR1492280](#)
- The Select services drop-down in IPS policy does not list the objects. [PR1492512](#)
- The publish and update jobs do not respond. [PR1492932](#)
- Security Director is unable to export the filtered search results for a rule to PDF. [PR1493016](#)
- Unable to change the name of the IPS policy for an SRX Series device. [PR1493326](#)
- When you run a publish or update job from Security Director, an error message is displayed. [PR1493795](#)
- After you upgrade Junos Space Security Director, an error message is seen in the global policy rules. [PR1494500](#)
- IPv6 address object search does not work as expected. [PR1496012](#)
- Security Director sends license expiry e-mails to the users for all the devices. [PR1497220](#)
- While creating an application or service object, a warning message is displayed for the source port. [PR1497931](#)
- Unable to push license to an SRX Series cluster device. [PR1497963](#)
- If the VPN name exceeds 32 characters in the device end point settings, Security Director fails to truncate the VPN name. [PR1499371](#)
- Search does not work as expected. [PR1499379](#)
- Security Director cannot search for a shared object in the address object list from a sub domain though it has access to the objects from the parent domain. [PR1499409](#)
- There is an issue with address object replacement. [PR1500407](#)

- Policy update fails when the same IDP or IPS policy is assigned to group device policies or device-specific policies for two or more devices. [PR1501723](#)
- After an upgrade, the UTM policy configuration lines for traffic-options are deleted. [PR1509739](#)
- Applications are not seen on the Application Visibility page after upgrade. [PR1438931](#)
- Search fails for service objects in IPS policy. [PR1469745](#)
- Random digits are appended to the VPN name. [PR1475408](#)
- Security Director dashboard widgets fail to load data whenever a specific device is selected. [PR1478355](#)
- Routing-instance does not bind to an interface while creating or editing a VPN. [PR1478948](#)
- User is unable to import device configuration. LSYS device discovery status shows Fab Link and Control Link are down. [PR1480360](#)
- VPN takes longer to publish. [PR1490718](#)
- Firewall policy export fails. [PR1490951](#)
- VPN tunnel creation pushes incomplete configuration for the interfaces. [PR1493192](#)
- Hostname, log source, and policy name shows N/A in the events for all domains. [PR1494356](#)
- Disabling monitoring for a device does not stop polling the device. [PR1506356](#)
- If Policy Enforcer is upgraded to any release later than Policy Enforcer Release 17.1R2, the custom feeds dynamic address group (DAG) user interface does not list all the DAGs created before Policy Enforcer Release 17.2R2. [PR1425871](#)

## Hot Patch Releases

This section describes the installation procedure, features, and resolved issues in Junos Space Security Director Release 20.1R1 hot patches.

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 20.1R1.103 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 20.1R1 Patch vX from the [download site](#).

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

2. Copy the **SD-20.1R1-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-20.1R1-hotpatch-vX.tgz.
```

4. Extract the **SD-20.1R1-hotpatch-vX.tgz** file:

```
tar -zxvf SD-20.1R1-hotpatch-vX.tgz
```

5. Change the directory to **SD-20.1R1-hotpatch-vX**.

```
cd SD-20.1R1-hotpatch-vX
```

6. Execute the **patchme.sh** script from the **SD-20.1R1-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-20.1R1-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.

## Supported Junos OS Releases

Junos Space Security Director Release 20.1R1 V1 and later hot patches support the following Junos OS releases:

- 20.1
- 20.2

## New and Enhanced Features in the Hot Patch

Junos Space Security Director Release 20.1R1 hot patch includes the following new features and enhancements:

- URL category support—Now, you can select URL categories while adding and editing rules in standard and unified firewall policies.
- Firewall policy enhancements—We've made the following enhancements:
  - You can convert a standard firewall policy (with devices assigned) to a unified policy. If any of the devices is running Junos OS version earlier than 18.2, conversion fails. You'll need to unassign the device to proceed with the conversion. Before unassigning the device, if required, you can clone the policy then convert the original standard firewall policy to unified policy.
  - You can convert firewall rules with IPS ON from standard firewall policy to unified firewall policy. After conversion, IPS ON is retained in the unified firewall rules. To use the IPS configurations in the device, you must configure IPS policy for the corresponding unified firewall rule with IPS ON in the Advanced Security column. The deprecated active IPS policy and IPS configurations are deleted on subsequent updates.
- Logical system support—Starting in Junos Space Security Director Release 20.1R1 V2 hot patch, we've provided support for logical systems in the Threat Prevention policy. It is supported on devices running Junos OS Release 18.4 and later.
- Support for deprecated CLIs—Deprecated CLIs for application firewall and IPS policies were not supported in Security Director. Starting in Junos Space Security Director Release 20.1R1 V2 hot patch, we've provided support for deprecated application firewall CLIs in devices running Junos OS Release 18.2 and later.

## Resolved Issues in the Hot Patches

[Table 8 on page 24](#) lists the resolved issues in Security Director Release 20.1R1 hot patches.

**NOTE:** Log4j vulnerabilities are addressed in the Junos Space Security Director Release 20.1R1 V4 hot patch.

**Table 8: Resolved Issues in Hot Patches**

PR	Description	Hot Patch Version
<a href="#">PR1593312</a>	Junos Space Network Management Platform is unable to upload offline signature database.	V4
<a href="#">PR1605902</a>	Data is not displayed on Application Visibility, User Visibility, and Source IP Visibility pages in Security Director.	V4
<a href="#">PR1518097</a>	When user selects a time-period such as 5m, 10m, 15m, and so on, events data is not populated and displays that the data is not available.	V3
<a href="#">PR1478921</a>	Performance issues are observed in Security Director.	V3
<a href="#">PR1508560</a>	There is an issue while calculating rules to publish when attempting to update through change management.	V3
<a href="#">PR1531343</a>	When you add an interface to a routing-instance, Security Director deletes the entire configuration and tries to reset the configuration.	V3
<a href="#">PR1533072</a>	Search option does not work as expected.	V3
<a href="#">PR1516089</a>	Security Director displays incorrect search results.	V3
<a href="#">PR1536398</a>	Policy rules filter does not work.	V3
<a href="#">PR1537434</a>	Firewall policy API calls do not work as expected.	V3
<a href="#">PR1537191</a>	VPN and NAT policies fail during update to the device.	V3
<a href="#">PR1543039</a>	There is an issue with the number of VPN profiles listed in the drop-down list.	V3
<a href="#">PR1533391</a>	Rule created in Security Director does not save position.	V3
<a href="#">PR1497932</a>	Security Director does not use Web proxy when configured in Junos Space Network Management Platform.	V3



Table 8: Resolved Issues in Hot Patches (*continued*)

PR	Description	Hot Patch Version
<a href="#">PR1552582</a>	User is unable to export events to CSV file.	V3
<a href="#">PR1548385</a>	Search objects and devices do not display the result.	V3
<a href="#">PR1545743</a>	Rule search or filtering does not work in Security Director.	V3
<a href="#">PR1555170</a>	Custom URL-pattern with special character is not updated as expected.	V3
<a href="#">PR1555848</a>	Import fails from SRX Series device after referencing a dynamic address in a global policy.	V3
<a href="#">PR1558568</a>	Signatures configured in static group cannot be sorted out based on column name.	V3
<a href="#">PR1533304</a>	When additional global firewall rules are configured in UI, the insertion order of the rules get changed.	V3
<a href="#">PR1557743</a>	There are issues during address object replacement.	V3
<a href="#">PR1549753</a>	Security Director displays delete autonomous system configuration during preview policy.	V3
<a href="#">PR1549930</a>	Junos Space Security Director report data is not formatted.	V3
<a href="#">PR1558913</a>	When a user tries to import an address, conflict resolution page appends ipv4-only to the imported addresses.	V3
<a href="#">PR1562272</a>	Security Director allows to create object name even when the character limit exceeds.	V3
<a href="#">PR1556335</a>	There are issues with addresses when a user tries to import policies into Security Director.	V3
<a href="#">PR1562130</a>	Security Director pushes incorrect configuration for the external IP addresses configured in the VPN.	V3
<a href="#">PR1561605</a>	Security Director sets the incorrect SHA authentication algorithm for Phase 2 proposals.	V3

Table 8: Resolved Issues in Hot Patches (*continued*)

PR	Description	Hot Patch Version
<a href="#">PR1556351</a>	Security Director deletes IDP policy match condition for source-address and destination-address.	V3
<a href="#">PR1551514</a>	Security Director does not show search results for some policies.	V3
<a href="#">PR1549187</a>	Security Director displays delete autonomous system configuration during preview policy.	V3
<a href="#">PR1562778</a>	There are inconsistencies with policy name sorting.	V3
<a href="#">PR1565817</a>	User is unable to click Ok/Cancel option after selecting the re-direct profile in a rule.	V3
<a href="#">PR1562760</a>	User is unable to edit static routes in the Modify Device Configuration > Static Routes page.	V3
<a href="#">PR1450479</a>	An issue with Install Signatures schedule job.	V3
<a href="#">PR1555362</a>	Create Exempt Rule option does not work.	V3
<a href="#">PR1523032</a>	The CRL validation disable option is missing in the SSL Forward Proxy profile.	V2
<a href="#">PR1500407</a>	Security Director replaces an address object but displays unexpected data.	V2
<a href="#">PR1535068</a>	The URL pattern of UTM custom object is deleted.	V2
<a href="#">PR1514445</a>	Unable to update or publish firewall policies in most of the devices.	V2
<a href="#">PR1536657</a>	Configuration update fails for UTM AV (Avira engine) configuration.	V2
<a href="#">PR1528454</a>	Device connection status is DOWN in Security Director, but the status is UP in Junos Space Network Management Platform.	V2
<a href="#">PR1532193</a>	Device import fails due to object conflicts.	V2
<a href="#">PR1533297</a>	Vertical scrollbar disappears when editing a global rule.	V2

Table 8: Resolved Issues in Hot Patches (*continued*)

PR	Description	Hot Patch Version
<a href="#">PR1546841</a>	VPN profile is not created when Perfect Forward Secrecy is set as None.	V2
<a href="#">PR1508215</a>	API for report management does not work.	V2
<a href="#">PR1541572</a>	Publish or update fails when the Change Management feature is used in Security Director.	V2
<a href="#">PR1537482</a>	Security Director refresh search index fails with an exception.	V2
<a href="#">PR1529235</a>	Auto Sync job gets stuck while trying to resolve out-of-band and auto-sync policy changes.	V2
<a href="#">PR1545929</a>	Security Director does not support the Application Quality of Service (AppQoS) feature, and deletes this feature when the firewall is updated.	V2
<a href="#">PR1447083</a>	Source-identity does not populate in the Policy Enforcer rules created as part of the Sky ATP with SDSN setup.	V1
<a href="#">PR1490998</a>	Junos Space is unable to push policy changes due to Traffic-option settings in Enhanced Web Filtering (EWF).	V1
<a href="#">PR1501832</a>	Preview of an update/publish job fails for SRX Series firewall.	V1
<a href="#">PR1505663</a>	Unexpected results are returned when using global search for Policies.	V1
<a href="#">PR1512652</a>	An error message is displayed on the Tunnels page.	V1
<a href="#">PR1513934</a>	There is an issue with the hit count settings.	V1
<a href="#">PR1514870</a>	There is an issue with non-English policy descriptions in the preview/update workflow.	V1
<a href="#">PR1517134</a>	Some devices do not show logical system (LSYS) information correctly.	V1
<a href="#">PR1517200</a>	Individual CPU and memory data is not displayed on the dashboard widgets.	V1

Table 8: Resolved Issues in Hot Patches (*continued*)

PR	Description	Hot Patch Version
<a href="#">PR1521812</a>	User is unable to add device to realm in Sky ATP/JATP mode.	V1
<a href="#">PR1516070</a>	User is unable to configure port-overloading-factor for the NAT pool.	V1
<a href="#">PR1518308</a>	User is unable to create threat prevention policy when unified policy is configured.	V1
<a href="#">PR1503129</a>	While publishing a VPN configuration, Junos Space deletes the AS number.	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>.

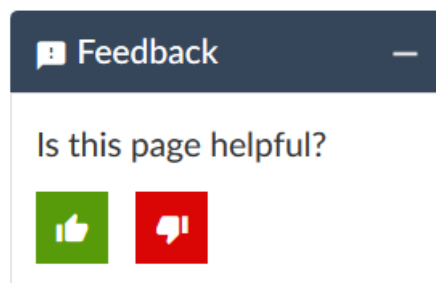
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

4 June, 2020—Revision 1—Junos Space Security Director Release 20.1R1

10 July, 2020—Revision 2—Junos Space Security Director Release 20.1R1

24 July, 2020—Revision 3—Junos Space Security Director Hot Patch Release 20.1R1 V1

11 November, 2020—Revision 4—Junos Space Security Director Hot Patch Release 20.1R1 V2

12 May, 2021—Revision 5—Junos Space Security Director Hot Patch Release 20.1R1 V3

13 January, 2022—Revision 6—Junos Space Security Director Hot Patch Release 20.1R1 V4

Copyright © 2022 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.