

# Release Notes: Junos Space Security Director Release 19.2R1

23 August 2019  
Revision 2

## Contents

Introduction .....	2
Release Notes for Junos Space Security Director .....	2
New and Changed Features .....	2
Supported Managed Devices .....	3
Supported Line Cards .....	4
Supported Junos OS Releases .....	5
Supported Policy Enforcer and Juniper Sky ATP Releases .....	6
Supported Browsers .....	6
Installation and Upgrade Instructions .....	7
Installing and Upgrading Security Director Release 19.2R1 .....	7
Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later .....	7
Loading Junos OS Schema for SRX Series Devices .....	8
DMI Schema Compatibility for Junos OS Service Releases .....	8
Management Scalability .....	9
Known Behavior .....	10
Known Issues .....	12
Resolved Issues .....	13
Finding More Information .....	14
Documentation Feedback .....	15
Requesting Technical Support .....	15
Self-Help Online Tools and Resources .....	15
Creating a Service Request with JTAC .....	16
Revision History .....	16

## 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 and application firewall signatures to a device.

---

## Release Notes for Junos Space Security Director

---

- [New and Changed Features on page 2](#)
- [Supported Managed Devices on page 3](#)
- [Supported Line Cards on page 4](#)
- [Supported Junos OS Releases on page 5](#)
- [Supported Policy Enforcer and Juniper Sky ATP Releases on page 6](#)
- [Supported Browsers on page 6](#)
- [Installation and Upgrade Instructions on page 7](#)
- [Loading Junos OS Schema for SRX Series Devices on page 8](#)
- [DMI Schema Compatibility for Junos OS Service Releases on page 8](#)
- [Management Scalability on page 9](#)
- [Known Behavior on page 10](#)
- [Known Issues on page 12](#)
- [Resolved Issues on page 13](#)

## New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director 19.2R1.

- **Introducing Quick Help in Security Director Release 19.2R1**—Our goal is to simplify help. You can now launch Quick Help from the **? Help Menu**. Alternatively, you can use the More... links on the user interface to access Quick Help. You no longer need to switch between windows to get help. Now, get quick help on all topics or the most popular ones, and also FAQs, in a tabbed interface.

We hope these changes help you find contextual information quickly and effectively within the user interface.

- **Synchronize out-of-band changes for firewall policies**—Starting in Junos Space Security Director Release 19.2R1, you can import or reject out-of-band changes from a device to Security Director manually or automatically. Out-of-band configuration changes are the changes you make to a device configuration using any method other

than by deploying the configuration change from Security Director. Automatic or manual synchronization of out-of-band changes are applicable only to firewall policies. Automatic synchronization is applicable for device-specific firewall policy, and manual synchronization is applicable for both device-specific and group policy.

For automatic or manual synchronization of out-of-band policy changes, the managed status of the device must be SD Changed, Device Changed, or In Sync. For this, you must update the device at least once from Security Director. In case of logical systems (LSYS), the root device might show the status as Device Changed if a policy is assigned to it. Update the root device so that the status is In Sync.

Out-of-band changes are not supported if more than one policy is assigned to a device or if rules are configured in All Devices Policy Pre/Post policies.

- **New predefined UTM policy**—Starting in Release 19.2R1, Junos Space Security Director supports junos-default-utm-policy in the predefined UTM policy list, which contains all the Junos default profiles. You can configure Junos default UTM policy on a device.
- **Usability enhancement in event viewer search**—Starting in Junos Space Security Director Release 19.2R1, in addition to manual search using keywords, you can drag and drop the values from non-empty cells in the grid into the event viewer search bar. The value is added as the search criterion and the search results are displayed. You can drag and drop only searchable cells. When you mouse over the rows in event viewer, searchable cells are displayed with a blue background. If you drag a searchable cell without any value or if the value = '-', you cannot drop the contents of such cells into the search bar. If the search bar already has a search criterion, all the subsequent drag and drop search criteria are prepended by 'AND'. After dropping the value in the search bar, the search condition is refreshed in the grid. This applies to both simple and complex search filters.
- **Source NAT pool**—Starting in Junos Space Security Director Release 19.2R1, you can choose an IP address from a source NAT pool. While creating the source NAT rule, you can choose the translation type as Pool. If you select the Pool option, then you must specify the source NAT pool from where the IP addresses are used for translation.

## Supported Managed Devices

Security Director Release 19.2R1 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 Line Cards

[Table 1 on page 5](#) shows the supported Juniper Networks line cards in Junos Space Security Director Release 19.2R1.

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>

## Supported Junos OS Releases

Security Director Release 19.2R1 supports the following Junos OS releases:

- 10.4
- 11.4
- 12.1
- 12.1X44
- 12.1X45
- 12.1X46
- 12.1X47
- 12.3X48
- 15.1X49
- vSRX 15.1X49
- 16.1R3-S1.3
- 15.1X49-D110
- 17.3
- 17.4
- 18.1
- 18.2
- 18.3
- 18.4

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 you to 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 6 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
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

## Supported Browsers

Security Director Release 19.2R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

## Installation and Upgrade Instructions

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

- [Installing and Upgrading Security Director Release 19.2R1 on page 7](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later on page 7](#)

### Installing and Upgrading Security Director Release 19.2R1

Junos Space Security Director Release 19.2R1 is supported only on Junos Space Network Management Platform Release 19.2R1 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 19.2R1, 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 19.2R1 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 19.2R1, 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 8](#).

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 8](#).

*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	18.2R1.1	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 4 on page 9](#).



*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 9](#).

*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 9](#).

*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

Junos Space Network Management Platform Release 19.2R1 does not support any new Junos OS releases. For information about Junos OS compatibility for releases up to and including Junos Space Platform Release 19.2R1, 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 -pnetscreen
mysql> update RuntimePreferencesEntity SET value=20 where
name='UPDATE_MAX_SUBJOBS_PER_NODE';
mysql> exit
```

Table 7 on page 10 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 10, 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 19.2R1.

- 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 18.1R1 and Policy Enforcer Release 18.1R1, you must migrate the existing vSRX VMs in NSX Manager from Policy Enforcer Release 17.1R1 to Release 18.1R1.

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"/>
```

## Known Issues

This section lists the known issues in Security Director Release 19.2R1.

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

- When out-of-band changes are imported to logical system (LSYS) device, the job is created for the root device along with the LSYS device, although changes are made only in the LSYS device. [PR1448667](#)
- The newly created first rule of a rule group always moves to the previous rule group when out-of-band changes are imported. [PR1451550](#)

Workaround: Manually move the imported rule to the appropriate rule group.

- You must not import a device with UTM traffic-options because Security Director throws a delta which causes update to fail. [PR1419135](#)

Workaround: Delete traffic-options from the UTM profiles.

- Import fails when a device is imported with UTM custom objects alone without a UTM policy. [PR1447779](#)

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

- Description search of firewall rules does not work if the search string is a combination of numerals and alphabets. [PR1441200](#)

Workaround: Enclose the search string with “\*”.

- Port range search of services in firewall rule page does not work. [PR1442093](#)
- Junos Space Security Director fails to import UTM configuration from devices with Junos OS version 18.2R1 or later because the new CLI changes are not supported. [PR1431759](#)
- Junos Space Security Director fails to import IPS policies from devices with Junos OS version 18.2R1 or later because the new CLI changes are not supported. [PR1411089](#)
- 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](#)
- Devices without unified support can be assigned under unified policies because Security Director does not have a validation check in the user interface. [PR1407283](#)
- 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 sometimes do not clear selected items. [PR1424112](#)
- The Show Unused option is removed for URL categories. [PR1431345](#)

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

## Resolved Issues

This section lists the issues fixed in Security Director and Policy Enforcer Release 19.2R1.

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

- There is an issue in the User ID field in a rule or policy. [PR1333296](#)
- Search does not work in Security Director. [PR1411949](#)
- Unable to update Chinese characters in policy description. [PR1414244](#)
- Search functionality in Security Director is unable to find specific IP address ranges or networks. [PR1414500](#)
- The Show Unused option for address objects does not show any result. [PR1415923](#)
- Incorrect Policy Enforcer URL is applied when a device is enrolled. [PR1419237](#)
- Security Director tries to update Junos Space VIP node IP address instead of Policy Enforcer IP address for security intelligence. [PR1426328](#)
- Publishing NAT policy on a firewall takes longer than usual. [PR1427016](#)

- Reports show incorrect graphs when the chart type is Timeline. [PR1427162](#)
- Unable to edit application firewall rules. [PR1428248](#)
- A warning related to Log Collector is displayed in Security Director. [PR1431604](#)
- Unable to publish policies. [PR1433546](#)
- Reports do not generate exact hit counts. [PR1434244](#)
- Unable to rename objects. [PR1437619](#)
- An error occurs during an import device configuration job. [PR1438257](#)
- IPS policy import is not successful. [PR1440101](#)
- Column filters are not persistent. [PR1441658](#)
- When you assign a device to a sub-domain, the logs from the device are shown in the global domain. [PR1441660](#)
- Search functionality does not work while importing new devices. [PR1444887](#)
- Shared objects are displayed with numbers and characters after import, instead of the actual names. [PR1444922](#)
- When you delete a device from Junos Space Platform, the device is not deleted from Security Director. [PR1445664](#)
- The source-except option in IPS policy is not working. [PR1449494](#)
- In Sky ATP mode, device cannot download the custom feeds. [PR1437088](#)
- Increase the current device limits in the **ondemand.yml** file. [PR1396064](#)
- When there is no realm present in the Sky ATP mode and you click the refresh grid, it tries to load the grid continuously. [PR1438093](#)
- Cloning unified policy in Security Director loses Dynamic Application information. [PR1447346](#)

---

## 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/>.

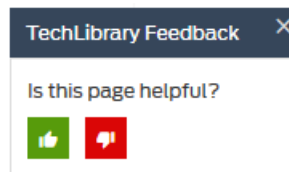
---

## 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

---

31 July, 2019—Revision 1—Junos Space Security Director Release 19.2R1

23 August, 2019—Revision 2—Junos Space Security Director Release 19.2R1

Copyright © 2019 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.