Release Notes: Junos Space Security Director Release 17.2R1

6 February 2018
Revision 3

Contents

Introduction

Junos Space is a comprehensive network management solution that simplifies and automates management of Juniper Networks switching, routing, and security devices.

Junos Space Management Applications optimize network management by extending the breadth of the Junos Space solution for various domains in service provider and enterprise environments.

Release Notes for Junos Space Security Director

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 17.2R1 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
- 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 17.2R1 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 SRX
- 17.4 SRX

- 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 4 shows the supported Policy Enforcer and Sky ATP releases.

Table 1: Supported Policy Enforcer and Sky ATP Releases

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (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

Table 1: Supported Policy Enforcer and Sky ATP Releases *(continued)*

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Sky ATP Supported Devices)
17.2R1	17.2R1	Junos15.1X49-D110 and later

Supported Browsers

Security Director Release 17.2R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

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

- Installing and Upgrading Security Director Release 17.2R1 on page 5
- Adding Security Director Log Collector Node in Security Director Release 17.2R1 on page 6

Installing and Upgrading Security Director Release 17.2R1

Junos Space Security Director Release 17.2R1 is supported only on Junos Space Network Management Platform Release 17.2R1 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 17.2R1, 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 17.2R1 image.

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

NOTE: Integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 eps.

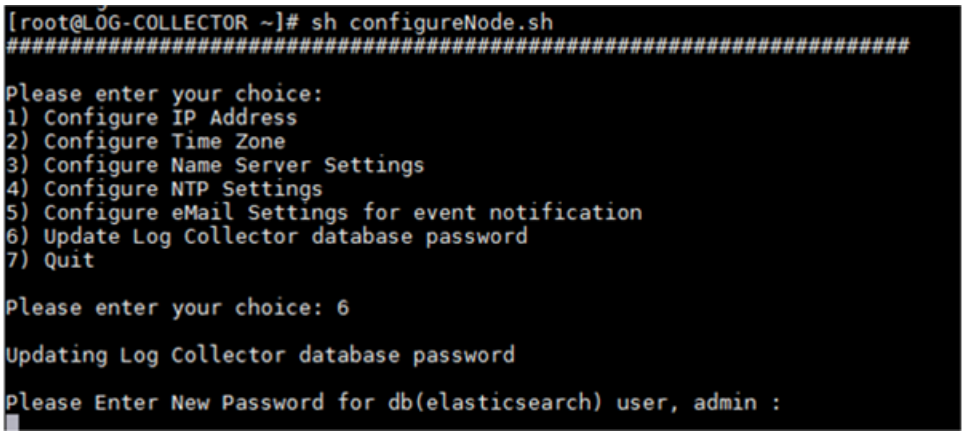
For more information about installing and upgrading Security Director Release 17.2R1, see Security Director Installation and Upgrade Guide.

Adding Security Director Log Collector Node in Security Director Release 17.2R1

From Security Director Release 17.2R1, use admin/juniper123 as default credentials to add Security Director Log Collector node to Security Director. You can change the default password from the Log Collector CLI using **configureNode.sh** as shown in Figure 1 on page 6.

The Security Director Log Collector node is no longer a special node in space fabric. You can only add the node directly to Security Director using admin credentials, as in the case of JSA node. For security reasons, non-root credentials are used to add node.

Figure 1: Change Password



For information on how to add 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

Table 2 on page 6 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

Table 2: Supported Firewall Rules per Policy *(continued)*

Number of Device Rules Processed Concurrently	JBoss Node Count	Memory	Platform OpenNMS Function	Log Collector	Hard Disk
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 this deployment, the performance of publish and update is better compared with the normal two-node Junos Space fabric setup.

The following management scalability features are supported on Security Director:

- By default, monitoring 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 a maximum of 10,000 SRX Series devices and 10,000 EX Series switches in a six-node Junos Space fabric (four JBoss servers and two database nodes). In a setup with 10,000 SRX Series devices, all settings for monitoring polling must be set to 60 minutes. If monitoring is not required, disable the monitoring to improve your publish or update job performance.
- To enhance the performance further, increase the update sub-jobs thread number in the database. To increase the update sub-jobs 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
```

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 17.2R1.

- **Application-based routing—**This release supports configuring and monitoring of advanced policy-based routing (APBR) on SRX Series devices on the basis of application and application groups to provide more context-based granularity. APBR is a type of session-based, application-aware routing. This mechanism combines the policy-based routing and application-aware traffic management solution.

  You can view apptrack events under Events and Logs in the Security Director user interface.

- **VPN monitoring—**VPN monitoring provides the status of IPsec VPNs and their tunnels between device endpoints after configuring, publishing, and updating them in Security Director. You can view the total number of monitored IPsec VPNs, tunnels, their status as either up or down, and historical tunnel data over time, ranging from 30 minutes to 2 months. The status is displayed in a dashboard and in tabular format. The number of tunnels for each VPN depends on the type of VPN, such as site-to-site, full-mesh, or hub-and-spoke. Security Director only supports route-based tunnel mode. You can view the tunnel status of IPsec VPNs configured on devices that are managed by Security Director.

- **End user profile—**An end user profile is a device identity profile. It is a collection of attributes that are characteristics of a specific group of devices, or of a specific device, depending on the attributes configured in the profile. The Packet Forwarding Engine of the SRX Series device maps the IP address of a device to the device identity profile. This feature supports Microsoft Windows Active Directory and third-party network access control (NAC) systems as authentication sources.

  You can create, edit, clone, view details, and delete an end user profile.

- **UTM enhancements—**This release supports downloading and installing of a URL category dynamically. You can download the Websense Enhanced Web Filtering category version from the category download site at https://update.juniper-updates.net and install it without upgrading Security Director. Websense occasionally releases new Enhanced Web Filtering categories. The category list is available in a file in JSON format. It supports a predefined base filter and all categories have default actions in the base filter. The base filter can be attached to a user profile, which acts like a backup filter. The base filter takes action for the categories that are not configured in a user profile.

  While creating Web filtering profiles, you can select one or more URL categories, an action, and a redirect profile.

- **JSA integration offense management—**An Administrator can integrate Security Director with Juniper Secure Analytics (JSA) or IBM QRadar using the Security Director extension application. The application is supported on JSA Release 2014.8 (IBM QRadar Release 7.2.8) and later.

  This integration provides a workflow to create Security Director firewall policies based on the events triggering the offense. You can create firewall rules in Security Director and apply them on firewall devices. You must register JSA or IBM QRadar with Security Director and on successful registration; a Security Director Extension wizard is added to the Offense summary page. This is where you can create Security Director firewall rules.

- **Threatmap enhancement—**This release supports Screen events and Sky ATP events.

Screen is a type of threat detected by SRX Series devices. The information reported about the attack includes:

- Attack name
- Action taken
- Source of the attack
- Destination of the attack

Sky ATP is a type of threat detected by SRX Series devices in collaboration with Sky ATP software. The information reported about the attack includes:

- Malware name
- Action taken
- Infected host
- Source of the attack
- Destination of the attack

- **Express path—**Express path (formerly known as *services offloading*) is a mechanism for processing fast-path packets in the network processor instead of in the Services Processing Unit (SPU). Express path considerably reduces packet-processing latency by 500–600 percent.

  You can use the Express Path section on the Modify Configuration page to view, create, edit, or delete Flexible PIC Concentrator (FPC) details on a device. You can toggle the status of one or more express paths. Express path is supported only on SRX5400, SRX5600, SRX5800, and rootLsys devices.

- **IPv6 settings to Screens Configuration—**This release supports IPv6-extension-header-limit, IPv6 malformed header, IPv6 extension header, hop-by-hop header, and destination header screen options.

- **Dashboard widgets—**This release supports the following dashboard widgets:

  - NAT Top Source Translation Hits—Displays the Network Address Translation (NAT) rule names with the most hits for source NAT.
  - NAT Top Destination Translation Hits—Displays the NAT rule names with the most hits for destination NAT.

- **Implementing threat policy on VMWare NSX—**Juniper Sky ATP identifies the infected virtual machines (VMs) running on VMware NSX and tags these VMs as infected. This action is based on the malware file exchange from the infected VMs, on the command and control communication with known botnet sites on the internet or both.

- **Environment variables and conditions—**Security Director supports configuring environment variables and conditions that can improve how you configure your firewall policy rules dynamically. With traditional firewall rules, if you want to block certain traffic or outbound traffic, then you must manually modify the action of the rules from permit to deny or vice versa. To avoid such manual configurations to the firewall rules and to improve your control over configurations, you can define your own environment variables and apply conditions using these variables.

- **Metadata-based policy enforcement—**The metadata-based policy enforcement enables you to create firewall rules based on user metadata. Traditionally, to create a firewall policy, you must know the IP address or range of IP addresses you wish to target. The introduction of metadata permits you to appropriately tag the IP addresses. These tags can then be used to create the firewall policy.
- **Sky ATP feature support—**The following Sky ATP features are supported:
  - IMAP e-mail support—You can use the Sky ATP Email Management page to configure e-mail management for IMAP. Enrolled SRX Series devices can transparently submit suspicious e-mails to Sky ATP for inspection and blocking. You can also take action on blocked e-mails, including releasing them and adding them to a blacklist.
  - X-Forwarded-For (XFF) header—XFF is a standard header added to packets by a proxy server that includes the real IP address of the client making the HTTP or HTTPS request. Therefore, if you add trusted proxy server IP addresses to a list in Sky ATP, by matching this list with the IP addresses in the HTTP header (or XFF) for requests sent from SRX Series devices, Sky ATP can determine the originating IP address.
  - Hash lookup—In the Create File Inspection Profile page, the Hash lookup only option is added to the File Categories section.
- **MX routers as enforcement points and DDoS profile support—**MX routers can be added as enforcement points to a Secure Fabric. Also, you can now include DDoS profile when configuring the threat prevention policies and create a custom feed for DDoS.

  The following actions can be taken when DDoS is detected on the MX router:
  - Block—Block a DDoS attack.
  - Rate limit value—Limit the bandwidth on the flow route. You can express the rate limit value in Kbps, Mbps, or Gbps units.
  - Forward to—Configure the routing next hop to forward the packets for scrubbing.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 17.2R1.

- 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 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 server 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 device reconnects to the Junos Space Network Management Platform. You can 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.
- After installing the Policy Enforcer Release 17.1 OVA image, you must manually start the following service commands:

  ```
  service sd_event_listener start
  service ssh_listener start
  ```

- If NSX-VSRX devices are managed in Security Director Release 17.1R1 and Policy Enforcer Release 17.1R1, then after upgrading to Security Director Release 17.1R2 and Policy Enforcer Release 17.1R2, the user has to login to the Policy Enforcer server using ssh and run the following command:

  cd /var/lib/nsxmicro

  ./migrate_devices.sh

This script will migrate the existing Release 17.1R1 NSX-VSRX devices into the currently compatible Release 17.1R2.

- If the NSX server SSL certificate has expired or changed, Security Director-to-NSX communication will not work and it will impact the functionality of the NSX, such as sync NSX inventory, security group update, and so on.

  You should refresh the NSX SSL certificate by performing the following:

  1. Log in to Policy Enforcer 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 Security Director-to-NSX communication.

Known Issues

- If you configure the inactivity timeout parameter as never and, instead of logging out of the session, close the browser, your session is shown as active until you log out. PR1152754
- After you upgrade Security Director, only superusers can view the data in the dashboard and event viewer.

  Workaround: Enable the View device logs permission under Event Viewer. PR1159530
- Grid column filter is not working for the Internet Explorer 11 browser. PR1161079
- Cluster devices are discovered in different domains. PR1162407
- When you invoke monitoring pages and the Top Compromised hosts dashboard widget, the **An Error occurred while requesting the data** error is displayed. PR1239956
- After you upgrade Security Director, the custom column is not visible in the firewall rule grid. PR1256789
- The Top Compromised hosts widget in the dashboard might not list all the realms. PR1262410
- You must manually synchronize NSX with the vCenter server to view the latest status. PR1285312
- The global search for a dynamic address group does not work as expected. PR1285893
- Any Service Groups notification sent from NSX to Security Director triggers an RPC update job for each vSRX device, instead of a single job with all the related vSRX devices. PR1288407
- If there is a change in the login password of NSX Manager, vCenter, or Junos Space, then use the Edit NSX Manager page in Security Director to modify the login password information. Otherwise, synchronization of NSX Manager and dynamic address groups update, fails.PR1291965

- If NSX is integrated with Security Director, you will see several login and logout entries in the audit log. PR1291972
- If you delete an NSX service, the associated firewall or IPS policies created by Security Director are also deleted. If you need a copy of the NSX created group firewall or IPS policies, you must clone them manually before deleting the NSX service. PR1291974
- As Security Director is not aware of the IDP licenses installed on the NSX with vSRX device, you must perform the full probe during the installation of the IDP signature. PR1291977
- If you add NSX Manager and deploy the Juniper Networks services before Security Director installs the IDP signatures, the vSRX device is discovered. However, you must install the IDP signature offline, create the IDP policy, and assign the NSX-vSRX devices. PR1291979
- If the Policy Enforcer VM is down or the NSX services are down when there is a change in the service group membership in NSX, you cannot trigger an event to vSRX to poll for the latest service group members from the feed server. PR1295882

  Workaround: Perform one of the following actions to trigger events to vSRX devices:

  - Modify the description of the service group when the services or Policy Enforcer VM is down.
  - Log in to the vSRX device using the SSH command and execute the following command:

    request security dynamic-address update address-name *Dynamic-Address-Name*

- Some Security Director dashboard preferences, such as dashboard widget selections, are not saved across multiple space fabric nodes. They must be configured independently on each node. PR1299082
- While upgrading Policy Enforcer Release 17.1R1 to Policy Enforcer Release 17.1R2, a blocked host, and firewall filters configured in the switches are not cleared.

  Workaround: Before the upgrade, manually resolve all the hosts as Resolved in the monitoring screen. After the upgrade, revert the status of Host Investigation to Open. This will reapply the firewall filters on to the switch. PR1309908
- If you directly go to the summary page instead of following the guided setup, the summary page may appear blank. As a workaround, follow each step in the guided setup. PR1309366
- Disenrolling the site in the infected custom feed does not remove the firewall filters from the switch for IP addresses that are in the custom feed. As a workaround, remove all the IPs from the custom feed and then disenroll the site from the Infected host feed page. PR1309819
- After upgrading to Security Director Release 17.1R2 and Policy Enforcer Release 17.1R2 from Security Director Release 17.1R1, when you add a new NSX, intermittently the dynamic address groups are not seen in the firewall rule source and destination address.

Workaround: Perform the following:

1. Restart the NSX microservice using the **service nsxmicro restart** command in Policy Enforcer.

2. Perform a manual synchronization of NSX from the user interface.

   You must see all the dynamic address groups in the source and destination addresses of a firewall rule. PR1310322

- When installing the Junos OS Release 17.4 schema on a Junos space server, publish or update might fail on SRX Series platforms when UTM custom-objects are present as part of the configuration.

  Workaround: You should restart JBoss. PR1330089

- Application firewall OCR is failing when OVER WRITE option is selected.

  Workaround: User can choose RE_NAME option and proceed with the rollback or import. PR1324941

- When user tries to add a child domain device specific values in variable address or zones, the changes are not saved in user interface. PR1330389

- NAT pool is not shown in OCR screen if the used address has conflicts. PR1330392

- Metadata feed server requires manual restart of secmgt-skyatp-proxy service when Security Director is installed or upgraded. PR1330400

  Workaround: After Security Director Release 17.2R1 is installed or upgraded, restart the following services manually:

  - service secmgt-skyatp-proxy stop
  - service secmgt-skyatp-proxy start

For known issues in Policy Enforcer, see Policy Enforcer Release Notes.

Resolved Issues

- The uploaded schema TAR file must be in the **/dmi/<device-type>/releases/<schema-version>/** folder. If the TAR is not in that folder, then although the installation is a success, the loading of the schema fails and, as a result, the Modify Configuration page does not load. PR1268413

- When you add NSX Manager and deploy Security Director as a service manager in NSX, the audit log shows the Policy Enforcer IP address as the currently logged in user. At the back end, the communication between NSX and Security Director happens through the REST API. PR1293841

- In Security Director Release 17.1R1, address object search does not work when integrated Log Collector is installed. PR1312104

- If a site is created with a CPPM connector, the site can be created only based on a location-based policy enforcement group. It cannot be created with an IP-based policy enforcement group. PR1288247
- You can configure only one Radius server as a controller for a connector. PR1287908

Documentation Errata

This section lists the errata in Security Director Release 17.2R1 documentation [PR1332378]:

- The Version text is repeated in the title bar of the What's New panel in the Security Director 17.2R1 user interface.
- The What's New panel content in the New Features tab is not current and Bug fixes tab is incorrect. Use the Release Notes link in the same panel to view all the new features and bug fixes in Security Director Release 17.2R1.

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 rating system—On any page of the Juniper Networks TechLibrary site at http://www.juniper.net/techpubs/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at http://www.juniper.net/techpubs/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 http://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: http://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: http://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- 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 http://www.juniper.net/support/requesting-support.html.

Revision History

26 December, 2017—Revision 1, Junos Space Security Director Release 17.2R1.

16 January, 2018—Revision 2, Junos Space Security Director Release 17.2R1

6 February, 2018—Revision 3, Junos Space Security Director Release 17.2R1