Release Notes: Junos Space Security Director Release 18.4R1

9 December 2019
Revision 3

Contents

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, 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.

Release Notes for Junos Space Security Director

IN THIS SECTION

Supported Managed Devices

Security Director Release 18.4R1 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 18.4R1 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
  - 18.2
  - 18.3
- SRX Series devices require Junos OS Release 12.1 or later to synchronize the Security Director description field with the device.
- The logical systems feature is supported on devices running Junos OS Release 11.4 or later.

NOTE: Before you can manage an SRX Series device by using Security Director, we recommend that you have the exact matching Junos OS schema installed on the Junos Space Network Management Platform. If there is a mismatch, a warning message is displayed during the publish preview workflow.

Supported Policy Enforcer and Juniper Sky ATP Releases

Table 1 on page 5 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 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
18.1R2	18.1R2	Junos15.1X49-D110 and later
18.2R1	18.2R1	Junos15.1X49-D110 and later
18.3R1	18.3R1	Junos15.1X49-D110 and later
18.4R1	18.4R1	Junos15.1X49-D110 and later

Supported Browsers

Security Director Release 18.4R1 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 18.4R1

Junos Space Security Director Release 18.4R1 is supported only on Junos Space Network Management Platform Release 18.4R1 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 18.4R1, 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 18.4R1 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 events per second (eps).

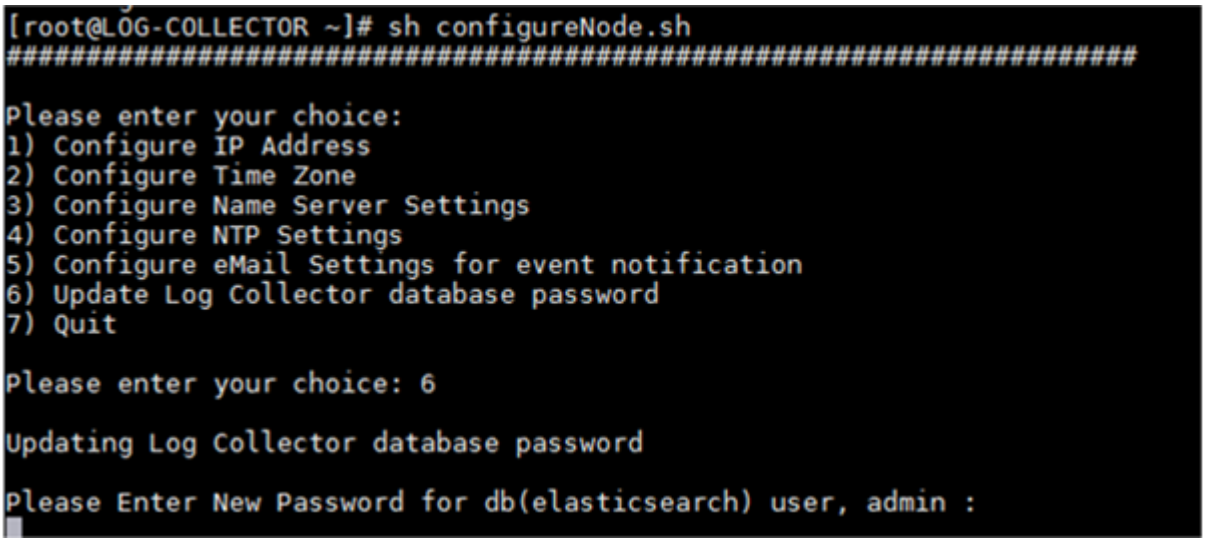
For more information about installing and upgrading Security Director Release 18.4R1, see Security Director Installation and Upgrade Guide.

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



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 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 9 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 and Policy Enforcer Release 18.4R1.

- **Usability enhancements**—Following are the usability enhancements:
  - In the event viewer, you can perform complex filtering using AND and OR logical operators, and brackets to group the search tokens. In the search text box, an icon is displayed and when you hover over the icon, it displays an example filter condition. When you start entering the search string, the icon indicates whether the filter string is valid or not.
  - In the event viewer, while entering search criteria, when you press the Backspace key at any point in time, only one character is deleted instead of the whole search token.
  - On the Application Signature page, when you click the filter icon, a drop-down list is available for category and subcategory columns. You can select any value and the grid is reloaded with the filtered category and subcategory.
- **Unified firewall policies**—Unified policies are security policies that enable you to use the dynamic applications as match conditions as part of the existing 5-tuple or 6-tuple (5-tuple with user firewall)

match conditions. Unified policies are used to detect the application changes over time. A unified policy leverages the information from AppID to match the application and take action as specified in the policy. In a unified policy configuration, you can use a predefined dynamic application (from the application identification signature package) or a user-defined custom application as a match condition.

The traditional firewall policies are the standard policies and an option is provided to convert the standard firewall policies to the unified firewall policies.

- **Default SSL proxy profiles—**You can configure a default SSL proxy profile. The initial policy lookup phase occurs prior to identifying a dynamic application. If there are multiple policies present in the potential policy list that contain different SSL proxy profiles, then the SRX Series device applies the default profile to manage conflicts until a suitable match is established.
- **Show duplicate objects—**You can view duplicate objects on the Show Duplicates page from parent domain and subdomains. You can merge shared objects from parent domain to subdomain and vice versa. You can delete objects only from the current domain. If you select multiple objects from across the domains, then the delete option is disabled. This is supported for shared objects and policies like addresses, services, zone sets, NAT pools, and NAT port sets.
- **TCP session option—**The TCP session option Window Scale is supported. You can enable this option to increase the network transmission speed.
- **Policy enforcement for public cloud with Microsoft Azure—**Policy Enforcer integrates with Microsoft Azure for workload discovery, allowing enterprises to configure a dynamic workload metadata-based policy that is always kept up-to-date without requiring security administrators to manually update the VM inventory in Security Director. In addition, Policy Enforcer updates Microsoft Azure Security Groups for the virtual machines identified as infected with malware or command and control activity, mitigating lateral threats inside the network.
- **Support of IPv6 feeds—**Policy Enforcer extends supports for IPv6 addresses for Command and Control (C&C), Whitelist and Blacklist Juniper Sky ATP feeds. With this enhancement, users can leverage both IPv4 and IPv6 based rich set of curated threat feeds from Juniper Sky ATP to proactively remediate threat in their environment. The custom feed and infected host do not support IPv6 feeds.
- **MX Series routers as perimeter devices—**In addition to SRX Series firewalls, Policy Enforcer now allows MX Series routers to be defined as perimeter devices within secure fabric, to support environments that deploy MX Series routers at the network edge. Policy Enforcer adds the ability to push C&C and GeoIP feeds to these MX Series devices allowing users to protect their network by proactively blocking outbound C&C communication.
- **Support of 256 DAGs per SRX Series device—**Policy Enforcer supports 256 dynamic address groups (DAGs) per SRX Series device running Junos OS Release 15.1X49-D160 and later. This provides users with greater flexibility and scale in using DAGs to define their firewall policy.

> **NOTE:** The maximum number of dynamic address groups supported by Policy Enforcer is 1000 with 16-GB RAM and 4 CPUs.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 18.4R1.

- 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 reconnect 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.

- In the case of coexistence setup where other applications are installed in Junos Space along with Security Director, the JBoss PermSize must be increased from 512m to 1024m in **/usr/local/jboss/domain/configuration/host.xml.slave** file. Under <jvm name="platform">, change the following in <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 18.4R1.

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

- After NAT policy rules are automatically grouped, the **Policy is unlocked** message is displayed for a fraction of a second. PR1390075
- JSA system logs are not parsing properly on the Application Visibility, User Visibility, and Source IP Visibility pages. PR1372721
- Search or filter in policy rules are not working. PR1398589
- Data is not displayed on the firewall, IPS, and NAT Select Policy Sequence pages. PR1396651
- Results are not shown as expected when the user navigates from Threatmap to Event Viewer. PR1403943
- Junos Space Security Director allows users to configure services other than junos-defaults, which is not supported when dynamic application value is "any" or "specific". PR1406932

Workaround: Do not configure services other than junos-defaults if dynamic application values are “any" or "specific".

- Update fails for unified policies when an SSL proxy profile is set as global in a device, but is not used in any policy for that device. PR1407389
- Rules are unavailable when Add Rule After and Add Rule Before actions are performed. PR1401111

  Workaround: Select the rule and click the newly added rule and enter the details.
- Invalid characters are displayed in the filter bar, when a saved custom complex filter is applied or if a predefined filter contains space. PR1405584
- Unsupported devices can also be assigned under unified policies. PR1407283
- 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 and Policy Enforcer Release 18.4R1.

For the most complete and latest information about resolved Security Director and Policy Enforcer defects, use the Juniper Networks online Junos Problem Report Search application.

- Domain-specific queries do not list policies in a specified domain. PR1341221
- Device managed status remains as "Device Changed" even after performing an update from Junos Space Security Director. PR1345764
- Unable to change sequence number of rules in a policy in Junos Space Security Director Releases 18.2 and 18.3. PR1396770
- Firewall policy takes more time to load in Junos Space Security Director Release 18.3 than in 18.2. PR1402164
- Report generation fails for scheduled reports. PR1352984
- Address or service objects search does not work after upgrading to Junos Space Security Director Release 17.2. PR1358229
- When you click firewall policies, Security Director does not respond. PR1395548
- After selecting Devices>Security devices>Modify configuration>Security Logging>Stream, clicking Log Collector or +, does not add Log collector entry as stream details. PR1397200

- An error message is displayed when user tries to add a VPN in Security Director for a specific domain by clicking Configure>IPSec VPN. PR1399939
- During import, Security Director is creating a new object for any address group instead of using the matching object in the global domain that NSM is using. PR1340106
- After upgrading Security Director from Junos Space Security Director Release 18.1R2 to 18.2, Log Director agent does not upgrade. PR1382664
- Error message is displayed while importing VPN to Junos Space Security Director. PR1400561
- When the same logical system (LSYS) name is used across different SRX Series firewalls, updating the group firewall policy might not push changes to a few LSYS devices. However, the update job will be shown as successful and with an empty configuration committed to affected LSYS devices. PR1400337
- When deleting an extranet device, which is currently used in the VPN, the extranet device is removed, but the corresponding preview and publish jobs fail. PR1397976
- Update VPN with proposal encryption-algorithm aes-256-gcm fails. PR1324529
- After upgrading to Junos Space Security Director Release 18.3, publish and update tasks are taking more time. PR1397828
- Junos Space Security Director Release 18.3 fails to import firewall using customer application signatures. PR1406489
- When NAT rule creation exceeds the actual grid visibility range, the user cannot view and edit the new record because the complete grid is unavailable. PR1369385

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.

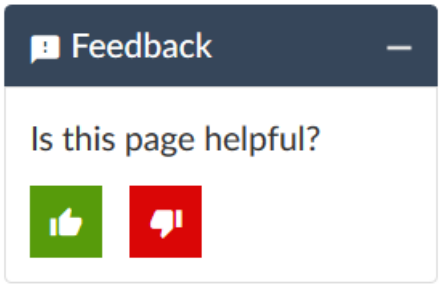
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at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

19 December, 2018—Revision 1—Junos Space Security Director Release 18.4R1

28 January, 2019—Revision 2—Junos Space Security Director Release 18.4R1

9 December, 2019—Revision 3—Junos Space Security Director Release 18.4R1