Release Notes: Junos Space Security Director Release 17.1

31 August 2017
Revision 2

Contents

Introduction 2
Release Notes for Junos Space Security Director 2
Supported Managed Devices 2
Supported Junos OS Releases 3
Supported Policy Enforcer and SkyATP Releases 4
Supported Browsers 4
Installation and Upgrade Instructions 5
Installing and Upgrading Security Director Release 17.1R1 5
Loading Junos OS Schema for SRX Series Releases 5
Management Scalability 5
New and Changed Features 6
Known Behavior 9
Known Issues 10
Resolved Issues 13
Finding More Information 14
Documentation Feedback 14
Requesting Technical Support 14
Self-Help Online Tools and Resources 15
Opening a Case with JTAC 15
Revision History 15

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 on page 2
- Supported Junos OS Releases on page 3
- Supported Policy Enforcer and SkyATP Releases on page 4
- Supported Browsers on page 4
- Installation and Upgrade Instructions on page 5
- Loading Junos OS Schema for SRX Series Releases on page 5
- Management Scalability on page 5
- New and Changed Features on page 6
- Known Behavior on page 9
- Known Issues on page 10
- Resolved Issues on page 13

Supported Managed Devices

Security Director Release 17.1R1 is 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 17.1R1 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

- 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 SkyATP Releases

Table 1 on page 4 shows the supported Policy Enforcer and SkyATP releases.

Table 1: Supported Policy Enforcer and SkyATP Releases

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (SkyATP 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

Supported Browsers

Security Director Release 17.1R1 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 17.1R1 on page 5

Installing and Upgrading Security Director Release 17.1R1

Junos Space Security Director Release 17.1 is supported only on Junos Space Network Management Platform Release 17.1 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 17.1, 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 17.1 image.

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 17.1, 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 5 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	32GB RAM	Enabled	Dedicated node	Any
15,000	1	32GB RAM	Off or dedicated node	Dedicated node	Any
40,000	2	32GB RAM per node	Off or dedicated node	Dedicated node	Any
100,000	2	32GB 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 high-end 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 17.1R1.

- **VMWare NSX integration**—VMware NSX is a network virtualization product owned by VMware. It integrates with vCenter server and provides users the ability to create and manage logical networks without modifying the underlying physical network. NSX supports the *distributed firewall* architecture. The VMWare distributed firewall currently supports only the basic firewall features such as Layer 2, Layer 3, and Layer 4. It does not provide advanced Layer 4 through Layer 7 security services, which are critical to provide complete protection in a software-defined data center (SDDC) environment.

  You can now add a vSRX virtual security appliance as a partner security service in the VMware NSX environment. The vSRX works in conjunction with Junos Space Security Director and VMware NSX Manager to deliver a complete and integrated virtual security solution for your SDDC environment. The vSRX provides advanced security services, including IPS and application control and visibility services through AppSecure.

- **Custom application signatures**—Application Identification supports defining your own custom application signatures and signature groups. Custom application signatures

are unique to your environment and are not part of the predefined application package when you install them into the device. The custom application signatures are pushed to the device when you publish or update, and subsequently, you can use them in the application firewall policy rules only.

You can import the custom application signatures from a device and also push the created custom application signatures to a device, by using the publish and update workflow. The custom application signatures are supported in Junos OS Release 15.1X49.D40 and later.

- **Packet Capture**—You can use the Packet Capture tool to download the packets captured by the SRX Series devices corresponding to attacks and analyze these packets externally using tools such as Wireshark, tcpdump, tshark, and so on. The Packet Capture tool captures the data packet and enables you to analyze the network traffic and troubleshoot network problems. The packet capture tool captures real-time data packets traveling over the network for monitoring and logging purposes. You must configure the SRX Series device to send the attack packets to the Junos Space Network Management Platform.

  Based on a preconfigured set of rules, SRX Series devices classify the packets as normal or an attack. When there is an attack, an SRX Series device sends the attack packets to the Junos Space Network Management Platform which runs a load balancer bound with a virtual IP.

  

  NOTE: Packet Capture is applicable only for intrusion prevention system (IPS) packets.

- **Captive portal support for unauthenticated browser users**—The SRX Series device now presents the user with a captive portal interface to enable users to be authenticated when they request access to an SRX Series protected resource, using an HTTP or HTTPS browser.

  Junos Space Security Director supports Auth Only Browser and Auth User Agent parameters to give you high control over how HTTP or HTTPS traffic is handled.

- **IKE path fragmentation**—IKEv2 message fragmentation allows IKEv2 to operate in environments where IP fragments might be blocked and peers would not be able to establish an IPsec security association (SA). The IKEv2 fragmentation splits a large IKEv2 message into a set of smaller ones so that there is no fragmentation at the IP level.

- **Advanced user identities query support**—You can query for advanced user identities from Juniper Identity Management Service (JIMS). JIMS provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. JIMS collects advanced user identities from different authentication sources for SRX Series devices.

  Junos Space Security Director is used to push the JIMS configuration to SRX Series devices to help them query JIMS to obtain IP address or user mapping and device information. SRX Series devices generate the authentication entries for the user firewall.

However, SRX Series firewall authentication can also push the authentication entries to JIMS.

- **ECDHE cipher suite support for SSL forward proxy**—Security Director provides an option to configure the following SSL Forward Proxy ciphers for the devices running Junos OS Release 15.1X49-D100.

  Elliptic Curve Diffie-Hellman Extchange (ECDHE) cipher suites are supported to enable perfect forward secrecy on an SSL forward proxy. The SSL forward proxy still uses RSA for authentication. However, it uses ECDH ephemeral key exchange to agree on a shared secret.

  The following ECDHE cipher suites are supported:

  - ECDHE-RSA-WITH-AES-256-GCM-SHA384
  - ECDHE-RSA-WITH-AES-256-CBC-SHA384
  - ECDHE-RSA-WITH-AES-256-CBC-SHA
  - ECDHE-RSA-WITH-AES-3DES-EDE-CBC-SHA
  - ECDHE-RSA-WITH-AES-128-GCM-SHA256
  - ECDHE-RSA-WITH-AES-128-CBC-SHA256
  - ECDHE-RSA-WITH-AES-128-CBC-SHA

- **Change control workflow**—The Change Control workflow enables you to request an approval for a change to a firewall or a NAT policy. The system tracks dependencies across change requests and makes these dependencies and change requests visible to the firewall administrator.

  The change control workflow provides the following benefits:

  - Direct correlation between a change ticket ID and its details and the associated firewall or NAT policy.
  - Policies that are modified within an activity (or configuration session) are locked and cannot be modified within other activities. This prevents conflicting changes that could make a policy unstable.
  - Activities are tracked within the workflow. You can use this information to determine what changes were made and who made the changes.
  - Approve and deploy the change requests to the network irrespective of the order in which they are created.

- **Aruba ClearPass in device configuration**—You can configure Aruba ClearPass as the authentication source for the integrated ClearPass authentication and enforcement feature. The SRX Series device and Aruba ClearPass collaborate to protect your network resources by enforcing security at the user identity level and controlling user access to the Internet.

- **Reporting enhancements**—The following predefined reports are added:

- Antivirus—Consolidated statistics related to all antivirus events.
- URL Report—Consolidated statistics related to all the URL events.
- Application and User Usage—Statistics related to the bandwidth usage by applications and users.
- Threat Report—Statistics related to top threats identified through IDP, Antivirus, Antispam, Screen, and Device Authentication failure events.

- **Additional dashboard widgets**—The following new dashboard widgets are available:
  - Application Top Application by Volume—Top applications based on volume or bandwidth.
  - IP Top Source IPs by Volume—Top source IP addresses of the network traffic by volume or bandwidth.
  - IP Top Spams By Source IPs—Top source IP addresses for spams.
  - Web Filtering Top Blocked Websites—Blocked websites, sorted by count.
  - Virus Top Blocked—Displays blocked viruses, sorted by count.
  - IP Top Source IPs by Sessions—Displays top source IP addresses of the network traffic by sessions.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 17.1R1.

- 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
```

Known Issues

- If you have access permissions for a firewall or NAT policy but do not have the permission to create objects, you cannot configure address, service, and other objects in the firewall or NAT policy. PR1140318
- 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 dashboard and event viewer.

  Workaround: Enable the View device logs permission under Event Viewer. PR1159530
- Grid column filter is not working in Internet Explorer 11 browser. PR1161079
- Cluster devices are discovered in different domains. PR1162407
- Upgrading Log Collector or Indexer from Security Director Release 15.2R1 to Security Director Release 15.2R2 does not update the version as expected. Log Collector is upgraded from Security Director Release 15.2R1 to Security Director Release 15.2R2. However, the version is displayed as Security Director Release 15.2R1 on the Security Director > Administration > Logging Management > Logging nodes page. PR1182608
- When you invoke monitoring pages and the Top Compromised hosts dashboard widget, the **An Error occurred while requesting the data** error is diplayed. PR1239956
- Custom column is not visible in the firewall rule grid after a Security Director upgrade. PR1256789
- The Top Compromised hosts widget in dashboard might not list all the realms. PR1262410

- 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
- 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, use the Edit NSX Manager page in Security Director to modify the login password information. Otherwise, synchronization of NSX Manager and updating of dynamic address groups fail. PR1291965
- If NSX is integrated with Security Director, you will see several login and logout entries in the audit log. PR1291972
- Because 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, vSRX device is discovered. However, you must install the IDP signature offline, create the IDP policy, and assign the NSX-vSRX devices. PR1291979
- When you add a NSX Manager that has more than 100 security groups, a proxy timeout error is shown on the Security Director UI. You can ignore this error because NSX Manager is already added to Security Director. Discard the Add NSX Manager page and manually synchronize the newly added NSX Manager. PR1292036
- 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
- If Policy Enforcer is not configured in Security Director and you access the NSX Manager or vCenter page, the page loading icon is shown forever. PR1294177
- RPC jobs are triggered for all the vSRX devices across services, on the same NSX Manager. PR1294566
- If you create firewall rules for group policies on multiple NSX Managers, and publish and update the firewall policies of all the vSRX devices belonging to the NSX Managers, then the auto redirect rule is created for only one NSX Manager and it fails for the other NSX Managers. PR1294568
- 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.
- Login to the vSRX device using the SSH command and execute the following command:

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

- During the Aruba ClearPass configuration, if you want to add user-query and no-user-query parameters at the same time, you must clear the Aruba ClearPass node completely and configure again.
- If the vSRX device is down or during the reboot, traffic still flows across VMs in NSX.

  Workaround: Double-click the Juniper service in the VMware vCenter and select the service instance, in the left pane. On the right pane, under the Manage tab, set the failOpen key value to False from True. PR1296801
- After the NSX discovery, you can view the VM details. However, if you click **View Networks**, only Network Adaptors are listed but the corresponding IPv4 and IPv6 addresses are not shown.

  Workaround: You must install VMware tools in all the VM payloads. PR1281873
- After the NSX discovery, you can view a list of service groups and corresponding dynamic address groups. However, if you click **View members** of any service group, the corresponding members of that selected service group is not shown. PR1281871
- Enrolling devices to Sky ATP through Policy Enforcer takes an average of four minutes to complete. Enrolling devices are done serially, not in parallel. [PR 1222713]
- The first time you open the Monitoring pages, you will receive an Error occurred while requesting the data message. This also happens the first time you open the Top Compromised Host dashboard widget. As a workaround, click your browser refresh button to refresh the page and display the information. [PR 1239956]
- The top compromised hosts widget in the dashboard does not list all the realms. As a workaround, drag and drop another top compromised host widget to the dashboard to display all realms. [PR 1262410]
- Connectors assigned to a site cannot be deleted. You must first unassign it from the site and then go to the Connectors window (Administration > Policy Enforcer > Connectors) to delete it.
- If a vSRX is properly enrolled in Sky ATP and you create a site within Policy Enforcer with that vSRX and a connector, the secure fabric page for that site shows the vSRX enroll status as failed. [PR 1284258]
- An infected host can be blocked using a custom feed, however there is no UI to indicate that the host is blocked. To unblock the infected host, remove it's IP address from the custom feed. [PR 1292394]
- 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. [PR 1288247]

- You can configure only one Radius server as a controller for a connector. [PR 1287908]
- Moving the C&C Threat Score slider in the Threat Prevention Policy window (Configure > Threat Prevention > Policy), for example from 10 to 8, may cause the Actions dropdown menu to appear empty. Click the arrow in the Actions menu to see the options. [PR 1296098]
- Removing a site from a realm may remove the SRX Series device from the Secure Fabric site. As a workaround, re-add the device to the site. [PR 1295460]
- When an SRX Series device is used as a Layer 3 gateway for a given host or subnet and a switch is part of the Secure Fabric, the block and unblock actions may fail when the PEG is created with the location group type. As a workaround, create the PEG with the IP/Subnet group type and associate that PEG to the threat prevention policy. [PR 1296535]
- Even when a device is unavailable (for example, the device is down), the removal of the device or site from the realm may state it as a successful dis-enroll.
- Adding the Malware Top Identified, File Categories Top Infected, File Categories Top Scanned, and Source Locations C & C Server and Malware dashlets to the dashboard before configuring Policy Enforcer or SkyATP realms in Security Director, causes the dashboard not to save any dashlets that are added. The dashlets do not appear on the dashboard after navigating to other pages or if you logout and login back.

  Workaround: Do one of the following steps:

  - If a SkyATP or Policy Enforcer setup is not available, delete the dashboard having the Malware Top Identified, File Categories Top Infected, File Categories Top Scanned, and Source Locations C&C Server and Malware widgets, and refresh the page.
  - If a SkyATP or Policy Enforcer setup is available, configure Policy Enforcer under Administration -> Policy Enforcer -> Settings in Security Director. Once Policy Enforcer is configured successfully, add a minimum of one realm in SkyATP Realms page under Configure -> Threat Prevention -> Sky ATP Realms in Security Director. Refresh the dashboard widgets again.

Resolved Issues

- Clicking the logical systems link in the root device must display all the logical systems devices of that root device. PR1155562
- The Modify Configuration page takes more than 10 seconds to load for the first time after each login. PR1240518
- Screens (Modify Configuration > Screens) are not activated through the right-click options but the activation works as expected from the More list. PR1240824
- Even after a fingerprint change is acknowledged, the device state remains as unverified. PR1241912

- Pagination support has been provided to view multiple static routes on the Modify Configuration page. PR1256633
- Predefined report definitions cannot be deleted, scheduled, or updated with e-mail address although the UI menu icons are enabled. PR1257172

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: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- 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://tools.juniper.net/SerialNumberEntitlementSearch/

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

7 August 2017—

31 August 2017—