

Junos Space Security Director Release 22.3R1

Published
2025-03-26

RELEASE

Table of Contents

[Introduction](#)

[New and Changed Features](#)

[Supported Managed Devices](#)

[Supported Log Collection Systems](#)

[Supported Junos OS Releases](#)

[Supported Policy Enforcer and Juniper® Advanced Threat Prevention \(ATP\) Cloud Releases](#)

[Supported Browsers](#)

[Installation and Upgrade Instructions](#)

[Loading Junos OS Schema for SRX Series Firewalls](#)

[DMI Schema Compatibility for Junos OS Service Releases](#)

[Management Scalability](#)

[Known Behavior](#)

[Known Issues](#)

[Resolved Issues](#)

[Hot Patch Releases](#)

[Finding More Information](#)

[Revision History](#)

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 AppFW.



NOTE: You need IPS and AppFW licenses to push IPS policies and AppFW signatures to a device.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 22.3R1.

- **DNS sinkhole**—Starting in Junos Space Security Director Release 22.3R1, we support DNS sinkhole. A DNS Sinkhole enables you to reject or resolve DNS requests for disallowed domains.
- **Enable and disable host inbound traffic in IPsec VPN**—Starting in Junos Space Security Director Release 22.3R1, we've provided a global option in Junos Space Network Management Platform for Security Director under Administration >Applications >Security Director >Modify Application Settings to enable or disable the host inbound configurations.

When you enable the option, the host inbound services are disabled and are not displayed in the configuration preview.

For new features and enhancements in Policy Enforcer, see [Policy Enforcer Release Notes](#).

Supported Managed Devices

You can use Security Director Release 22.3R1 to manage the following devices:

- SRX100
- SRX110
- SRX210

- SRX220
- SRX240
- SRX240H
- SRX300
- SRX320
- SRX320-POE
- SRX340
- SRX345
- SRX380
- SRX550
- SRX550M
- SRX650
- SRX1400
- SRX1500
- SRX3400
- SRX3600
- SRX4100
- SRX4200
- SRX5400
- SRX5600
- SRX5800
- SRX4600
- vSRX
- MX240
- MX480
- MX960

- MX2010
- MX2020
- LN1000-V
- LN2600

Supported Log Collection Systems

The following log collection systems are supported:

- Log Collector 22.3 (Security Director Insights VM)
- Juniper Networks® Secure Analytics (JSA) Series Virtual Appliance as Log Collector on JSA Release 2014.8.R4 and later
- QRadar as Log Collector on QRadar Release 7.2.8 and later



NOTE: Starting in Security Director Release 20.2R1 onward, we're not supporting standalone Log Collector and Integrated Log Collector 20.1R1.

Supported Junos OS Releases

Security Director Release 22.3R1 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
- 18.1R2.6
- 18.2
- 18.2R3.4
- 18.3
- 18.4
- 18.4R3.3
- 19.1
- 19.2
- 19.3
- 19.4
- 20.1
- 20.2
- 20.3
- 20.4
- 21.1
- 21.2
- 21.3
- 21.4

- 22.1
- 22.2

SRX Series Firewalls 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 the device that run Junos OS Release 11.4 or later.



NOTE: NOTE: To manage an SRX Series Firewall by using Security Director, we recommend that you 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® Advanced Threat Prevention (ATP) Cloud Releases

Table 1 on page 5 shows the supported Policy Enforcer and Juniper ATP Cloud releases.

Table 1: Table 1: Supported Policy Enforcer and Juniper ATP Cloud Releases

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud Supported Devices)
19.3R1	19.3R1	Junos OS Release 15.1X49-D120 and later
19.4R1	19.4R1	Junos OS Release 15.1X49-D120 and later
20.1R1	20.1R1	Junos OS Release 15.1X49-D120 and later
20.3R1	20.3R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later

Table 1: Table 1: Supported Policy Enforcer and Juniper ATP Cloud Releases (Continued)

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud Supported Devices)
21.1R1	21.1R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
21.2R1	21.2R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
21.3R1	21.3R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
22.1R1	22.1R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
22.2R1	22.2R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later
22.3R1	22.3R1	Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later



NOTE: For Policy Enforcer details, see [Policy Enforcer Release Notes](#).

Supported Browsers

Security Director Release 22.3R1 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 22.3R1](#) | 7

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

Installing and Upgrading Security Director Release 22.3R1

Junos Space Security Director Release 22.3R1 is supported only on Junos Space Network Management Platform Release 22.3R1 that can run on the following devices:

- Junos Space virtual appliance
- KVM server installed on CentOS Release 7.2.1511

For more information about installing and upgrading Security Director and Log Collector 22.3 (Security Director Insights VM), see [Security Director Installation and Upgrade Guide](#).

Loading Junos OS Schema for SRX Series Firewalls

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

DMI Schema Compatibility for Junos OS Service Releases

The following tables explain how the Junos Space Network Management Platform chooses Device Management Interface (DMI) schemas for devices running Junos OS Service Releases.

If a Junos OS Service Release is installed on your device with a major release version of a DMI schema installed on Junos Space Network Management Platform, then Junos Space chooses the latest corresponding major release of DMI schemas, as shown in [Table 2 on page 8](#).

Table 2: Device with Service Release and Junos Space with FRS Release

Junos OS Version on the Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.4R1.8 18.3R1.1 18.2R1.1	18.2R1.1	18.4R1.8

If 18.4R1.8 version is not available, then Junos Space chooses the nearest lower version of DMI schema installed.

Junos OS Version on the Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If a Junos OS Service Release is installed on your device without a matching DMI schema version in Junos Space Network Management Platform, then Junos Space chooses the nearest lower version of DMI schema installed, as shown in [Table 3 on page 9](#).

Table 3: Device with Service Release and Junos Space without matching DMI Schema

Junos OS Version on the Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.5R1.1 18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If more than one version of the DMI schemas are installed in Junos Space Platform for a single Junos OS Service Release version, Junos Space chooses the latest version of the DMI schema, as shown in [Table 4 on page 9](#).

Table 4: Device with Service Release and Junos Space with more than one DMI Schemas

Junos OS Version on the Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.4R1.8 18.4R1.7 18.4R1.6 18.3R1.1	18.3R1.1	18.4R1.8

If 18.4R1.x versions are not available, then Junos Space chooses the nearest lower version of DMI schema installed.

Junos OS Version on the Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1-S1	18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

If a Junos OS Service Release is installed on your device without a corresponding DMI schema version in Junos Space Network Management Platform, then Junos Space chooses the nearest lower version of DMI schema installed, as shown in [Table 5 on page 10](#).

Table 5: Device with Service Release and Junos Space without more DMI Schemas

Junos OS Version on Device	Junos Space DMI Schemas Installed	Junos Space Default Version	Junos Space Version Chosen for Platform
18.4R1.1	18.5R1.1 18.3R1.1 18.2R1.1	18.2R1.1	18.3R1.1

For information about Junos OS compatibility, see [Junos OS Releases Supported in Junos Space Network Management Platform](#).

Management Scalability

The following management scalability features are supported in Junos Space 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 Firewall 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 Firewall with a six-node Junos Space fabric. In a setup with 15,000 SRX Series Firewalls, 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 -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.



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

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 22.3R1.

- You can generate a temporary password in Security Director under **Administration >Users & Roles >Users** by either creating a user or editing a user.

Make sure you check the **Generate** check box on the **Create User** or the **Edit User** window to create a temporary password.

After you generate the temporary password in Security Director, you must first log in through Junos Space Network Management Platform GUI and not Security Director GUI.

- To discover the tenant devices in Security Director Release 21.2R1, we recommend the schema to be greater than or equal to 20.1R1. You must install the schema before Security Director discovers a tenant device.
- If you configure VPN in Security Director Release earlier to 19.4R1 and upgrade Security Director to Release 20.1R1 and later, IKE ID is displayed blank if IKE ID is defined as Default.
- Security Director does not generate CLIs for deletion if a VPN is already configured in the device and the same device is used for creating another VPN from Security Director.
- In Security Director Release 20.1R1 and later, you must configure a tunnel IP address for dynamic routing protocols. In Security Director Release 19.4R1 and earlier, if you configure VPN as unnumbered with a dynamic routing protocol, you are prompted to provide a tunnel IP address while editing the VPN after upgrading to Security Director Release 20.1R1 and later.
- After upgrade, you cannot edit profiles with predefined proposals because the profiles in Security Director Release 20.1R1 and later support only custom proposals.
- In Security Director Release 19.4R1 and earlier, if you configure a VPN with static routing or a traffic selector with protected network as the zone or interface, you must perform the following tasks:

1. Before you upgrade to Security Director Release 20.1R1 and later, update the configuration on the device, and delete the VPN policy from Security Director.
2. After you upgrade, import the VPN configuration.



NOTE: In Security Director Release 20.1R1 and later, we support only address objects in protected networks for static routing and traffic selector.

- You must enable the **Enable preview and import device change** option, which is disabled by default:
 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, the Junos Space Network Management Platform and Security Director UI 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 Firewalls.
- 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 reports 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 20.3R1 and Policy Enforcer Release 20.3R1, we recommend that you migrate the existing vSRX VMs in NSX Manager from Policy Enforcer Release 17.1R1 to Release 20.3R1.

To migrate the existing vSRX VMs:

1. Log in to the Policy Enforcer server by using SSH.
2. Run the following commands:

```
cd /var/lib/nsxmicro
./migrate_devices.sh
```

- 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 fetches 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 Network Management Platform 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"/>
```

- When you import addresses through CSV, a new address object is created by appending `a_1` to the address object name if the address object already exists in Security Director.

Knowns Issues

This section lists the known issues in Junos Space Security Director Release 22.3R1.

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

- A policy analysis report with more than 20000 rules cannot be generated. [PR1708393](#)
- SSL certificate error is displayed while analyzing threat prevention policy. [PR1648734](#)
- When you use Security Director Insights as a log collector, device selection on Monitor page does not work when a logical system or a tenant system device is selected. [PR1621052](#)
- Security Director displays device lookup failed error during preview. [PR1617742](#)

Workaround:

1. Move the device to RMA state. Navigate to Junos Space Network Management Platform. Select **Devices > Device Management**. Select a device, right-click and select **Device Operations** and then select **Put in RMA State**.

2. Reactivate the device from RMA state. Navigate to Junos Space Network Management Platform. Select **Devices >Device Management**. Select a device, right-click and select **Device Operations** and then select **Reactivate from RMA**.
- Primary cluster displays the status as DOWN while both devices in the device cluster displays the status as UP. [PR1616993](#)

Workaround:

1. Move the device to RMA state. Navigate to Junos Space Network Management Platform. Select **Devices >Device Management**. Select a device, right-click and select **Device Operations** and then select **Put in RMA State**.
 2. Reactivate the device from RMA state. Navigate to Junos Space Network Management Platform. Select **Devices >Device Management**. Select a device, right-click and select **Device Operations** and then select **Reactivate from RMA**.
- Security Director does not clear uncommitted logical system or tenant system device management configuration in case of job failure, which causes subsequent updates to fail. You must clear the configuration from space node before proceeding with next update. [PR1603146](#)

Workaround: Navigate to **Junos Space Network Management Platform >Devices >Device Management >Modify Configuration >Deploy >Reject Changes**.

- Security Director fails to import policies when custom dynamic-applications are configured at root-level and referred in logical system or tenant system policies. [PR1602677](#)
- An icon showing OOB changes is seen for firewall and IPS policies, although the corresponding policy changes are not made on the device. [PR1484953](#)

Workaround: Clear the OOB icon on the policies when changes are not made on the device.

Navigate to the corresponding policy, and right-click the policy. Select **View Device Policy Changes** and reject all changes, and then click **OK**.

- Deployment of cipher list CLI works only when you perform Save, or Save and Deploy. [PR1485949](#)

Workaround: You must save or deploy the selected Cipher list before you view the preview changes.

- An object conflict occurs when you import Web filter profiles with duplicate names, although the values are the same. [PR1420341](#)

Workaround: Select either **Overwrite with Imported Value** or **Keep Existing Object** to avoid duplicate objects.

- Junos Space Security Director does not support routing instances and proxy profiles in an antivirus pattern update for the Content Security default configuration. [PR1462331](#)

- When you import OOB changes to a logical system device, a job is created for the root device along with the logical system device, although changes are made only in the logical system device. [PR1448667](#)

- Import fails when a device is imported only with Content Security custom objects without a Content Security policy. [PR1447779](#)

Workaround: Delete the Content Security custom objects if they are not used in a policy, or assign a Content Security policy.

- 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](#)
- A policy analysis report with a large number of rules cannot be generated. [PR1418125](#)
- When a column filter is used, the **Deselect all** and **Clear all** options do not clear selected items occasionally. [PR1424112](#)
- The Show Unused option is not available for URL categories. [PR1431345](#)
- Restart of a single JBoss node does not recover the system even if the issue is present on a single node. [PR1478804](#)

Workaround: Restart all JBoss nodes.

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

Resolved Issues

This section lists the issues fixed in Junos Space Security Director 22.3R1:

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

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

Hot Patch Releases

IN THIS SECTION

- [Installation Instructions | 16](#)
- [Resolved Issues in the Hot Patches | 17](#)

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 22.3R1 hot patch.

During hot patch installation, the script performs the following operations:

- Blocks the device communication.
- Stops JBoss, JBoss Domain Controller (JBoss-dc), and jmp-watchdog services.
- Backs up existing configuration files and EAR files.
- Updates the Red Hat Package Manager (RPM) files.
- Restarts the watchdog process, which restarts JBoss and JBoss-dc services.
- Unblocks device communication after restarting the watchdog process for device load balancing.



NOTE: You must install the hot patch on Security Director Release 22.3R1 or on any previously installed hot patch. The hot patch installer backs up all the files which are modified or replaced during hot patch installation.

Installation Instructions

Perform the following steps in the CLI of the JBoss-VIP node only:

1. Download the Security Director 22.3R1 Patch vX from the [download site](#).

Here, X is the hot patch version. For example, v1, v2, and so on.

2. Copy the SD-22.3R1-hotpatch-vX.tgz file to the /home/admin location of the VIP node.

3. Verify the checksum of the hot patch for data integrity:

```
md5sum SD-22.3R1-hotpatch-vX.tgz.
```

4. Extract the SD-22.3R1-hotpatch-vX.tgz file:

```
tar -zxvf SD-22.3R1-hotpatch-vX.tgz
```

5. Change the directory to SD-22.3R1-hotpatch-vX.

```
cd SD-22.3R1-hotpatch-vX
```

6. Execute the patchme.sh script from the SD-22.3R1-hotpatch-vX folder:

```
sh patchme.sh
```

The script detects whether the deployment is a standalone deployment or a cluster deployment and installs the patch accordingly.

A marker file, /etc/.SD-22.3R1-hotpatch-vX, is created with the list of RPM details in the hot patch.



NOTE:

- We recommend that you install the latest available hot-patch version, which is the cumulative patch.

Resolved Issues in the Hot Patches

Table 6 on page 17 lists the resolved issues in Security Director Release 22.3R1 hot patch.

Table 6: Table 6: Resolved Issues in the Hot Patch

PR	Description	Hot Patch Version
PR1664682	Geographical location report shows incorrect data in Security Director.	V1
PR1679106	Security Director updates the database with incorrect cyclic service group.	V1

Table 6: Table 6: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1701645	SRX Series Firewalls do not show any data in the IPS report with log event IDP_ATTACK_LOG_EVENT_LS.	V1
PR1702216	The application visibility feature does not show the log data for last eight hours and earlier.	V1
PR1703135	User is unable to search for an object in Security Director even when the objects exist in Shared Objects.	V1
PR1707744	When you try to preview, publish, or update configuration in Security Director, it fails with an error.	V1
PR1709345	The MTU is not visible during the edit workflow, when provided as default.	V1
PR1709403	Security Director fails to import the policy zip files with more than 20000 rules.	V1
PR1710418	Security Director fails to publish the SRX Series Firewall cluster policy with Content Security is not available in the device error message.	V1
PR1711219	Security Director fails to update the Content Security policies in SRX Series Firewalls and vSRX Series Firewalls.	V1

Table 6: Table 6: Resolved Issues in the Hot Patch (*Continued*)

PR	Description	Hot Patch Version
PR1719887	Unexpected changes for Content Security are visible in the preview after upgrading to Junos Space Network Management Platform release 22.3R1.	V1



NOTE: If the hot patch contains a UI fix, then you must clear the Web browser's cache to reflect the latest changes.

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/>.

Revision History

22 December, 2022—Revision 1—Junos Space Security Director Release 22.3R1.

8 May, 2023—Revision 2—Junos Space Security Director Release 22.3R1 Hot Patch V1.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the 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. Copyright © 2025 Juniper Networks, Inc. All rights reserved.