

Release Notes: Junos Space Security Director Release 18.1R1

9 December 2019
Revision 4

Contents	Introduction 2
	Release Notes for Junos Space Security Director 2
	Supported Managed Devices 3
	Supported Junos OS Releases 4
	Supported Policy Enforcer and Sky ATP Releases 5
	Supported Browsers 5
	Installation and Upgrade Instructions 6
	Installing and Upgrading Security Director Release 18.1R1 6
	Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later 7
	Loading Junos OS Schema for SRX Series Releases 7
	Management Scalability 8
	New and Changed Features 9
	Known Behavior 9
	Known Issues 11
	Resolved Issues 12
	Finding More Information 13
	Documentation Feedback 14
	Requesting Technical Support 14
	Self-Help Online Tools and Resources 15
	Creating a Service Request with JTAC 15
	Revision History 16

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

- Supported Managed Devices | 3
- Supported Junos OS Releases | 4
- Supported Policy Enforcer and Sky ATP Releases | 5
- Supported Browsers | 5
- Installation and Upgrade Instructions | 6
- Loading Junos OS Schema for SRX Series Releases | 7
- Management Scalability | 8
- New and Changed Features | 9
- Known Behavior | 9
- Known Issues | 11
- Resolved Issues | 12

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 18.1R1 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 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 18.1R1 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
 - 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 5 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	Junos15.1X49-D80 and later
17.1R1	17.1R1	Junos15.1X49-D80 and later
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

Supported Browsers

Security Director Release 18.1R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

Installation and Upgrade Instructions

IN THIS SECTION

- [Installing and Upgrading Security Director Release 18.1R1 | 6](#)
- [Adding Security Director Log Collector Node in Security Director Release 17.2R1 and Later | 7](#)

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

Installing and Upgrading Security Director Release 18.1R1

Junos Space Security Director Release 18.1R1 is supported only on Junos Space Network Management Platform Release 18.1R1 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 18.1R1, 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 18.1R1 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 18.1R1, 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 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 7](#).

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 -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.

Table 2 on page 8 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

Table 2: Supported Firewall Rules per Policy (continued)

Number of Device Rules Processed Concurrently	JBoss Node Count	Memory	Platform OpenNMS Function	Log Collector	Hard Disk
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

There are no new features or enhancements to existing features in Junos Space Security Director Release 18.1R1.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 18.1R1.

- 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 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 18.1R1.

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

- Grid column filter does not work for Internet Explorer 11. [PR1161079](#)
- 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](#)
- You must manually synchronize NSX with the vCenter server to view the latest restart or power off status. [PR1285312](#)
- The global search for a dynamic address group does not work as expected. [PR1285893](#)
- Any Service Groups notification sent from NSX to Security Director triggers an RPC update job for each vSRX device, instead of a single job with all the related vSRX devices. [PR1288407](#)
- If there is a change in the login password of NSX Manager, vCenter, or Junos Space, then use the Edit NSX Manager page in Security Director to modify the login password information. Otherwise, synchronization of NSX Manager and dynamic address groups update fails. [PR1291965](#)
- If NSX is integrated with Security Director, 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](#)
- 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 instances:

- Modify the description of the service group when the services or Policy Enforcer VM is down.
- Log in to the vSRX device by using the SSH command and execute the following command:
request security dynamic-address update address-name *Dynamic-Address-Name*
- 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](#)
- In the Job Management page, Date and Time filter for columns is not working as expected. [PR1350906](#)
- When an SRX Series device is managed directly by Juniper Sky ATP for Advanced Threat Prevention, and is used in Security Director without integrating Policy Enforcer, then Security Director should not manage the threat prevention configuration. For example, security-intelligence policy and advanced-anti-malware policy. However, currently Security Director manages threat prevention configuration and tries to modify the configuration incorrectly. [PR1403904](#)

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

Resolved Issues

This section lists the issues fixed in Security Director Release 18.1R1.

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

- When a user tries to log in to Security Director after password expiry, the myprofile change password pop-up is displayed to change the password. Security Director does not display user password expiry notification before the password expires. [PR1324507](#)
- In the UTM policy page, after clicking on filter icon, filter fields are not visible for all the columns to provide input for column search. [PR1334852](#)
- When one device is selected and updated in Security Director, it triggers an update on all devices. [PR1341964](#)
- In Security Director Release 17.2R1, invalid cron task entry is seen, for example, `5 1 * * * sh /etc/init.d/packetpurger start`. [PR1344084](#)
- Unable to import NAT policies using NSM migration tool and XDIFF. [PR1344829](#)
- Unable to rollback security policy. The *Error please retry* message is displayed. [PR1346791](#)
- The metadata feed server requires manual restart of the `secmgt-skyatp-proxy` service when Security Director is installed or upgraded. [PR1330400](#)
- In the Threat Prevention Policy page, triggering a rule analysis may throw an error like this: An error occurred while triggering the rule analysis. Please try again later. [PR1331439](#)
- When you install the Junos OS Release 17.4 schema on a Junos space server, publish or update operations might fail on SRX Series platforms when UTM custom objects are present as part of the configuration. [PR1330089](#)
- After upgrading from Junos Space Security Director Release 15.1 to Junos Space Security Director Release 17.1, scheduler object behavior changed. [PR1351659](#)
- IDP packet capture feature is not stable in Junos Space Security Director Release 17.2R2. [PR1352209](#)

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>.

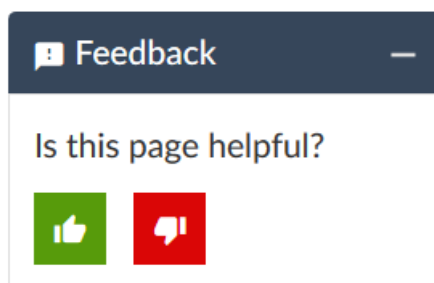
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: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

3 May, 2018—Revision 1, Junos Space Security Director Release 18.1R1

31 July, 2018—Revision 2, Junos Space Security Director Release 18.1R1

28 January, 2019—Revision 3, Junos Space Security Director Release 18.1R1

9 December, 2019—Revision 4, Junos Space Security Director Release 18.1R1

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.