

Release Notes: Junos Space Security Director Release 20.3R1

14 December 2020

Contents	Introduction 2
	Release Notes for Junos Space Security Director 2
	New and Changed Features 3
	Supported Managed Devices 4
	Supported Junos OS Releases 5
	Supported Policy Enforcer and Juniper Sky ATP Releases 7
	Supported Browsers 8
	Installation and Upgrade Instructions 8
	Installing and Upgrading Security Director Release 20.3R1 9
	Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later 10
	Loading Junos OS Schema for SRX Series Devices 10
	DMI Schema Compatibility for Junos OS Service Releases 11
	Management Scalability 12
	Known Behavior 13
	Known Issues 16
	Resolved Issues 17
	Finding More Information 19
	Documentation Feedback 19
	Requesting Technical Support 20
	Self-Help Online Tools and Resources 20
	Creating a Service Request with JTAC 21
	Revision History 21

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 | 3](#)
- [Supported Managed Devices | 4](#)
- [Supported Junos OS Releases | 5](#)
- [Supported Policy Enforcer and Juniper Sky ATP Releases | 7](#)
- [Supported Browsers | 8](#)
- [Installation and Upgrade Instructions | 8](#)
- [Loading Junos OS Schema for SRX Series Devices | 10](#)
- [DMI Schema Compatibility for Junos OS Service Releases | 11](#)
- [Management Scalability | 12](#)
- [Known Behavior | 13](#)
- [Known Issues | 16](#)
- [Resolved Issues | 17](#)

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 20.3R1.

- **IPsec VPN enhancements**—We've simplified and modernized the IPsec VPN workflow:
 - Create and edit an IPsec VPN based on the selected tunnel mode and topology type.
 - Create, edit, and clone a VPN profile based on the selected VPN topology.
- **Remote VPN support**—Starting in Junos Space Security Director Release 20.3R1, we've provided the remote VPN support:
 - Create remote access VPNs such as Network Control Protocol (NCP) Exclusive Client and Juniper Secure Connect.
 - Configure RADIUS server and Local Authentication service options when you create access profiles.
 - View and modify global settings for a remote access VPN.
 - Create and edit address pools.
 - Monitor remote VPNs.
- **Extranet device enhancements**—We've made the following enhancements in extranet devices:
 - You can avoid duplicate IP addresses when you create extranet devices.
 - You can find the usage of extranet devices in IPsec VPNs.
- **Shared object enhancements**—We've made the following enhancements in shared objects:
 - When you import an address object from a CSV file, you can resolve object conflicts, if any. If there is a conflict, you can rename the object, overwrite the object with an imported value, or keep the existing object.
 - You can import service objects from a CSV file.
- **Disable firewall policy rules with no hits**—You can disable firewall policy rules that have not been hit for a specific duration. If you disable these rules, you'll notice performance improvement when you update the policies on devices.
- **Option to delete user ID**—You can now delete a user ID that is not configured in any policy, when you create standard and unified firewall policy rules. If you try to delete a user ID that is configured in a policy, then its reference ID and user ID are displayed.
- **Vendor description enhancement**—When you create an intrusion prevention system (IPS) signature dynamic group in a device running Junos OS Release 18.2 and later, only the product type value *All* is supported. Therefore, all vendor names are displayed in the drop-down list.
- **Firewall policy conversion enhancements**—We've made the following enhancements when you convert a traditional firewall policy to an unified firewall policy:

- We've added an option to select IDP policy. If you select an IDP policy during conversion from traditional to unified firewall policy, all firewall policy rules with IPS ON will be set to OFF and the selected IDP policy will be assigned to the firewall policy rule. If you do not select an IDP policy during conversion, firewall policy rules with IPS ON will be retained as is.
- You can convert a traditional firewall policy with devices assigned to an unified firewall policy.
- **Deprecated application firewall support**—Starting in Junos Space Security Director Release 20.3, we've provided import/update support for deprecated application firewall.

NOTE: If device configuration has a combination of both deprecated application firewall and dynamic application, import fails and you must migrate to unified policies and then re-import.

- **Performance improvements**— You'll observe enhanced performance in the provisioning workflows such as import, preview, snapshot, publish, and update.

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

Supported Managed Devices

Security Director Release 20.3R1 manages the following devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX240H
- SRX300
- SRX320
- SRX320-POE
- SRX340
- SRX345
- 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 Junos OS Releases

Security Director Release 20.3R1 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
- 19.2R3.5
- 19.3
- 19.4
- 19.4R3.11
- 20.1R1.11
- 20.2R2.11
- 20.3R1.8

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 1 on page 7 shows the supported Policy Enforcer and Juniper Sky Advanced Threat Prevention (Juniper Sky ATP) releases.

Table 1: 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
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 Sky ATP Releases (*continued*)

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

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

Supported Browsers

Security Director Release 20.3R1 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 20.3R1 | 9](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later | 10](#)

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

NOTE: You must use 20.1R1 Log Collector builds for Security Director Release 20.3R1. There are no Log Collector builds for 20.3R1 release. When you upgrade Security Director from 19.3R1, 19.4R1, 20.1R1 version to 20.3R1 version, you must upgrade Log Collector to 20.1R1 version.

If required, you can run LogCollectorVersionChange.sh script to change the Log Collector version from 20.1R1 to 20.3R1:

1. Copy LogCollectorVersionChange.sh to Junos Space/home/admin location
2. Run `chown jboss:jboss LogCollectorVersionChange.sh`
3. Run `chmod 777 LogCollectorVersionChange.sh`
4. Run `sh LogCollectorVersionChange.sh`

Installing and Upgrading Security Director Release 20.3R1

Junos Space Security Director Release 20.3R1 is supported only on Junos Space Network Management Platform Release 20.3R1 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

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 20.3R1, 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 10](#).

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 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	18.2R1.1	18.4R1.8
	18.3R1.1		
	18.2R1.1		

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 default DMI schema version, 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	18.3R1.1	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 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	18.3R1.1	18.4R1.8
	18.4R1.7		
	18.4R1.6		
	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 a default DMI schema version, 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	18.3R1.1	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 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 20.3R1.

- After upgrading from Security Director Release 19.3 or 19.4 to Security Director Release 20.3R1, IKE ID is displayed blank if IKE ID is defined as Default.
- Security Director does not generate delete CLIs if VPN already exist in the device and same device is used for creating another VPN from Security Director.
- In Junos Space Security Director Release 20.3R1, 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 20.3R1.
- After upgrade you will not be allowed to edit profiles with predefined proposals because profiles in Junos Space Security Director Release 20.3R1 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 20.3R1, you must import the VPN configuration.

NOTE: In Junos Space Security Director Release 20.3R1, 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 20.3R1. This is because you must select one of the routing protocols for creating a VPN in Junos Space Security Director Release 20.3R1.
- 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 20.3R1 and Policy Enforcer Release 20.3R1, we recommend you to 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 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 Junos Space Security Director Release 20.3R1.

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

- 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 the corresponding policy and right-click the policy. Select **View Device Policy Changes** and reject all changes, and then click **OK**. [PR1484953](#)

- Deployment of cipher list CLI works only when you perform Save or Save and Deploy.

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

- 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 (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](#)
- 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 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 Release 20.3R1:

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

- Junos Space Security Director generates incomplete CLIs for the 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](#)
- Junos Space Security Director deletes only one VPN at a time, although the UI allows you to delete multiple VPNs of the same device in a single delete attempt. [PR1508265](#)
- Junos Space Security Director fails to import a 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](#)
- Performance issues are observed in Security Director. [PR1478921](#)
- The user is unable to install the integrated Log Collector on a JA2500 appliance. [PR1490922](#)
- Security Director is unable to push policy changes due to connection limit for Enhanced Web Filtering (EWF). [PR1490998](#)
- Unable to generate policy analysis report for unused rules. [PR1495804](#)
- Junos Space Security Director cannot read the policy hit-count from the SRX 20.1. [PR1500139](#)
- Update or publish job preview fails for the SRX Series firewall. [PR1501832](#)
- Security Director deletes the autonomous system (AS) number while publishing a VPN configuration. [PR1503129](#)
- The report management API does not work. [PR1508215](#)
- There is an issue in Change Management to push updates in Security Director. [PR1508560](#)
- Security Director deletes UTM policy configuration lines for traffic-options. [PR1509739](#)
- Logical systems (LSYS) logs are not displayed in the domain where the logical system is present. [PR1510972](#)
- Error message is displayed on the Tunnels page. [PR1512652](#)
- The policy hit count scheduler does not work. [PR1513934](#)
- Security Director is unable to update or publish devices. [PR1514445](#)
- Security Director is unable to update policies to firewall. [PR1516046](#)

- The user is unable to configure port-overloading-factor for NAT pool in Security Director. [PR1516070](#)
- Security Director displays incorrect search results. [PR1516089](#)
- Update takes longer to show the configuration in the user interface. [PR1516842](#)
- There is an issue while deleting logical systems (LSYS). [PR1517134](#)
- Individual CPU and memory data are not displayed on the Dashboard widget page. [PR1517200](#)
- There is an issue with the threat prevention policy. [PR1518308](#)
- Certificate revocation list (CRL) validation disable option is missing for SSL Forward Proxy profile. [PR1523032](#)
- There is an issue with the scheduled report generation. [PR1527124](#)
- Security Director changed some of the rules to the "Then permit - tunnel" and "Destination address any" statements. [PR1527152](#)
- Device shows the status as DOWN in Security Director but the status is UP in Junos Space Network Management Platform. [PR1528454](#)
- There is an issue while trying to resolve out-of-band firewall policy changes. [PR1529235](#)
- When you add an interface to a routing-instance, Security Director deletes the entire configuration and tries to reset the configuration. [PR1531343](#)
- Unable to import devices to Security Director. [PR1532193](#)
- Search option does not work as expected. [PR1533072](#)
- The vertical scrollbar disappears when editing a global rule. [PR1533297](#)
- Rule created in Security Director does not save position. [PR1533391](#)
- After Security Director upgrade, UTM custom-object URL-pattern gets deleted. [PR1535068](#)
- The user is unable to configure custom-URL-object from Security Director. [PR1535957](#)
- UTM profiles cannot be applied because of missing URL-pattern. [PR1536021](#)
- Policy rules filter does not work. [PR1536398](#)
- Configuration update fails for UTM AV (Avira engine) configuration. [PR1536657](#)
- Firewall policy API calls do not work as expected. [PR1537434](#)
- Security Director refresh search index fails. [PR1537482](#)
- There is an issue in Change Management to push updates in Security Director. [PR1541572](#)
- There is an issue with the number of VPN profiles listed in the drop-down list. [PR1543039](#)
- Security Director preview does not display the configuration changes. [PR1545202](#)
- Security Director does not support the AppQoS feature and hence deletes it during an update to firewall. [PR1545704](#)

- Rule search or filtering does not work in Security Director. [PR1545743](#)
- Search objects and devices do not display the result. [PR1548385](#)
- During policy import URL patterns get deleted. [PR1552218](#)
- The user is unable to enroll device in Juniper ATP Cloud. [PR1555060](#)
- Custom URL-pattern with special character is not updated as expected. [PR1555170](#)
- There are issues during address object replacement. [PR1557743](#)
- Cluster status is not displayed as expected. [PR1560767](#)
- Junos Space Security Director report data is not formatted. [PR1549930](#)

NOTE: As part of release hardening, issues are resolved in the major areas such as usability, provisioning, device management, search framework, and monitoring.

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

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>.

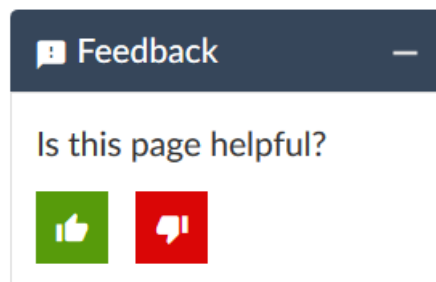
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

14 December, 2020—Revision 1—Junos Space Security Director Release 20.3R1

Copyright © 2020 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.