# Release Notes

Published

2025-11-06

## Junos Space Security Director Release Notes 24.1



Juniper Business Use Only




Juniper Business Use Only

# Table of Contents





Juniper Business Use Only

# 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

## New and Changed Features in Junos Space Security Director Release 24.1R1

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 24.1R1.

- Support for the SRX1600 firewall—Starting in Junos Space Security Director Release Hot Patch 23.1R1, we provide support for the SRX1600.
- Support for the SRX2300 firewall—Starting in Junos Space Security Director Release Hot Patch 23.1R1, we provide support for the SRX2300.
- We've upgraded the Junos Space host Linux OS to Rocky Linux 9.2. For more details on the upgrade, see Upgrading to Junos Space Network Management Platform Release 24.1R1.
- Starting in Junos Space Security Director Release 24.1R1, we've upgraded to MySQL v8.
- DNS Filter Support—Starting in Junos Space Security Director Release 24.1R1, we've provided DNS Filter support to the Firewall Policy, where you can create, view, modify, delete, or clone a filter. You can also assign or unassign a device to a filter, assign a DNS filter to a domain, publish and update a DNS Filter configuration. For more details on the DNS Filter support, see Firewall policy-DNS Filter.
- Standalone Policy Enforcer is not supported—Starting in Junos Space Security Director Release 24.1R1, you cannot use standalone Policy Enforcer. You'll need to migrate to Policy Enforcer running on Security Director Insights 24.1R1. For more details on the migration of Policy Enforcer, see Migrate Policy Enforcer Release 23.1R1 to Policy Enforcer Release 24.1R1.



Juniper Business Use Only

**NOTE**:

- Security Director Release 24.1R1 supports only non-FIPS mode
- Security Director Release 24.1R2 supports Security Director Insights Release 24.1 R1 and above versions
- Security Director 24.1R2 Hot Patch v1 is mandatory for Security Director Insights Policy Enforcer 24.1R1 to operate with Security Director Release 24.1R2.

# New and Changed Features in Junos Space Security Director Release 24.1R3

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 24.1R3.

- Support for the SRX4700 Firewall—Starting in Junos Space Security Director Release 24.1R3, we provide support for SRX4700.

  **NOTE**: High Availability is not supported on Junos Space Security Director for SRX4700 firewall.

- Deprecated Signature Management for Firewall Policies—Starting in Junos Space Security Director Release 24.1R3, we've provided the Aggregate And Update Lsys Tsys configuration checkbox in Junos Space Network Management Platform to manage the deprecated signatures associated with firewall policies.

  For details, see Publishing Policies.

- Starting in Junos Space Security Director Release 24.1R3, we've upgraded Elasticsearch to version 6.8.17.



Juniper Business Use Only

# New and Changed Features in Junos Space Security Director Release 24.1R4

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 24.1R4.

Junos Space Security Director supports sharing of point-to-point st0 logical interface when you run IPsec VPN service using the IKED process to provide a migration path from the kmd process. You can configure multiple VPNs objects to share a point-to-point st0 interface.

# New and Changed Features in Junos Space Security Director Release 24.1R5

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 24.1R5.

Modify traffic selectors for route-based VPNs—You can use the Edit Traffic Selector option in the GUI to enhance route-based VPN flexibility. Define, enable, or disable traffic selectors based on local and remote address pairs to control permitted tunnel traffic. Apply traffic selectors to Site-to-Site, Hub-and-Spoke (establish all peers), Full Mesh, and Remote Access VPNs (secure client). Ensure the selected device is managed, protected networks are assigned, and the device routing topology is set to traffic selector.

# Supported Managed Devices

You can use Security Director Release 24.1 to manage the following devices:

- SRX300
- SRX320
- SRX320-POE
- SRX340
- SRX345
- SRX380
- SRX1500



Juniper Business Use Only

- SRX4100
- SRX4200
- SRX5400
- SRX5600
- SRX5800
- SRX4600
- vSRX
- MX240
- MX480
- MX960
- MX2010
- MX2020

# Supported Log Collection Systems

The following log collection systems are supported:

- Log Collector 24.1 (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 21.1R1 onward, we're not supporting standalone Log Collector and Integrated Log Collector.

# Supported Junos OS Releases

Security Director Release 24.1 supports the following Junos OS releases:

- 19.3
- 19.4



Juniper Business Use Only

- 20.1
- 20.2
- 20.3
- 20.4
- 21.1
- 21.2R3-S2
- 21.3
- 21.4
- 22.1
- 22.2
- 23.1



Juniper Business Use Only

- 23.2
- 24.4R1

**NOTE**: EoL Junos releases might continue to work as the support is not removed. However, we have not tested.

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 devices that run Junos OS Release 11.4 or later.

**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: Supported Policy Enforcer and Juniper ATP Cloud Releases**

| Security Director Release | Compatible Policy Enforcer Release | Junos OS Release (Juniper ATP Cloud Supported Devices) |
|---|---|---|
| 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 |



Juniper Business Use Only

**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) |
|---|---|---|
| 22.3R1 | 22.3R1 | Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later |
| 23.1R1 | 23.1R1 | Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later |
| 24.1R1 | 24.1R1 | Junos OS Release 15.1X49-D120 or Junos OS Release 17.3R1 and later |

**NOTE**: Starting in Junos Space Security Director Release 24.1R1, you cannot use standalone Policy Enforcer. You'll need to migrate to Policy Enforcer running on Security Director Insights 24.1R1.

# Supported Browsers

Security Director Release 24.1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome



Juniper Business Use Only

# Installation and Upgrade Instructions

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

# Supported Software Versions

Junos Space Security Director is supported only on specific software versions mentioned in Table 2 on page 7.

**Table 2: Supported Software Versions**

| Security Director Version | Compatible with Junos Space Network Management Platform Version | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | 24.1R1 Hot Patch v1 | 24.1R1 Hot Patch v2 | 24.1R2 | 24.1R2 Hot Patch v1 | 24.1R3 | 24.1R3 Hot Patch v1 | 24.1R4 | 24.1R4 Hot Patch v1 | 24.1R5 |
| Security Director 24.1 R1 | Yes | | | | | | | | |
| Security Director 24.1 R2 | Yes | Yes | | | | | | | |
| Security Director 24.1 R2 Hot Patch v1 | Yes | Yes | | | | | | | |



Juniper Business Use Only

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Security Director 24.1 R3 | | Yes | Yes | | | | | | |

**Table 2: Supported Software Versions *(Continued)***

| Security Director Version | | Compatible with Junos Space Network Management Platform Version | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Security Director 24.1 R3 Hot Patch v1 | | | Yes | | Yes | | | |
| Security Director 24.1 R3 Hot Patch v2 | | | | Yes | Yes | | | |
| Security Director 24.1 R3 Hot Patch v3 | | | | | Yes | Yes | | |
| Security Director 24.1 R3 Hot Patch v4 | | | | | Yes | Yes | | |
| Security Director 24.1 R4 | | | | | | | Yes | |
| Security Director 24.1 R4 Hot Patch v1 | | | | | | | Yes | Yes |



Juniper Business Use Only

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Security Director 24.1 R5 | | | | | | | Yes | Yes |

# Installing and Upgrading Security Director Release 24.1R1

**CAUTION**: You must install the Junos Space 24.1R1 hot patch v1 before installing or upgrading Junos Space Security Director application.

Junos Space Security Director Release 24.1R1 is supported only on Junos Space Network Management Platform Release 24.1R1 that can run on the following devices:

- Junos Space virtual appliance
- KVM server



Juniper Business Use Only

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

# Installing and Upgrading Security Director Release 24.1R2

**CAUTION**: You must install the Junos Space 24.1R1 hot patch v2 before installing or upgrading Junos Space Security Director application.

**NOTE**: Junos Space Network Management Platform Release 24.1R2 is qualified and is compatible with Security Director Release 24.1R2.

Junos Space Security Director Release 24.1R2 is supported only on Junos Space Network Management Platform Release 24.1R1 that can run on the following devices:

- Junos Space virtual appliance
- KVM server

Starting in Junos Space Security Director Release 24.1R2, after you install or upgrade Security Director, the following cronjob is added in existing crontab in all JBOSS nodes:

```
10 1 * * * /var/www/cgi-bin/ApplicationVisibility_DataReduction.sh >/dev/null 2>&1
```

The cronjob runs every day at 1:10 AM. The ApplicationVisibility_DataReduction.sh script is added in **/var/www/cgi-bin**.

If you want to purge the Application Visibility database, then in ApplicationVisibility_DataReduction.sh script, update APP_VISIBILITY=false to APP_VISIBILITY=true in all JBOSS nodes. However, purging is triggered only in VIP node.

By default, the data is retained for 7 days. You can modify the number of days for which you want to retain the data in Application Visibility database using the following parameters in ApplicationVisibility_DataReduction.sh script:

```
DAYS_IN_SECONDS_1=86400000
DAYS_IN_SECONDS_7=604800000
DAYS_IN_SECONDS_14=1209600000
DAYS_IN_SECONDS_21=1814400000
```



Juniper Business Use Only

```
DAYS_IN_SECONDS_30=2592000000
# MODIFY HERE if needed:  Replace Variable in next line for selected time
SELECTED_DAYS=$DAYS_IN_SECONDS_7
```

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

# Installing and Upgrading Security Director Release 24.1R3

Junos Space Security Director Release 24.1R3 is supported on Junos Space Network Management Platform Release 24.1R2 that can run on the following devices:

- Junos Space virtual appliance
- KVM server

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

# Installing and Upgrading Security Director Release 24.1R4

Junos Space Security Director Release 24.1R4 is supported only on Junos Space Network Management Platform Release 24.1R4 that can run on the following devices:

- Junos Space virtual appliance
- KVM server

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

# Installing and Upgrading Security Director Release



Juniper Business Use Only

## 24.1R5

Junos Space Security Director Release 24.1R5 is supported only on Junos Space Network Management Platform Release 24.1R5 that can run on the following devices:

- Junos Space virtual appliance
- KVM server

For more information about installing and upgrading Security Director, 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 Firewalls. 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 3 on page 11.

**Table 3: 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 |
|---|---|---|---|



Juniper Business Use Only

| | | | |
|---|---|---|---|
| 18.4R1-S1 | 18.4R1.8<br>18.3R1.1<br>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.



Juniper Business Use Only

| 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<br>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 4 on page 11.

**Table 4: 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<br>18.3R1.1<br>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 5 on page 12.

**Table 5: 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<br>18.4R1.7<br>18.4R1.6<br>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<br>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 6 on page 12.

**Table 6: Device with Service Release and Junos Space without more DMI Schemas**

| Junos OS Version on the Device | Junos Space DMI Schemas Installed | Junos Space Default Version | Junos Space Version Chosen for Platform |
|---|---|---|---|
| 18.4R1.1 | 18.5R1.1<br>18.3R1.1<br>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 Firewalls 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 Firewalls 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**: Contact Juniper Support team for MySQL username and password details.

**NOTE**: If you use a database dedicated setup (SSD hard disk VMs), the performance of publish and update is better compared with 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 24.1.

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



Juniper Business Use Only

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.

- When you install a signature to a device, upgrade Application Signatures fails with the message: Updating data-plane with new attack or detector:failed.

  Workaround: Push the IPS policy from Security Director before installing a signature to the root device.

- 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 DRP. In Security Director Release 19.4R1 and earlier, if you configure VPN as unnumbered with a DRP, 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 UI and Security Director UI are launched within 20 minutes. The



Juniper Business Use Only

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 objects already exist in Security Director.



Juniper Business Use Only

# Known Issues

This section lists the known issues in Junos Space Security Director Release 24.1.

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

- Preferred vs Default Link Usage widget does not show the date for the APBR on App Based Routing page. PR1747794
- 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



Juniper Business Use Only

- 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 not used in a policy, or assign a Content Security policy.



Juniper Business Use Only

- 

- 

  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 many 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.

- Clis are not generating for authentication type used in firewall policy profile. PR1787073

- Logging session CLIs are not getting generated for TSYS device. PR1802193

# Resolved Issues

# Resolved Issues in Junos Space Security Director Release 24.1R1

This section lists the issues fixed in Junos Space Security Director Release 24.1R1:

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

- When two or more route based VPNs are created in Security Director, the preview changes for the last created VPN does not display the zone and routing instance configuration. PR1806457

- Multiple IKE policy pre-shared-key statements are pushed to the firewall. PR1486055
  Security Director Release 19.3R1.3 fails to display the reason for the failure of devices with and without OOB changes. PR1488680

  The preshared keys (PSK) for the VPNs under Security Director fail to update correctly on the devices. PR1488781

- When you try to clone a rule in Security Director, the cloned rule does not consist of the tunnel information. PR1489303



Juniper Business Use Only

- 
- 
- Security Director cannot search for a shared object in the address object list from a sub domain though it has access to the objects from the parent domain. PR1499409
- Device connection status is DOWN in Security Director, but the status is UP in Junos Space Network Management Platform. PR1528454
- Search option does not work as expected. PR1533072
- There are issues with addresses when a user tries to import policies into Security Director. PR1556335
- There are issues during address object replacement. PR1557743
- When you switch the Security Director logs to a specific domain, it shows No data available. PR1558940
- When you try to update multiple devices at once in Security Director, the device update fails with device lookup failed error message. PR1561848
- Column filter does not work for source address with IP address and address object. PR1570439
- There are issues with the service object search. PR1573475
- When the user updates a policy on the device, the rules are deleted incorrectly. PR1581760
- IPv6 search does not work in Security Director. PR1586900
- There are issues with IPsec VPN extranet device IP deployment. PR1597978
- The user is unable to change interface binding for IPsec VPN. PR1598301
- There are issues with Security Director Log Collector. PR1602705
- The user cannot delete unused address objects. PR1655068
- The policy update job fails. PR1655881
- When you rename a policy based VPN in Security Director, it displays an error asking for st0 interface value. PR1679991

  The user is unable to edit the tunnel settings when creating a route based VPN with multi proxy-ID. PR1770960

  The user is unable to delete the details of users and roles from Security Director. PR1787314
- The Rollback function is not working properly in Security Director. PR1787570



Juniper Business Use Only

- 
- 
- The Intrusion Detection and Prevention (IDP) policy update is successful, but the SRX Series Firewall CLI failed due to mismatches between node0 and node1 in the NSM-download file. PR1795041
- The Application Visibility page takes longer than usual to display data in Security Director. PR1764875

# Resolved Issues in Junos Space Security Director Release 24.1R2

This section lists the issues fixed in Junos Space Security Director Release 24.1R2:

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

- Content Security default configuration pushes extra configurations from Security Director. PR1769834
- When you try to either preview, publish, or update a NAT policy configuration, it fails with an error message. PR1818400
- The configuration preview takes longer than usual to complete in Security Director. PR1809047
- Policy based VPN is missing from the security policy rule. PR1821775
- When you try to publish a VPN job in Security Director, it fails with an error message. PR1816247
- IP filter tab search is not working as expected. PR1774699
- The search criteria show incorrect results in Security Director. PR1775496
- IDP packet capture process fails to run on the JBoss VIP node. PR1811578
- The user is unable to login to Security Director with a system generated password. PR1817001
- The user is unable to import the firewall policy in Security Director. PR1816006
  The Source Zone category under Web Filtering does not show any data in Security Director GUI. PR1803773
- When the user tries to select the source NAT pool in a sub domain, Security Director displays NAT pools across all sub domains in the drop-down list. PR1825006



Juniper Business Use Only

- 
- 
- Error while importing variable using CSV in Security Director PR1827777
- The snapshot policy job takes longer than usual to complete after upgrading from Security Director Release 21.3R1 to Security Director Release 23.1R1. PR1829529
- The search functionality does not work properly in Security Director Release 22.2R1 HP v6. PR1825791

# Resolved Issues in Junos Space Security Director Release 24.1R4

This section lists the issues fixed in Junos Space Security Director Release 24.1R4:

- Security Director shows incorrect interval values when DPD mode is enabled. PR1872073
- Unable to create security logging nor NTP when selecting multiple devices on Security Director. PR1877029
- The quick template doesn't list in the profile for the selection after upgrading to 24.1 in Security director. PR1872102
- Security Director Firewall Log Export to CSV Missing Source/Destination Country. PR1883846
- Vulnerabilities reported in Junos Space Security Director. PR1829067

# Resolved Issues in Junos Space Security Director Release 24.1R5

This section lists the issues fixed in Junos Space Security Director Release 24.1R5:

- SD - VPN Traffic selectors not displayed in "view tunnels". PR1909787



Juniper Business Use Only

# Hot Patch Releases

## Junos Space Security Director Release 24.1R2 Hot Patch Release

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 24.1R2 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 23.1R1 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.



Juniper Business Use Only

### Installation Instructions

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

1. Download the Security Director 24.1R2 Patch *vX* from the download site.

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

2. Copy the SD24.1R2-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 SD24.1R2-hotpatch-vX.tgz.
```

4. Extract the SD24.1R2-hotptach-vX.tgz file:

```
tar -zxvf SD24.1R2-hotpatch-vX.tgz
```

5. Change the directory to SD24.1R2-hotpatch-vX.

   ```
   cd SD24.1R2-hotpatch-vX
   ```

6. Execute the patchme.sh script from the SD24.1R2-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/.SD24.1R2-hotpatch-vX, is created with the list of Red Hat Package Manager (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 7 on page 23 lists the resolved issues in Security Director Release 24.1R2 hot patch.

**Table 7: Resolved Issues in the Hot Patch**



Juniper Business Use Only

| PR | Description | Hot Patch Version |
|---|---|---|
| PR1835150 | The user is unable to download SummaryReport.zip file in Security Director. | v1 |



Juniper Business Use Only

# Junos Space Security Director Release 24.1R3 Hot Patch Release

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 24.1R3 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 23.1R1 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 24.1R3 Patch *vX* from the download site.

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

2. Copy the SD24.1R3-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 SD24.1R3-hotpatch-vX.tgz.
```

4. Extract the SD24.1R3-hotptach-vX.tgz file:

```
tar -zxvf SD24.1R3-hotpatch-vX.tgz
```

5. Change the directory to SD24.1R3-hotpatch-vX.

   ```
   cd SD24.1R3-hotpatch-vX
   ```

6. Execute the patchme.sh script from the SD24.1R3-hotpatch-vX folder:

```
sh patchme.sh
```



Juniper Business Use Only

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

A marker file, /etc/.SD24.1R3-hotpatch-vX, is created with the list of Red Hat Package Manager (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 8 on page 25 lists the resolved issues in Security Director Release 24.1R3 hot patch.

**Table 8: Resolved Issues in the Hot Patch**

| PR | Description | Hot Patch Version |
|---|---|---|
| PR1866711 | In Security Director Release 24.1R3, the metadata filter under Configure > Firewall Policy > Standard Policies page fails to perform intersection (AND) or union (OR) functions. | v4 |
| PR1858790 | The user is unable to search services with port numbers in Security Director Release 24.1R2. | v3 |
| PR1846929 | The user is unable to install IDP signatures offline and is unable to schedule new poll license jobs. | v3 |
| PR1864422 | Security Director fails to push the address book entries to the SRX Series Firewall. | v3 |



Juniper Business Use Only

**Table 8: Resolved Issues in the Hot Patch *(Continued)***

| PR | Description | Hot Patch Version |
|---|---|---|
| PR1854243 | The databases are out of sync in Security Director.<br><br>Workaround:<br><br>1. Login to the JBoss CLI using the following command:<br><br>`/usr/local/jboss/bin/jboss-cli.sh --connect --user=admin --password=$(grep jboss.admin /etc/sysconfig/JunosSpace/pwd \| awk -F= '{print $2}') --controller=jmp-CLUSTER`<br><br>2. Run the following command in the JBoss CLI and set tcp-keep-alive to false.<br><br>`/profile=full-ha/subsystem=undertow/server=default-server/http-listener=default:write-attribute(name=tcp-keep-alive, value=false)`<br><br>3. Verify the value<br><br>`/profile=full-ha/subsystem=undertow/server=default-server/http-listener=default:read-resource`<br><br>4. Stop JBoss and JBoss-dc on the VIP node and JBoss on the non-VIP node.<br><br>5. Start JBoss and JBoss-dc on the VIP node and JBoss on the non-VIP node. | v2 |



Juniper Business Use Only

**Table 8: Resolved Issues in the Hot Patch *(Continued)***

| PR | Description | Hot Patch Version |
|---|---|---|
| PR1853552 | The user is unable to modify the system log configuration in Security Director. | v2 |
| PR1849595 | The user is unable to view data in the Application tab under Monitor >Applications. The page displays An error occurred while requesting the data message. | v1 |
| PR1851141 | The user is unable to configure rule sets for a NAT policy using change control workflow. | v1 |
| PR1852966 | The user is unable to install AppSecure license on the vSRX Virtual Firewall through Security Director. | v1 |
| PR1852986 | The user is unable to scroll down on the IDP policy rules list under Configure >IPS Policy >Policies in Security Director 24.1R1. | v1 |



Juniper Business Use Only

# Junos Space Security Director Release 24.1R4 Hot Patch Release

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 24.1R4 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 24.1R4 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:

7. Download the Security Director 24.1R4 Patch *vX* from the download site.

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

8. Copy the SD24.1R4-hotpatch-vX.tgz file to the /home/admin location of the VIP node.

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

```
md5sum SD24.1R4-hotpatch-vX.tgz.
```

10. Extract the SD24.1R4-hotptach-vX.tgz file:

```
tar -zxvf SD24.1R4-hotpatch-vX.tgz
```

11. Change the directory to SD24.1R4-hotpatch-vX.

```
cd SD24.1R4-hotpatch-vX
```

12. Execute the patchme.sh script from the SD24.1R4-hotpatch-vX folder:



Juniper Business Use Only

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/.SD24.1R4-hotpatch-vX, is created with the list of Red Hat Package Manager (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 9 on page 25 lists the resolved issues in Security Director Release 24.1R4 hot patch.

**Table 9: Resolved Issues in the Hot Patch**

| PR | Description | Hot Patch Version |
|---|---|---|
| PR1886084 | Global search for variable address shows number of usage, but no content. | V1 |
| PR1886086 | Delete variable, has usage. Click here to see them does not work. | V1 |
| PR1890175 | | V1 |



Juniper Business Use Only

| | | |
|---|---|---|
| | Security Director variables are not getting deleted, and others are not reflected in the GUI. | |
| PR1872073 | Security Director shows incorrect interval values when DPD mode is enabled. | V1 |
| PR1879410 | Update of unified policy to SRX1500 devices with logical systems failed with statement creation failed IDP-policy. | V1 |
| PR1878172 | Configuration Update Failed - statement creation failed batteryupdate. | V1 |



Juniper Business Use Only

# Junos Space Security Director Release 24.1R5 Hot Patch Release

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 24.1R5 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 24.1R5 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:

13. Download the Security Director 24.1R5 Patch *vX* from the download site.

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

14. Copy the SD24.1R5-hotpatch-vX.tgz file to the /home/admin location of the VIP node.

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

```
md5sum SD24.1R5-hotpatch-vX.tgz.
```

16. Extract the SD24.1R4-hotptach-vX.tgz file:

```
tar -zxvf SD24.1R5-hotpatch-vX.tgz
```

17. Change the directory to SD24.1R5-hotpatch-vX.

```
cd SD24.1R5-hotpatch-vX
```

18. Execute the patchme.sh script from the SD24.1R5-hotpatch-vX folder:

```
sh patchme.sh
```



Juniper Business Use Only

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

A marker file, /etc/.SD24.1R5-hotpatch-vX, is created with the list of Red Hat Package Manager (RPM) details in the hot patch.

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

# New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 24.1R5.

**Edit Support of VPN Profile**—Starting Junos Space Security Director Release 24.1R5 Hot Patch V1, we've have enabled option to edit the IPsec VPN profiles for VPNs that are imported or already saved or published to device. The new functionality includes a drop-down selection for updating compatible VPN profiles and is applicable for both imported VPNs and VPNs created by Security Director.

# Finding More Information

For the latest, most complete information about known and resolved issues, 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 feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: https://apps.juniper.net/feature-explorer/.



Juniper Business Use Only

# Revision History

**Table 9: Revision History Table**

| Release | Release Date | Updates |
|---|---|---|
| Junos Space Security Director Release 24.1R5 Hot Patch V1 | 05 January 2026 – Revision 12 | Updated the following:<br>• New and Changed Features in Junos Space Security Director 24.1R5 V1 hot patch<br>• Installation and Upgrade Instructions |
| Junos Space Security Director Release 24.1R5 | 6 November, 2025—Revision 11 | Updated the following:<br>• New and Changed Features<br>• Installation and Upgrade Instructions<br>• Known Issues<br>• Resolved Issues |
| Junos Space Security Director Release 24.1R4 Hot Patch V1 | 7 October, 2025—Revision 10 | Added Resolved Issues in Junos Space Security Director Release<br>24.1R4 Hot Patch V1 |
| Junos Space Security Director Release 24.1R4 | 30 June, 2025—Revision 9 | Updated the following:<br>• New and Changed Features<br>• Installation and Upgrade Instructions<br>• Known Issues<br>• Resolved Issues |



Juniper Business Use Only

| | | |
|---|---|---|
| Junos Space Security Director Release 24.1R3 Hot Patch V4 | 15 April, 2025—Revision 8 | Added a Resolved Issue in Junos Space Security Director Release 24.1R3 Hot Patch V4 |
| Junos Space Security Director Release 24.1R3 Hot Patch V3 | 26 March, 2025—Revision 7 | Added Resolved Issues in Junos Space Security Director Release 24.1R3 Hot Patch V3 |
| Junos Space Security Director Release 24.1R3 Hot Patch V2 | 19 February, 2025—Revision 6 | Added Resolved Issues in Junos Space Security Director Release 24.1R3 Hot Patch V2 |
| Junos Space Security Director Release 24.1R3 Hot Patch V1 | 3 February, 2025—Revision 5 | Added Resolved Issues in Junos Space Security Director Release 24.1R3 Hot Patch V1 |
| Junos Space Security Director Release 24.1R3 | 30 December, 2024—Revision 4 | Updated the following:<br>• New and Changed Features<br>• Installation and Upgrade Instructions |
| Junos Space Security Director Release 24.1R2 Hot Patch V1 | 29 October, 2024—Revision 3 | • Added Resolved Issues in Junos Space Security Director Release 24.1R2 Hot Patch V1<br>• Updated the Note under New and Changed Feature section. |



Juniper Business Use Only

**Table 9: Revision History Table *(Continued)***

| Release | Release Date | Updates |
|---|---|---|
| Junos Space Security Director Release 24.1R2 | 1 October, 2024—Revision 2 | Added the following sections:<br>• Resolved Issues in Junos Space Security Director Release 24.1R2<br>• Installing and Upgrading Security Director Release 24.1R2<br>Updated the note in the New and Changed Feature section. |
| Junos Space Security Director Release 24.1R1 | 30 May, 2024—Revision 1 | Initial Release Notes |

Juniper Business Use Only