Release Notes: Junos Space Security Director Release 21.1R1

10 January 2022
Revision 4

Contents

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

This section describes the new features and enhancements to existing features in Junos Space Security Director and Policy Enforcer Release 21.1R1.

- **Secure Web Proxy setting for firewall policy—** Starting in Junos Space Security Director Release 21.1R1, you can use secure Web proxy to enable traffic for the selected dynamic applications to bypass the external proxy server and sent directly to a webserver.

  You must define a Web proxy profile by specifying external proxy server details and dynamic application. You can associate this secure Web proxy profile with standard firewall policy rule for advanced security. The traffic matching the firewall rule is sent to the configured external proxy server on the rule, unless the selected dynamic application matches.

- **Application visibility and threat map support for unified firewall policies—** Starting in Junos Space Security Director Release 21.1, when unified policy rules permit the traffic, selecting block action creates block rules in the appropriate unified policy.

- **LSYS support for log collector—** Starting in Junos Space Security Director Release 21.1, we've provided the support for source type for security logging configuration.

- **Inline address support for IPS policies—** Starting in Junos Space Security Director Release 21.1, you can import a valid source or destination inline address for an IPS Policy from an SRX Series device to Security Director. In the case of an inline address, the address object can be assigned in the device without creating the address object in the address-book. After import of inline address, you can edit the inline address in shared object. You can edit the name and IP address listed on the Addresses page. This is applicable for devices with Junos OS release 18.1 or later.

- **Support for NSX-T North-South traffic—** VMware NSX-T is the latest generation of VMware's network virtualization product series. NSX-T is the successor to NSX-V. VMware NSX-T provides framework to integrate the advanced security services as North-South at Edge Gateway. vSRX runs as a service virtual machine and provides advanced services such as L4 to L7 services. To deploy the advanced security features of the vSRX Virtual Services Gateway in the VMware NSX-T environment, the Junos Space Security Director, vSRX, and NSX-T Manager operate together as a solution to fully automate the provisioning and deployment of the vSRX to protect applications and data from advanced cyberattacks.

Supported Managed Devices

Security Director Release 21.1R1 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 21.1R1 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
- 18.1R2.6
- 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

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

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)
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
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

NOTE: For Policy Enforcer details, see Policy Enforcer Release Notes.

Supported Browsers

Security Director Release 21.1R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

IN THIS SECTION

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 21.1R1. There are no Log Collector builds for 21.1R1 release. When you upgrade Security Director release to 21.1R1, you must use Log Collector 20.1R1.

Installing and Upgrading Security Director Release 21.1R1

Junos Space Security Director Release 21.1R1 is supported only on Junos Space Network Management Platform Release 21.1R1 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

> **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 21.1R1, 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 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 18.3R1.1 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 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 18.4R1.7 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 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 21.1R1.

- If VPN is configured in Security Director Release earlier to 19.4 and upgraded to Security Director Release 20.1R1 and later, 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 20.1R1 and later, 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 and later.
- After upgrade you will not be allowed to edit profiles with predefined proposals because profiles in Junos Space Security Director Release 20.1R1 and later 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 and later, you must import the VPN configuration.

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

- 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 21.1R1.

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 and Policy Enforcer Release 21.1R1:

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

- The user is unable to export events to CSV for logs from Log collector. PR1552582
- In the Security Director UI, Create Exempt rule option does not work in Monitor > Events & logs > IPS > IPS events. PR1555362
- SRX imports get failed after adding a new dynamic address that is being called in a global policy. PR1555848
- Security Director pushes incorrect configuration for the external IP-Addresses that are configured in VPN. PR1562130
- Publish/Update of Threat Prevention Policy fails when Policy Enforcement Group (PEG) is changed from Location type to IP Address/Subnet type. PR1572517
- The custom feeds downloaded from remote server through HTTPS does not work. PR1576467
- Policy Enforcer does not allow the creation of custom feeds with a URL or domain. You can only create IP-based custom feeds. PR1522841
- The country codes available in the Security Director GeoIP feed does not match with SRX CLI GeoIP. PR1582766
- An issue with GeoIP country code for Serbia / Montenegro. PR1569964
- In Security Director UI, finish button for Add Sky ATP Realm/Modify Sky ATP Realm does not work in Configure > Threat Prevention > Feed Sources from Firefox 83.0 onward. PR1564456

Hot Patch Releases

This section describes the installation procedure, features, and resolved issues in Junos Space Security Director Release 21.1R1 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 21.1R1.47 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 21.1R1 Patch v*X* from the download site.

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

2. Copy the **SD-21.1R1-hotpatch-v*X*.tgz** file to the **/home/admin** location of the VIP node.

3. Verify the checksum of the hot patch for data integrity:

   md5sum SD-21.1R1-hotpatch-v*X*.tgz.

4. Extract the **SD-21.1R1-hotptach-v*X*.tgz** file:

   tar -zxvf SD-21.1R1-hotpatch-v*X*.tgz

5. Change the directory to **SD-21.1R1-hotpatch-v*X***.

   cd SD-21.1R1-hotpatch-vX

6. Execute the **patchme.sh** script from the **SD-21.1R1-hotpatch-v*X*** folder:

   sh patchme.sh

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

A marker file, **/etc/.SD-21.1R1-hotpatch-v*X***, is created with the list of Red-hat Package Manager (RPM) details in the hot patch.

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

New and Enhanced Features in the Hot Patch

Junos Space Security Director Release 21.1R1 hot patch includes the following enhancement:

- Log Director configuration changes—Starting in Junos Space Security Director Release 21.1R1 V1 hot patch, when you add Security Director Insights as a log collector, you must enable the **Enable SDI Log Collector Query Format** option in Junos Space Network Management Platform.

  To enable the option:

  1. Log in to Junos Space Network Management Platform.
  2. Select **Administration** > **Applications**.
  3. Right-click Log Director and select **Modify Application Settings**.
  4. Enable the **Enable SDI Log Collector Query Format** check box.

Resolved Issues in the Hot Patches

Table 6 on page 19 lists the resolved issues in Security Director Release 21.1R1 hot patches.

> **NOTE:** Log4j vulnerabilities are addressed in the Junos Space Security Director Release 21.1R1 V3 hot patch.

Table 6: Resolved Issues in Hot Patches

PR	Description	Hot Patch Version
PR1501832	The preview job fails for an SRX Series device.	V2
PR1573475	There are issues with the service object search.	V2
PR1587200	There are issues with top-talker and top source IPs by bandwidth reports.	V2
PR1593312	The user is unable to upload the IDP signature package.	V2
PR1597074	Security Director generates additional UTM commands after the user upgrades the SRX Series device.	V2

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

PR	Description	Hot Patch Version
PR1597978	There are issues with IPsec VPN extranet device IP address deployment.	V2
PR1598039	The commit check fails on Security Director.	V2
PR1598341	Proxy ARP delete commands are generated though the proxy ARP setting is enabled.	V2
PR1599595	The Configure Rules Sets option does not work as expected.	V2
PR1602370	Policy update to cluster devices fail without any error message.	V2
PR1602705	There are issues with Security Director Log Collector.	V2
PR1603010	When the application name is Any, there is a dynamic application name mismatch between SRX Series device and Security Director.	V2
PR1603617	There is an issue with the SRX Series device packet capture time stamp.	V2
PR1608469	There are issues with the service object search.	V2
PR1609767	The SRX Series device import fails.	V2
PR1581760	There are issues with policy update to the SRX Series device.	V2
PR1579779	VPN update fails without displaying any error message.	V2
PR1586900	The IPv6 related search in the UI does not work.	V2
PR1556335	There are issues with address resolution during policy import.	V2
PR1573316	Publish/update of security policies fail in Security Director.	V2
PR1601704	There are issues in policy update after you rename objects.	V2
PR1580860	When Security Director Insight is added as a Log Collector, it does not display the bubble chart in Application Visibility page.	V1

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

PR	Description	Hot Patch Version
PR1592620	Custom application signatures are not listed while user configures application firewall rule.	V1
PR1592626	For service objects Show Unused option does not work as expected.	V1
PR1579730	User is unable to use both IPS ON and idp-policy in a standard firewall group policy.	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.

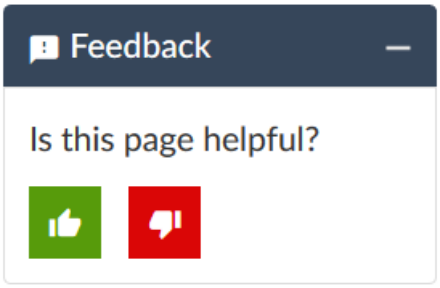
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

12 April, 2021—Revision 1—Junos Space Security Director Release 21.1R1

25 May, 2021—Revision 2—Junos Space Security Director Release 21.1R1 V1 hot patch

13 September, 2021—Revision 3—Junos Space Security Director Release 21.1R1 V2 hot patch

10 January, 2022—Revision 4—Junos Space Security Director Release 21.1R1 V3 hot patch