

Release Notes: Junos Space Security Director Release 19.1R1

26 April 2019

Contents

Introduction	2
Release Notes for Junos Space Security Director	2
Supported Managed Devices	2
Supported Junos OS Releases	3
Supported Policy Enforcer and Juniper Sky ATP Releases	4
Supported Browsers	5
Installation and Upgrade Instructions	5
Installing and Upgrading Security Director Release 19.1R1	5
Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later	6
Loading Junos OS Schema for SRX Series Devices	7
Management Scalability	7
New and Changed Features	8
Known Behavior	9
Known Issues	10
Resolved Issues	11
Finding More Information	12
Documentation Feedback	13
Requesting Technical Support	13
Self-Help Online Tools and Resources	13
Creating a Service Request with JTAC	14
Revision History	14

Introduction

The Junos Space Security Director application is a powerful and easy-to-use solution that enables you to secure your network by creating and publishing firewall policies, IPsec VPNs, Network Address Translation (NAT) policies, Intrusion Prevention System (IPS) policies, and application firewalls.



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

Release Notes for Junos Space Security Director

- [Supported Managed Devices on page 2](#)
- [Supported Junos OS Releases on page 3](#)
- [Supported Policy Enforcer and Juniper Sky ATP Releases on page 4](#)
- [Supported Browsers on page 5](#)
- [Installation and Upgrade Instructions on page 5](#)
- [Loading Junos OS Schema for SRX Series Devices on page 7](#)
- [Management Scalability on page 7](#)
- [New and Changed Features on page 8](#)
- [Known Behavior on page 9](#)
- [Known Issues on page 10](#)
- [Resolved Issues on page 11](#)

Supported Managed Devices

Security Director Release 19.1R1 manages the following devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX240H
- SRX300
- SRX320
- SRX320-POE
- SRX340
- SRX345

- SRX550
- SRX550M
- SRX650
- SRX1400
- SRX1500
- SRX3400
- SRX3600
- SRX4100
- SRX4200
- SRX5400
- SRX5600
- SRX5800
- SRX4600
- vSRX
- MX240
- MX480
- MX960
- MX2010
- MX2020
- LN1000-V
- LN2600

The following log collection systems are supported:

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

Supported Junos OS Releases

Security Director Release 19.1R1 supports the following Junos OS releases:

- 10.4
- 11.4
- 12.1
- 12.1X44
- 12.1X45

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

SRX Series devices require Junos OS Release 12.1 or later to synchronize the Security Director description field with the device.

The logical systems feature is supported only on devices running Junos OS Release 11.4 or later.



NOTE: To manage an SRX Series device by using Security Director, we recommend you to install the matching Junos OS schema on the Junos Space Network Management Platform. If the Junos OS schemas do not match, a warning message is displayed during the publish preview workflow.

Supported Policy Enforcer and Juniper Sky ATP Releases

Table 1 on page 4 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 OS Release 15.1X49-D60 and later
16.2R1	16.2R1	Junos OS Release 15.1X49-D80 and later
17.1R1	17.1R1	Junos OS Release 15.1X49-D80 and later
17.1R2	17.1R2	Junos OS Release 15.1X49-D80 and later
17.2R1	17.2R1	Junos OS Release 15.1X49-D110 and later

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

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper Sky ATP-supported Devices)
17.2R2	17.2R2	Junos OS Release 15.1X49-D110 and later
18.1R1	18.1R1	Junos OS Release 15.1X49-D110 and later
18.1R2	18.1R2	Junos OS Release 15.1X49-D110 and later
18.2R1	18.2R1	Junos OS Release 15.1X49-D110 and later
18.3R1	18.3R1	Junos OS Release 15.1X49-D110 and later
18.4R1	18.4R1	Junos OS Release 15.1X49-D110 and later
19.1R1	19.1R1	Junos OS Release 15.1X49-D110 and later

Supported Browsers

Security Director Release 19.1R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

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

- [Installing and Upgrading Security Director Release 19.1R1 on page 5](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later on page 6](#)

Installing and Upgrading Security Director Release 19.1R1

Junos Space Security Director Release 19.1R1 is supported only on Junos Space Network Management Platform Release 19.1R1 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 19.1R1, a single image installs Security Director, Log Director, and the Security Director Logging and Reporting modules. All three applications are installed when you install the Security Director Release 19.1R1 image.



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



NOTE: An integrated Log Collector on a JA2500 appliance or Junos Space virtual appliance supports only 500 events per second (eps).

For more information about installing and upgrading Security Director Release 19.1R1, see [Security Director Installation and Upgrade Guide](#).

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

For distributed Log Collector deployment, you must add only a Log Receiver node. You can add the node directly to Security Director using admin credentials, as in the case of the JSA node. For security reasons, non-root credentials are used to add a node.



CAUTION: For Security Director Log Collector, provide the default credentials: username is admin and password is juniper123. You must change the default password by using the Log Collector CLI command `configureNode.sh` as shown in [Figure 1 on page 6](#).

Figure 1: Change Password

```
[root@LOG-COLLECTOR ~]# sh configureNode.sh
#####
Please enter your choice:
1) Configure IP Address
2) Configure Time Zone
3) Configure Name Server Settings
4) Configure NTP Settings
5) Configure eMail Settings for event notification
6) Update Log Collector database password
7) Quit

Please enter your choice: 6

Updating Log Collector database password

Please Enter New Password for db(elasticsearch) user, admin :
```

For JSA, provide the admin credentials that are used to log in to the JSA console.

For information about how to add the Log Collector node to Security Director, see [Security Director Installation and Upgrade Guide](#).

Loading Junos OS Schema for SRX Series Devices

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

Management Scalability

The following management scalability features are supported in Security Director:

- By default, monitor polling is set to 15 minutes and resource usage polling is set to 10 minutes. This polling time changes to 30 minutes for a large-scale data center setup such as one for 200 SRX Series devices managed in Security Director.



NOTE: You can manually configure the monitor polling on the **Administration > Monitor Settings** page.

- Security Director supports up to 15,000 SRX Series devices with a six-node Junos Space fabric. In a setup with 15,000 SRX Series devices, all settings for monitor polling must be set to 60 minutes. If monitoring is not required, disable it to improve the performance of your publish and update jobs.
- To enhance the performance further, increase the number of update subjobs thread in the database. To increase the update subjobs thread in the database, run the following command:

```
#mysql -pnetscreen
mysql> update RuntimePreferencesEntity SET value=20 where
name='UPDATE_MAX_SUBJOBS_PER_NODE';
mysql> exit
```

Table 2 on page 7 shows the supported firewall rules per policy that are 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 a database dedicated setup (SSD hard disk VMs) for the deployment mentioned in [Table 2 on page 7](#), the performance of publish and update is better compared to the performance in a normal two-node Junos Space fabric setup.

New and Changed Features

This section describes the enhancements to existing features in Junos Space Security Director 19.1R1.

- **ESXi 6.7 support**—Junos Space Security Director Release 19.1R1 is supported on VMware ESXi 6.7 hypervisor.
- **Cleanup scripts**—You can now use the following cleanup scripts from the Junos Space CLI:
 - **Shared object stale references cleanup script**—Removes unwanted stale references from the database. In previous releases, this script was part of Junos Space Security Director deployment, and hence the deployment took longer to finish. Starting in Junos Space Security Director Release 19.1R1, we have added this script as part of the cleanup script and we have also provided a separate Rest API.
 - **Stale device entries cleanup script**—Removes unwanted stale devices from the database. If you delete a device from Junos Space Network Management Platform and if the device is still present in Junos Space Security Director, you can use the cleanup script to delete those entries from the database.
 - **Stale VPN entries cleanup script**—Removes any stale VPN entries from the database.
 - **Unresponsive job cleanup script**—Removes any job that is unresponsive. A job may become unresponsive in the following scenarios:
 - If rule entries are present in Security Director CLI model tables and are not present in Security Director rule page, then those entries will be updated with deleted field as true in Security Director database.
 - If the older versions of a published rule still has the deleted field as false, then those are updated to true in Security Director database.
 - On renaming a rule if you still see the deleted field of the old rule as false, then it is updated to true in Security Director database.
- **Device polling for dashboard monitors**—Device polling performance is now improved. All polling threads run in parallel, which reduces memory usage.
- **Optimized refresh search index**—Following are the performance improvements:
 - The performance of the manual refresh search index has been improved.
 - The scheduled refresh search index has been implemented. By default, scheduled time is every Saturday 2 AM. Administrators can change the scheduled time by navigating to Junos Space Network Management Platform > Administration >

Applications. Right-click Security Director, select Modify Application Settings, and then select Search-Index.

- Security Director elastic search is upgraded from version 5.4 to version 6.5. The performance of the manual refresh search index has been improved.
- **MySQL queries**—Optimized MySQL queries related to edit and unused shared objects.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 19.1R1.

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

To disable OpenNMS:

1. Select **Network Management Platform > Administration > Applications**.
2. Right-click **Network Management Platform**, and select **Manage Services**.
3. Select **Network Monitoring**, and click the Stop Service icon.

The network monitoring service is stopped, and the status of OpenNMS is changed to Disabled.



NOTE: You must ensure that Junos Space Network Management Platform and Security Director are already installed on a JA2500 appliance or Junos Space virtual appliance.

- The **Enable preview and import device change** option is disabled by default.

To enable this option:

1. Select **Network Management Platform > Administration > Applications**.
 2. Right-click **Security Director**, and select **Modify Application Settings**.
 3. From Update Device, select the **Enable preview and import device change** option.
- If you restart the JBoss application servers manually in a six-node setup one-by-one, Junos Space Network Management Platform and the Security Director user interfaces are launched within 20 minutes, and the devices reconnect to Junos Space Network Management Platform. You can then edit and publish the policies. When the connection status and the configuration status of all devices are UP and IN SYNC, respectively, click **Update Changes** to update all security-specific configurations or pending services on SRX Series devices.

- To generate reports in the local time zone of the server, you must modify **/etc/sysconfig/clock** to configure the time zone. Changing the time zone on the server by modifying **/etc/localtime**, does not generate report in the local time zone.
- If the vSRX VMs in NSX Manager are managed in Security Director Release 17.1R1 and Policy Enforcer Release 17.1R1, then after upgrading to Security Director Release 18.1R1 and Policy Enforcer Release 18.1R1, log in to the Policy Enforcer server by using SSH and run the following commands:

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

```
./migrate_devices.sh
```

This script migrates the existing vSRX VMs in NSX Manager from Policy Enforcer Release 17.1R1 to Release 18.1R1.

- If the NSX Server SSL certificate has expired or changed, communication between Security Director and NSX Manager fails, thereby impacting the functionality of NSX Manager, such as sync NSX inventory and security group update.

To refresh the NSX SSL certificate:

1. Log in to Policy Enforcer by using SSH.

2. Run the following command:

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

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

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

```
<option value="-XX:PermSize=1024m"/>
```

```
<option value="-XX:MaxPermSize=1024m"/>
```

Known Issues

This section lists the known issues in Security Director Release 19.1R1.

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

- Junos Space Security Director fails to import UTM configuration from devices with Junos OS version 18.2R1 or later because the new CLI changes are not supported. [PR1431759](#)
- Junos Space Security Director fails to import IPS policies from devices with Junos OS version 18.2R1 or later because the new CLI changes are not supported. [PR1411089](#)

- After upgrading Junos Space Security Director release to 19.1R1, predefined reports are not shown in Reports page. [PR1431601](#)

Workaround: Restart JBoss node to see the predefined reports.

- Update fails for unified policies when an SSL proxy profile that is set as global in a device is not used in any policy for that device. [PR1407389](#)
- Devices without unified support can be assigned under unified policies as Security Director does not have a validation check in the user interface. [PR1407283](#)
- While upgrading Security Director Log Collector along with Junos Space Network Management Platform, dashboard widget preferences are not retained. [PR1350292](#)
- Junos Space Security Director fails to import VPN if a device uses master password encryption because VPN preshared key with \$8\$ format is not supported. [PR1416285](#)
- Junos Space Security Director tries to delete the UTM custom object URL pattern used in the firewall with UTM services, which causes policy update to fail. [PR1406969](#)
- Junos Space Security Director generates wrong CLI commands for deleting Application Based Routing (APBR) rules. [PR1417708](#)
- A policy analysis report with huge number of rules cannot be generated. [PR1418125](#)
- When a column filter is used, deselect all and clear all sometimes do not clear selected items. [PR1424112](#)
- The Create Exempt Rule option does not work in the IPS event viewer. [PR1380415](#)
- The scheduled report is not sent when the user is logged out. [PR1352984](#)
- The Show Unused option is removed for URL categories. [PR1431345](#)

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

Resolved Issues

This section lists the issues fixed in Security Director Release 19.1R1.

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

- JSA system logs are not parsed correctly. [PR1372721](#)
- There are issues related to search and filter in policy rules. [PR1398589](#)
- There is a mismatch in the device details in IP domain mapping. [PR1390925](#)
- Unable to navigate to firewall policy from an SRX log. [PR1390963](#)
- When you update a device, an error message is displayed. [PR1395550](#)
- Applications are displayed as Unknown. [PR1399255](#)
- There are issues while adding JSA to Junos Space Security Director. [PR1401510](#)
- Existing VPN configurations are altered in a device. [PR1402386](#)
- A few changes made in the device are not displayed. [PR1403916](#)

- While deploying changes through Junos Space Security Director, you can see a display issue. [PR1407168](#)
- There is an issue related to deletion of address group object. [PR1408463](#)
- There is an issue related to number of usages displayed in the Find Usage option. [PR1408519](#)
- After upgrade, latest signature list is not updated. [PR1409305](#)
- You can see a publishing error. [PR1411325](#)
- Search issue in Junos Space Security Director. [PR1411949](#)
- After upgrade, preview configuration fails for a specific policy. [PR1412836](#)
- Recurrence job issue in download URL categories. [PR1413658](#)
- There are issues with Publish View button display in Internet Explorer browser. [PR1414777](#)
- There is an issue with display of unused address objects. [PR1414866](#)
- Update issue is seen on an SRX5400 device. [PR1415302](#)
- When you create a new rule, a duplicate entry is seen. [PR1415869](#)
- An issue is seen with scheduler configuration. [PR1415924](#)
- SRX Series device does not generate IPS logs in the correct format. [PR1419022](#)
- There are issues with VPN monitoring. [PR1419205](#)
- There are issues with assigning policies to newly discovered devices. [PR1419289](#) and [PR1424996](#)
- After upgrade, an issue is seen with publish jobs. [PR1421731](#)
- There is an issue while deleting the unused address objects. [PR1409740](#)

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>.

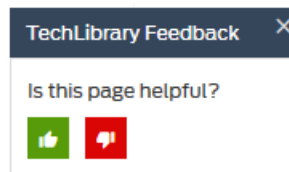
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

April 26, 2019—Revision 1—Junos Space Security Director Release 19.1R1.

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.