Release Notes: Junos Space Security Director Release 17.1R2

9 December 2019
Revision 2

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

IN THIS SECTION

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 17.1R2 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 17.1R2 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
- 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 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

Supported Browsers

Security Director Release 17.1R2 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

IN THIS SECTION

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

Installing and Upgrading Security Director Release 17.1R2

Junos Space Security Director Release 17.1R2 is supported only on Junos Space Network Management Platform Release 17.1R1 that can run on the following devices:

- JA2500
- Junos Space Virtual Appliance
- Kernel-based virtual machine (KVM) server installed on CentOS Release 7.2.1511

In Junos Space Security Director Release 17.1R2, 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 17.1R2 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 17.1R2, 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 7 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 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 -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.

New and Changed Features

This section describes the new feature and enhancement to existing feature in Junos Space Security Director Release 17.1R2.

- **Threat map block fix**—To block a country based on the threats detected from Live Threat Map, you need not configure Policy Enforcer with Sky ATP. Security Director now runs a microservice that handles retrieving the cloud feeds and other operations. The microservice runs a proxy in the background and registers the SRX Series device to Sky ATP upon publishing and updating the firewall policy with block operations to the SRX Series device.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 17.1R2.

- 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 17.1R1 and Policy Enforcer 17.1R1, after upgrade of Security Director 17.1R2 and Policy Enforcer 17.1R2, user has to login to Policy Enforcer server using ssh and run the following command:

cd /var/lib/nsxmicro

./migrate_devices.sh

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

- If NSX server SSL certificate is expired or changed, SD-NSX communication will not work and it will impact the functionality of 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 machine 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 SD-NSX communication.

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 displayed. 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 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 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.
- 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

- If you delete a 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
- While upgrading Policy Enforcer Release 17.1R1 to Policy Enforcer Release 17.1R2, blocked host in switch is not getting cleared and firewall filters configured in 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
- 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 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

- Unable to update reth interface speed from Security Director. Device update fails due to wrong CLI.

  Workaround: Configure reth interface speed directly from Device. To discard reth speed changes already made on Security Director user interface, use NMP schema based editor approve and deploy workflow. You can start updating device for other pending configuration. PR1296675
- In the default mode, when you go through the general setup wizard, blank page is shown in summary and user is unable to click OK. To exit, you need to cancel the wizard.

  Workaround: Go through each of the guided setup pages in sequence. PR1309366
- While upgrading to 17.1R2 from 16.1R1 or 16.2R1, data migration is not supported on multimode Log Collector. PR1309790
- On rebooting JA2500 Log Collector, eth1 interface configuration is lost . PR1310033
- 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.
- 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 its IP address from the custom feed. [PR 1292394]
- You can configure only one Radius server as a controller for a connector. [PR 1287908]
- 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 Sky ATP 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 Sky ATP 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 Sky ATP 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 Sky ATP Realms page under Configure > Threat Prevention > Sky ATP Realms in Security Director. Refresh the dashboard widgets again.

- If you entered incorrect credentials in the Realm window, the OK button is disabled. As a workaround, close this window, re-open it and enter your correct credentials. [1310817]
- After upgrading the Policy Enforcer software, logs are incorrectly appended to the latest logs (config_server.log.1) instead of following the log file rotation method. [1310695]
- 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. [1309819]
- In a multi-site scenario with a Radius server as the DOT1X for AAA services, assigning all sites and the enforcement points (firewalls and switches) within a single Sky ATP realm may cause issues in picking the correct threat prevention infected host policy. As a workaround, after creating a connector for the Radius Controller and assigning it to all the sites, register or create a unique Sky ATP realm and associate it with a site. [1309881]

- When multiple sites are configured with multiple realms (and all sites have connectors), the Sky ATP policy overwrites all SRX Series devices in the site instead of the specific SRX Series device. [1308737]
- If you go directly to the summary page instead of following each step in the guided setup, the summary page may appear blank. As a workaround, go follow each step in the guided setup. [1309366]
- You cannot delete the configuration for an SRX Series device when the threat prevention policy is associated with multiple PEGS. [1309383]
- Resolving an infected host fails when there is no endpoint session available in the Radius server. [1311081]
- The following minor UI issues are present:
  - For connectors with IP subnets, sometimes the subnets cannot be moved to available.
  - When you modify a threat prevention policy, the GeoIP state changes from updated to assign to groups. The state should be maintained.
  - Deleting a realm displays an OK message with a red notification window or popup. [1310813]
- The third-party adapter package for KVM displays version 17.1R1 instead of 17.1R2. For example:

  [user@host]# cat /etc/redhat-release

  CentOS release 6.8 (Final)

  Policy Enforcer Package Version: 17.1R2-3-

  3rd Party Adapter Package Version: 17.1R1-24

Resolved Issues

- 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
- If the vSRX device is inactive or during reboot, traffic still flows across VMs in NSX. PR1296801
- 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
- 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

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.

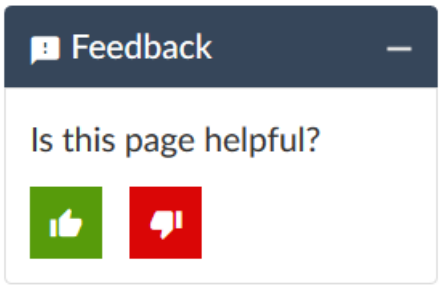
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

4 October 2017—

9 December 2019—