

Release Notes: Junos Space Security Director Release 18.3R1

9 December 2019
Revision 3

Contents	Introduction 2
	Release Notes for Junos Space Security Director 2
	Supported Managed Devices 3
	Supported Junos OS Releases 4
	Supported Policy Enforcer and Sky ATP Releases 5
	Supported Browsers 6
	Installation and Upgrade Instructions 6
	Installing and Upgrading Security Director Release 18.3R1 6
	Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later 7
	Loading Junos OS Schema for SRX Series Releases 8
	Management Scalability 8
	New and Changed Features 9
	Known Behavior 11
	Known Issues 13
	Resolved Issues 14
	Finding More Information 15
	Documentation Feedback 16
	Requesting Technical Support 16
	Self-Help Online Tools and Resources 17
	Creating a Service Request with JTAC 17
	Revision History 17

Introduction

The Junos Space Security Director application is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls.

Release Notes for Junos Space Security Director

IN THIS SECTION

- [Supported Managed Devices | 3](#)
- [Supported Junos OS Releases | 4](#)
- [Supported Policy Enforcer and Sky ATP Releases | 5](#)
- [Supported Browsers | 6](#)
- [Installation and Upgrade Instructions | 6](#)
- [Loading Junos OS Schema for SRX Series Releases | 8](#)
- [Management Scalability | 8](#)
- [New and Changed Features | 9](#)
- [Known Behavior | 11](#)
- [Known Issues | 13](#)
- [Resolved Issues | 14](#)

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, NAT policies, IPS policies, and application firewalls.

NOTE: You need IPS and application firewall licenses to push IPS and application firewall signatures to a device.

Supported Managed Devices

Security Director Release 18.3R1 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 supported log collection systems are:

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

Supported Junos OS Releases

- Security Director Release 18.3R1 supports the following Junos OS branches:
 - 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
- 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 on devices running Junos OS Release 11.4 or later.

NOTE: Before you can manage an SRX Series device by using Security Director, we recommend that you have the exact matching Junos OS schema installed on the Junos Space Network Management Platform. If there is a mismatch, a warning message is displayed during the publish preview workflow.

Supported Policy Enforcer and Sky ATP Releases

Table 1 on page 5 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 15.1X49-D60 and later
16.2R1	16.2R1	Junos15.1X49-D80 and later
17.1R1	17.1R1	Junos15.1X49-D80 and later
17.1R2	17.1R2	Junos15.1X49-D80 and later
17.2R1	17.2R1	Junos15.1X49-D110 and later
17.2R2	17.2R2	Junos15.1X49-D110 and later
18.1R1	18.1R1	Junos15.1X49-D110 and later
18.1R2	18.1R2	Junos15.1X49-D110 and later
18.2R1	18.2R1	Junos15.1X49-D110 and later
18.3R1	18.3R1	Junos15.1X49-D110 and later

Supported Browsers

Security Director Release 18.3R1 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 18.3R1 | 6](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later | 7](#)

This section contains the procedures to install and upgrade Junos Space Security Director and Log Collector.

Installing and Upgrading Security Director Release 18.3R1

Junos Space Security Director Release 18.3R1 is supported only on Junos Space Network Management Platform Release 18.3R1 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

In Junos Space Security Director Release 18.3R1, 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 18.3R1 image.

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

NOTE: 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 18.3R1, 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 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 7](#).

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 is used to login 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 Releases

You must download and install the matching Junos OS schema to manage SRX Series devices. To download the correct schema, under the Network Management Platform list, select **Administration > DMI Schema**, and click **Update Schema**. See [Updating a DMI Schema](#).

Management Scalability

The following management scalability features are supported on 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 your publish or update job performance.
- To enhance the performance further, increase the update subjobs thread number in the database. To increase the update subjobs thread in the database, run the following command:

```
#mysql -u <mysql-username> -p <mysql-password> sm_db;
mysql> update RuntimePreferencesEntity SET value=20 where
name='UPDATE_MAX_SUBJOBS_PER_NODE';
mysql> exit
```

NOTE: For mysql username and password, contact Juniper Support.

[Table 2 on page 9](#) shows the supported firewall rules per policy processed concurrently.

Table 2: 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	32 GB of RAM	Enabled	Dedicated node	Any
15,000	1	32 GB of RAM	Off or dedicated node	Dedicated node	Any
40,000	2	32 GB of RAM per node	Off or dedicated node	Dedicated node	Any
100,000	2	32 GB of RAM per node	Off or dedicated node	Dedicated node	SSD required

NOTE: If you use the database dedicated setup (SSD hard disk VMs) for the deployment mentioned in the table above, the performance of publish and update is better compared with the normal two-node Junos Space fabric setup.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director and Policy Enforcer Release 18.3R1.

- **Automatic grouping of policy rules**—In NAT policies, the rule group name is the same as the rule set name. The rule set name is a combination of source ingress and destination egress values. If you modify the value of source ingress or destination egress and save the changes, the policy rule set name changes and it is pushed to the device. However, because the rule group is specific to Security Director, the rule group name does not change and the modified rule is a part of the existing rule group. Starting in Security Director Release 18.3, if you modify the source ingress and destination egress values, you can rearrange the NAT policy rules, and the modified policy rules are grouped based on the rule set name.

To group the rules automatically, select **Configure>NAT Policies>Policies**. Right-click the rule that you want to auto group, or select **Auto Group** from the More list.

- **Shared objects enhancements**—The following are the enhancements for shared objects:

By default, you can create duplicate addresses, address groups, services, and service groups in Security Director. If you do not want to allow creation of duplicate addresses and services in Security Director, then go to Junos Space Network Management Platform and select **Administration>Application>Modify**

Application Settings>Shared Objects. Select the relevant check boxes to prevent creation of addresses and services with duplicate content. After the check box is selected, when duplicate addresses and services are selected in Security Director, an error message is displayed.

- While creating an address object, if you enter a duplicate host IP address, address range, network IP address, wildcard mask, or DNS name, then the creation of addresses with duplicate content is based on the shared objects settings in Junos Space Network Management Platform.
- While creating a service object, if you enter duplicate protocol details such as name, destination port, timeout duration, and source port or port ranges, then the creation of services with duplicate content is based on the shared objects settings in Junos Space Network Management Platform.
- While address or service groups are being created, if the selected address or service groups are already available, then the creation of address and service groups with duplicate content is based on the shared objects settings in Junos Space Network Management Platform.
- While creating a service object, if you do not provide a value in the source port or destination port field, a message is displayed that the default value will be Any. Any represents null or empty. Click **Cancel** and enter the destination or source port value or click **OK** to continue with the default value.
- **Inline creation of application firewall policy and SSL proxy profiles**—When you create a firewall policy rule and the rule action is **permit**, you can create inline an application firewall policy, SSL forward proxy profiles, and SSL reverse proxy profiles.
- **Drag and drop in NAT policy**—On the NAT policy rules page, you can drag and drop shared objects such as addresses and services to the corresponding cells in the rules grid. You can drag and drop data from source ingress to destination egress and vice versa, source port to destination port and vice versa, and source address to destination address and vice versa. You can also drag and drop the ports, addresses, and protocols across the rules in the grid.
- **Visual indicator for republishing the published policy rules**—After the published IPS, NAT, or firewall policy rules are edited and saved, you see an icon next to the check box for each saved policy rule on the corresponding policies page. When you hover over the icon, a message appears, indicating that the policy was edited and needs to be pushed to the device.
- **Manual lock**—By default, the locking mode for policies is automatic and policies are automatically locked when you start editing the rules. When you leave the rules editing page, the policy is automatically unlocked. The timeout interval for automatic locking is 15 minutes.

However, if required, you can choose the option to manually lock a policy. There is no timeout interval in case of manual lock. When you lock the policy and leave the page or log out, the policy remains locked. After you have completed editing the policy, you can unlock the policy and it then becomes available to other users for editing. The policy can be unlocked by the same user or by any other user with the same RBAC permissions. Only those users who have the permission to lock or unlock a policy are able to toggle between automatic mode and manual mode.

For manually locking a policy, select **Configure>Firewall Policy> Policies** and then select **Manual Mode** from the Locking list.

- **Feed Sources page**—The threat feeds from Sky ATP and custom feeds are now consolidated under the Feed Sources page, available under **Configure>Threat Prevention>Feed Sources**.
- **Update interval in Settings page**—You can now configure the update interval for each feed type in the Setting page, under **Configure>Threat Prevention>Feed Sources>Custom Feed>Settings**. You can specify how often feeds must be updated in minutes. The default interval is for every 5 minutes.
- **Monitor option for the infected hosts**—The Monitor option is enabled for the infected host profiles along with the existing Block and Quarantine actions. For certain infected hosts, Policy Enforcer will log all the traffic to monitor it.
- **Enhancements to the Sky ATP Realms**—The following additional information is available for a Sky ATP Realm under **Configure>Threat Prevention>Feed Sources>Sky ATP** tab:
 - **Feed status**—You can see the consolidated status of all the feeds of a Sky ATP realm. If the status of any one of the feeds is FAILED, then the consolidated status is shown as FAILED.
 - **Last downloaded**—You can now view the date and time of the last downloaded feed. Hover over the field to see a detailed list.
 - **Token expiry**—You can see the expiry date and time of a token generated at the Sky ATP side when a realm is registered. The token will be valid for one year. Once the token expires, the status is flipped to Expired. Thirty days prior to the expiry date, renew option is enabled to renew the token.
- **Device Feed Status details**—The detailed view of the download status of feeds from various feed sources is available under the **Monitor>Threat Prevention>Device Feed Status** page. You can view the status of feeds for each device.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 18.3R1.

- You must disable OpenNMS before installing the integrated Log Collector.

To disable OpenNMS:

1. Select **Network Management Platform > Administration > Applications**.

The Applications page appears.

2. Right-click **Network Management Platform** and select **Manage Services**.

The Manage Services page appears.

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 the Junos Space Network Management Platform and Security Director are already installed on a JA2500 or virtual machine.

- The *Enable preview and import device change* option is disabled by default. To enable this option, select **Network Management Platform > Administration > Applications**. Right-click **Security Director** and select **Modify Application Settings**. Under 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 the Security Director user interfaces are launched within 20 minutes, and the devices reconnects to the 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` is not sufficient.
- If 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, log in to the Policy Enforcer server by using SSH and run the following command:

```
cd /var/lib/nsxmicro
```

```
./migrate_devices.sh
```

This script migrates the existing Release 17.1R1 vSRX VMs in NSX Manager into the currently compatible Release 18.1R1.

- If the NSX server SSL certificate has expired or changed, communication between Security Director and NSX Manager does not work, thereby impacting the functionality of the NSX Manager, such as sync NSX inventory, security group update, and so on.

You must refresh the NSX SSL certificate by performing the following steps:

1. Log in to Policy Enforcer by using SSH.

2. Run the command:

```
nsxmicro_refresh_ssl --server <<NSX IP ADDRESS>>--port 443
```

This script gets the latest NSX SSL certificate and stores it for communication between Security Director and NSX.

- In the case of coexistence setup where other applications are installed in Junos Space along with Security Director, the JBoss PermSize must be increased from 512m to 1024m in `/usr/local/jboss/domain/configuration/host.xml.slave` file. Under `<jvm name="platform">`, change the following in `<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 18.3R1.

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

- When NAT rule creation exceeds the actual grid visibility range, the user cannot view and edit the new record as the complete grid is grayed out. [PR1369385](#)

Workaround: If create NAT rule grid is grayed out, click the Cancel icon and edit the newly created rule.

- After NAT policy rules are automatically grouped, **Policy is unlocked** message is displayed for fraction of a second. [PR1390075](#)
- JSA system logs are not parsing properly in Application Visibility, User Visibility, and Source IP Visibility pages. [PR1372721](#)
- When an SRX Series device is managed directly by Juniper Sky ATP for Advanced Threat Prevention, and is used in Security Director without integrating Policy Enforcer, then Security Director should not manage the threat prevention configuration. For example, security-intelligence policy and advanced-anti-malware policy. However, currently Security Director manages threat prevention configuration and tries to modify the configuration incorrectly. [PR1403904](#)

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 18.3R1.

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

- In Junos Space Security Director Release 16.2R1, manual lock is not supported. [PR1289918](#)
- The Security Director Plugin for JSA Offense Integration, **JSA_SD_App_17.2R1.zip**, is not working on JSA 2014.8r5 and later patches. [PR1336146](#)
- After discovering an SRX Series chassis cluster, importing a policy, and publishing that policy, when you delete the device from Junos Space Platform, the device remains in Security Director. [PR1356317](#)
- Unable to import policies from a **.zip** file. [PR1360965](#)
- The user encounters a `javax.ejb.EJBException: java.lang.NullPointerException` error while trying to preview a policy on Junos Space before installing it on the SRX Series device. [PR1362341](#)
- In Junos Space Security Director Release 17.2R1, the Export Policy to PDF feature does not list addresses and services objects. [PR1366494](#)
- In Junos Space Security Director Release 17.2R1, searching for source or destination address in a policy shows the exact match for the objects and does not show the subnets to which these addresses belong. [PR1366506](#)
- In Junos Space Security Director Release 17.2R1, searching for selected services in a rule displays all the services instead of only the selected services. [PR1368668](#)
- In Junos Space Security Director Release 17.1R2, the user is unable to reorder a firewall policy rule. [PR1372013](#)
- In Junos Space Security Director Release 17.2R2, the device is present in Junos Space platform, but missing in Security Director. [PR1372362](#)
- In Junos Space Security Director Release 17.2R1, the value for the “hit-count-details” field is missing in the API that is used to view the rule by rule ID in firewall policies. [PR1376371](#)
- In Junos Space Security Director Release 18.2R1, the routing-instance configuration is missing in View Configuration when you are publishing a new IPsec VPN. [PR1378743](#)
- Unable to import from the **.csv** file with address object hosts containing underscores. [PR1382657](#)
- In Junos Space Security Director Release 18.1R1, polymorphic variable import fails. [PR1376874](#)
- On the Security Director devices page, the logical system devices are shown as **undefined**. [PR1375971](#)

- In Junos Space Security Director Release 18.2R1, the Firewall Top Denials widget does not display data because of the use of an incorrect filter operator. [PR1377888](#)
- In Junos Space Security Director Release 17.2, you cannot filter events by using an IPv6 subnet mask. [PR1381723](#)
- A User ID field issue in a rule or policy is encountered while using the Update ID roles from Policy Devices option. [PR1333296](#)
- The user is unable to list available zones for a device when creating a zone variable. [PR1344807](#)
- In Junos Space Security Director Release 18.1R1, the user is unable to import the policy configuration from the SDG device (MX960). [PR1388783](#)
- After upgrading to Junos Space Security Director Release 18.1, you encounter an issue in the Security Director group policy order. [PR1386252](#)
- In Junos Space Security Director Release 18.2R1, CPU utilization is displayed as 100% for all the SRX Series devices. [PR1382170](#)
- When the policy action changed from block to quarantine, the VACL association on the quarantine VLAN was applied on the output (egress) on the VLAN stanza instead of input. [PR1376836](#)
- When the quarantined host moves from one VLAN to other VLAN and as part of the VACL update, the "Then" part of the term action is missed. The actual intended traffic redirection does not occur. [PR1375117](#)
- Quarantine fails, if the EX switch has an existing block VACL configuration stanza. [PR1373771](#)
- Quarantine fails for the second time for the same VLAN because of the presence of the ALLOW_ALL_OTHER_HOST_SDSN term. [PR1361896](#)

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>.

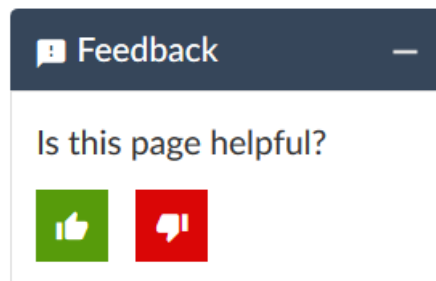
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

11 October, 2018—Revision 1 - Junos Space Security Director Release 18.3R1

28 January, 2019—Revision 2- Junos Space Security Director Release 18.3R1

9 December, 2019—Revision 3- Junos Space Security Director Release 18.3R1

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.