

Release Notes: Junos Space Security Director Release 18.2R1

12 July 2018

Contents

- Introduction 2
- Release Notes for Junos Space Security Director 2
 - Supported Managed Devices 2
 - Supported Junos OS Releases 3
 - Supported Policy Enforcer and Sky ATP Releases 4
 - Supported Browsers 5
- Installation and Upgrade Instructions 5
 - Installing and Upgrading Security Director Release 18.2R1 5
 - Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later 6
- Loading Junos OS Schema for SRX Series Releases 7
- Management Scalability 7
- New and Changed Features 8
- Known Behavior 9
- Known Issues 10
- Resolved Issues 11
- Finding More Information 12
- Documentation Feedback 12
- Requesting Technical Support 12
 - Self-Help Online Tools and Resources 13
 - Opening a Case with JTAC 13
- Revision History 13

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 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 Releases 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 18.2R1 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
- SRX4600
- vSRX
- MX240
- MX480
- MX960
- MX2010
- MX2020
- LN1000-V
- LN2600

The supported log collection systems are:

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

Supported Junos OS Releases

- Security Director Release 18.2R1 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
 - 17.4
 - 18.1
- 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 Advanced Threat Prevention (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	Junos 15.1X49-D80 and later
17.1R1	17.1R1	Junos 15.1X49-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)
17.1R2	17.1R2	Junos15.1X49-D80 and later
17.2R1	17.2R1	Junos15.1X49-D110 and later
17.2R2	17.2R2	Junos15.1X49-D110 and later
18.1R1	18.1R1	Junos15.1X49-D110 and later
18.1R2	18.1R2	Junos15.1X49-D110 and later
18.2R1	18.2R1	Junos15.1X49-D110 and later

Supported Browsers

Security Director Release 18.2R1 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 18.2R1 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 18.2R1

Junos Space Security Director Release 18.2R1 is supported only on Junos Space Network Management Platform Release 18.2R1 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 18.2R1, 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 18.2R1 image.



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



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

For more information about installing and upgrading Security Director Release 18.2R1, see [Security Director Installation and Upgrade Guide](#).

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

For distributed deployment, you can add only Log Receiver node in Security Director and cannot add Log Storage 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 is used to login to the JSA console.

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

Loading Junos OS Schema for SRX Series Releases

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

Management Scalability

The following management scalability features are supported on Security Director:

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



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

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

```
#mysql -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 processed concurrently.

Table 2: Supported Firewall Rules per Policy

Number of Device Rules Processed Concurrently	JBoss Node Count	Memory	Platform OpenNMS Function	Log Collector	Hard Disk
5,000–7,000	1	32 GB of RAM	Enabled	Dedicated node	Any
15,000	1	32 GB of RAM	Off or dedicated node	Dedicated node	Any
40,000	2	32 GB of RAM per node	Off or dedicated node	Dedicated node	Any
100,000	2	32 GB of RAM per node	Off or dedicated node	Dedicated node	SSD required



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

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 18.2R1.

- **Logical systems**—You can create logical systems in Security Director. Logical systems for SRX Series devices enable you to partition a single device into secure contexts. Each logical system has its own discrete administrative domain, logical interfaces, routing instances, security firewall, and other security features. To distribute security resources across logical systems, you must create security profiles that specify the type and amount of resources to be allocated to a logical system. Security Director supports logging and reporting for each configured logical system.
- **Installing and upgrading Security Director from Junos Space Store**—Junos Space Store displays the latest compatible versions of the Junos Space applications, which can be installed or upgraded on the current version of Junos Space Network Management Platform. You must configure the Juniper Networks Software download credentials to connect to Junos Space Store. Junos Space accesses the metadata repository hosted by Juniper Networks to discover the available applications and published versions. You can configure the Log Collector and Policy Enforcer components while installing the Security Director application. Junos Space Store does not handle the upgrade of components such as Log Collector and Policy Enforcer. Therefore, refer to the existing method of upgrading the Log Collector and Policy Enforcer components after upgrading the Security Director application.
- **Reports**—Following are the enhancements in Reports:
 - You can generate reports for a selected time range by choosing the Custom Time Range Selection option. For a custom time range, you can select the top records to be displayed in the report for a specific period or time range. You can select the custom time range while creating the log report and bandwidth report. You can also select the custom time range for the Run Now, Preview as PDF, and Send Report options.
 - The Top Talkers report is added. This generates a report on the source IP addresses, with the highest bandwidth usage or maximum sessions, over a specified period.
- **IPsec VPN enhancements**—Following are the enhancements for IPsec VPN:
 - You can now delete multiple IPsec VPNs. While you are deleting the IPsec VPNs, a confirmation message is displayed for redirecting the user to the Security Devices page to delete the IPsec VPNs from the device.
 - You can rename an IPsec VPN while importing the VPN.
 - For a custom proposal, you can specify Diffie-Hellman (DH) Group, Authentication, or Encryption, as selecting all three values is not mandatory.

- You can add a maximum of five IKE addresses on an extranet device when dead peer detection (DPD) is enabled.
- You can create an IPsec VPN with eBGP. The interface type must be numbered and you must set the autonomous system (AS) number.
- **IPv6 support for Juniper Secure Analytics (JSA)**—When you add JSA as a log collector in Security Director, IPv6 addresses are supported when logging nodes are added.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 18.2R1.

- 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 of OpenNMS is changed to Disabled.



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

- The *Enable preview and import device change* option is disabled by default. To enable this option, select **Network Management Platform > Administration > Applications**. Right-click **Security Director** and select **Modify Application Settings**. Under Update Device, select the **Enable preview and import device change** option.
- If you restart the JBoss application servers manually in a six-node setup one-by-one, the Junos Space Network Management Platform and the Security Director user interfaces are launched within 20 minutes, and the devices reconnects to the Junos Space Network Management Platform. You can then edit and publish the policies. When the connection status and the configuration status of all devices are UP and IN SYNC, respectively, click **Update Changes** to update all security-specific configurations or pending services on SRX Series devices.
- To generate reports in the local time zone of the server, you must modify `/etc/sysconfig/clock` to configure the time zone. Changing the time zone on the server by modifying `/etc/localtime` is not sufficient.

- If vSRX VMs in NSX Manager are managed in Security Director Release 17.1R1 and Policy Enforcer Release 17.1R1, then after upgrading to Security Director Release 18.1R1 and Policy Enforcer Release 18.1R1, log in to the Policy Enforcer server by using SSH and run the following command:

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

```
./migrate_devices.sh
```

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

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

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

1. Log in to Policy Enforcer by using SSH.
2. Run the command:

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

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

Known Issues

This section lists the known issues in Security Director Release 18.2R1.

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

- Cluster devices are discovered in different domains. [PR1162407](#)
- After you upgrade Security Director, the custom column is not visible in the firewall rule grid. [PR1256789](#)
- The global search for a dynamic address group does not work as expected. [PR1285893](#)
- 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, several login and logout entries are observed 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 Manager with vSRX VM, you must perform the full probe during the installation of the IDP signature. [PR1291977](#)
- Application firewall OCR fails when the **OVER WRITE** option is selected.
Workaround: You can choose the RE_NAME option and proceed with the rollback or import. [PR1324941](#)
- When you try to add device-specific values for child domains in variable addresses or zones, the changes are not saved in the user interface. [PR1330389](#)
- NAT pool is not shown in the OCR screen if the used address has conflicts. [PR1330392](#)
- While upgrading log collector from Security Director Release 17.2R2 to Security Director Release 18.1R1 using a log collector upgrade script, if log collector reboots during the upgrade, then the Security Director node addition procedure fails. [PR1350341](#)
- Importing variables from CSV is not working as expected. [PR1350890](#)
- Dashboard widget preferences are not retained after upgrading log collector from Security Director Release 17.1R1 to Security Director Release 18.1R1. [PR1350292](#)
- When you invoke the monitoring pages and dashboard widget (Top Compromised Hosts) for the first time, the message **An Error occurred while requesting the data** is displayed. [PR1239956](#)
Workaround: Refresh the browser and select the appropriate realm to show the right data.
- When the integrated Log Collector is installed, searching for address objects in Security Director Release 17.1R1 displays the error message **no data available**. [PR1312104](#)
- The Top Compromised Hosts widget user interface loads with the error message **An error occurred while requesting data**. [PR1370388](#)
- When NAT rule creation exceeds the actual grid visibility range, the user cannot view and edit the new record as the complete grid is grayed out. [PR1369385](#)
Workaround: If create NAT rule grid is grayed out, click the Cancel icon and edit the newly created rule.

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

Resolved Issues

This section lists the issues fixed in Security Director Release 18.2R1.

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

- On the Job Management page, the Date and Time filter for columns does not work as expected. [PR1350906](#)

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 <https://www.juniper.net/documentation/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 <https://www.juniper.net/documentation/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/>
- Open a case online in the CSC Case Management tool: <https://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 <https://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 <https://www.juniper.net/support/requesting-support.html>.

Revision History

12 July , 2018—Junos Space Security Director Release 18.2R1.

Copyright © 2018 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.