Release Notes

Published
2024-12-03

Junos Space Security Director Release Notes 23.1R1

Table of 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, intrusion prevention system (IPS) policies, and application firewalls.

NOTE: You need IPS and application firewall licenses to push IPS policies and application firewall 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 23.1R1.

- **DNS sinkhole**-Starting in Junos Space Security Director Release 23.1R1, you can use DNS sinkhole to reject or resolve DNS requests for disallowed domains.
- **Data Plane Packet Capture**-Starting in Junos Space Security Director Release 23.1R1, you can capture and analyze router data plane traffic on Juniper Networks® SRX Series Firewalls. You can download the captured packets that are written to a packet capture file (**.pcap** file). You can capture data packets only from SRX4600, SRX5400, SRX5600, and SRX5800 Firewalls running the Junos OS Release 19.3 or later.
- **IDP package installation for FreeBSD12**-Starting in Junos Space Security Director Release 23.1R1, we support IDP package installation on SRX300, SRX320, SRX340, SRX345, and SRX380 Firewalls with FreeBSD12 running the Junos OS Release 23.2.

Supported Managed Devices

You can use Security Director Release 23.1R1 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 23.1 (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 23.1R1 supports the following Junos OS releases:

- 19.3
- 19.4
- 20.1
- 20.2
- 20.3
- 20.4

- 21.1
- 21.2R3-S2
- 21.3
- 21.4
- 22.1
- 22.2
- 23.1
- 23.2

> **NOTE**: EOL Junos releases may continue to work (support is not removed). However, we have not tested.

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 only on devices running Junos OS Release 11.4 or later.

> **NOTE**: To manage an SRX Series device 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)
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
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
23.1R1	23.1R1	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 23.1R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome

Installation and Upgrade Instructions

IN THIS SECTION

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

Installing and Upgrading Security Director Release 23.1R1

Junos Space Security Director Release 23.1R1 is supported only on Junos Space Network Management Platform Release 23.1R1 that can run on the following devices:

- Junos Space virtual appliance
- Kernel-based virtual machine (KVM) server installed on CentOS Release 7.2.1511

When you install Junos Space Security Director Release 23.1R1 hot patch V7, 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
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 and Log Collector 23.1 (Security Director Insights VM), see Security Director Installation and Upgrade Guide.

Loading Junos OS Schema for SRX Series Devices

You must download and install correct Junos OS schema to manage SRX Series devices. 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 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 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 8.

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

Junos OS Version on 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 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 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 9.

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 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 the performance of your publish and update jobs.

  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.

- 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.

Known Behavior

This section contains the known behavior and limitations in Junos Space Security Director Release 23.1R1.

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

  Make sure you check the **Generate** checkbox 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 user interfaces 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 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** 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.

Known Issues

This section lists the known issues in Junos Space Security Director Release 23.1R1.

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 Advanced Policy-Based Routing (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

- An icon showing out-of-band changes is seen for firewall and IPS policies, although the corresponding policy changes are not made on the device. PR1484953

  Workaround: Clear the out-of-band 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 out-of-band 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 23.1R1:

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.

- The user is unable to change destination address for static NAT rules. PR1700163
- The search result for shared objects is not displayed correctly. PR1703135
- The user is unable to preview, publish, or update configuration. PR1707744
- Publish fails with error "Content Security is not available in the device". PR1710418
- Security Director saved a cyclic service group. PR1679106
- The created object addresses do not show in the search result. PR1689483
- The log source is shown as 127.0.0.1 when Security Director Insights is used as the log collector. PR1568417
- The MTU size is not set correctly. PR1638491
- There are discrepancies in the geo location report. PR1664682
- Security Director deletes device configuration due to SRX DMI schema 22.1R1.10. PR1687371

- Security Director is unable to import configuration from a discovered device. PR1698572
- The logical systems policy update via Security Director from standby SRX cluster member displays an error. PR1698840
- The rule position is not saved correctly. PR1701008
- The IPS report for some devices do not return any data. PR1701645
- The user is unable to import policy from the zip file. PR1709403
- Application visibility logs are not displayed for the last 8 hours and earlier. PR1702216
- The Content Security policies update on SRX Series Firewalls and vSRX Virtual Firewall fail. PR1711219
- The Auto Policy Sync in Security Director does not work. PR1653054
- The service search by port number does not work. PR1659212
- When adding new addresses to an address group, the existing addresses in the group disappear. PR1714846
- Security Director is unable to import Firewall policy in SRX4200. PR1722324
- The user is unable to modify zone with more than 100 interface units. PR1723625
- Save Comments does not work after upgrade to Security Director 22.3.PR1723715
- Security Director API displays internal server error during policy edit if the policy is locked.PR1731271

Hot Patch Releases

IN THIS SECTION

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

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

2. Copy the `SD23.1R1-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 SD23.1R1-hotpatch-vX.tgz.
   ```

4. Extract the `SD23.1R1-hotptach-vX.tgz` file:

   ```
   tar -zxvf SD23.1R1-hotpatch-vX.tgz
   ```

> **NOTE**: For only Security Director 23.1R1 Hot Patch v7, extract the `SD23.1R1-hotptach-v7.tgz` file:
>
> ```
> tar -xvf SD23.1R1-hotpatch-v7.tgz
> ```

5. Change the directory to `SD23.1R1-hotpatch-vX`.

   cd SD23.1R1-hotpatch-vX

6. Execute the `patchme.sh` script from the `SD23.1R1-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/.SD23.1R1-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 Enhanced Features in the Hot Patch

Junos Space Security Director Release 23.1R1 hot patch includes the following enhancements:

- **Support for SRX2300**—Starting in Junos Space Security Director Release 23.1R1 hot patch v3, we've provided support for SRX2300 Firewall.
- **Support for SRX1600**—Starting in Junos Space Security Director Release 23.1R1 hot patch v2, we've provided support for SRX1600 Firewall.

Supported Devices in the Hot Patch

Table 6 on page 19 lists the devices supported in Security Director 23.1R1 Hot Patch Releases.

Table 6: Supported Devices in the Hot Patch

Supported Device	Hot Patch Release Version
SRX1600	Junos Space Security Director 23.1R1 Hot Patch v2
SRX2300	Junos Space Security Director 23.1R1 Hot Patch v3

Resolved Issues in the Hot Patches

Table 7 on page 19 lists the resolved issues in Security Director Release 23.1R1 hot patch.

Table 7: Resolved Issues in the Hot Patch

PR	Description	Hot Patch Version
PR1741255	The **Application Visibility** page does not show the exact number of applications in the Security Director GUI.	v7
PR1764875	The **Application Visibility** page takes longer than usual to display data in Security Director.	v7
PR1769834	UTM default configuration pushes extra configurations from Security Director.	v7
PR1788204	The user is unable to view UTM categories in Security Director GUI.	v7
PR1791715	The user is unable to fetch geo IP from PE, the progress bar is stuck at zero percent in Security Director.	v7

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1803773	The **Source Zone** category under **Web Filtering** does not show any data in Security Director GUI.	v7
PR1814140	The user is unable to push multiple metadata-based policies in custom LSYS from Security Director.	v7
PR1816006	The user is unable to import the firewall policy in Security Director.	v7
PR1816247	When you try to publish a VPN job in Security Director, it fails with `Another publish, unpublish, preview or update job is in progress for this device. Re-try after sometime.` error message.	v7
PR1817001	The user is unable to login to Security Director with a system generated password.	v7
PR1821775	Policy based VPN is missing from the security policy rule.	v7
PR1823959	The user is unable to change the MTU (Maximum Transmission Unit) size from the **Create Hub & Spoke (Establishment All Peers) VPN** page in Security Director.	v7
PR1825006	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.	v7

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1827777	Error while importing a variable using CSV in Security Director.	v7
PR1835150	The user is unable to download **SummaryReport.zip** file in Security Director, fails with `File wasn't available on site` error.	v7
PR1829529	Snapshot policy job takes longer than usual to complete after upgrading from Security Director Release 21.3R1 to Security Director Release 23.1R1.	v6
PR1809047	The configuration preview takes longer than usual to complete in Security Director.	v5
PR1762212	The user is unable to import the CSV file for variable objects in Security Director.	v5
PR1784546	The user is unable to preview, publish, and update a configuration in Security Director. The job fails with `Zone [ junos-host ] does not exist in device` error message.	v5
PR1787314	The user is unable to delete the details of users and roles from Security Director.	v5
PR1787570	The Rollback function is not working properly in Security Director.	v5

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1795041	The Intrusion Detection and Prevention (IDP) policy update is successful, but the SRX series CLI failed due to a mismatch between node0 and node1 in the NSM-download file.	v5
PR1798433	The user is unable to upload the latest-space-update zip file to the IDP signature database offline.	v5
PR1803701	Firewall Policy preview fails when you upgrade from Security Director Release 21.3R1 to Security Director Release 23.1R1.	v5
PR1811578	IDP packet capture process fails to run on the JBoss VIP node.	v5
PR1783380	When user tries to delete a security policy rule between two zones, Security Director generates two delete statements and the update fails.	v4
PR1782360	User is unable to create static route under Security Director 22.3R1.20 while using host/32.	v4
PR1774699	IP filter tab search is not working as expected.	v4
PR1763709	User is unable to publish a policy.	v4

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1741484	User is unable to change password from **Security Director** > **My Profile** > **Change Password**.	v4
PR1764858	When user selects the application session under appvisibility page, Security Director redirects to the wrong filter under all events.	v3
PR1756160	Devices missing from the UTM Install Category page.	v3
PR1755886	During NAT policy import, Security Director creates address object with value 0.0.0.0/0 and not any IP4 adresses.	v3
PR1754759	Security Director fails to search rule name for imported rules.	v3
PR1765982	Security Director API fails to prevent creation of duplicate addresses.	v3
PR1771392	User is unable to add an extranet device without an IP address when creating a site-to-site IPSec VPN where the remote site has a dynamic IP address.	v3
PR1752533	LC under Insights Nodes disappears after discovery.	v3

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1724644	Frequent syslog data parsing and **circuit_breaking_exception** error appers while fetching it via curl query.	v2
PR1751227	Security director is unable to get the policy hit count using the rest API.	v2
PR1741255	The application visibility feature shows incorrect application data in Security Director.	v2
PR1754290	VPN publishing jobs fail.	v2
PR1755392	When you search for a policy in Security Director through the rest API, the source or destination address of the policy is not displayed.	v2
PR1732842	The Pie chart is not displayed in the generated report because of the exceeding character limit in the URL.	v2
PR1737807	When you try to preview the changes done to a policy before publishing, it fails with `Calculating XML Edit Config` error message.	v1
PR1737807	Security Director deletes the routing options autonomous-system configuration, when you try to update the devices with IPsec VPN.	v1

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1736563	Security Director modifies the device setup by adding an additional set of VPN configurations.	v1
PR1735089	Security Director deletes the configurations for the policy-based VPNs that do not get imported to Security Director.	v1
PR1727372	The **VPN Monitoring** page does not load the data in Security Director Release 22.3R1.	v1
PR1698920	Security Director shows invalid configuration in the update configuration preview.	v1
PR1744985	After upgrading Security Director to 23.1R1 release, report generation fails with an error.	v1
PR1732842	The Pie chart is not displayed in the generated report because of the exceeding character limit in the URL.	v1
PR1746082	When you schedule a job to generate a report, it fails with exceptions.	v1
PR1741255	The application visibility feature shows incorrect application data in Security Director.	v1
PR1728629	User is unable to sort the columns on the **Logging Devices** page in Security Director.	v1

Table 7: Resolved Issues in the Hot Patch *(Continued)*

PR	Description	Hot Patch Version
PR1743599	Security Director displays the Tunnel Status as **UNKNOWN** when user tries to create a VPN through the GUI.	v1

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

Known Issues in the Hot Patch

Junos Space Security Director Release 23.1R1 hot patch includes the following known issue:

The user is unable to update IPS Policy for multiple logical systems when one of the logical systems is configured with all-attack signature. The job fails with `Device is down` error message. PR1827871

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

Release	Release Date	Updates
Junos Space Security Director Release 23.1R1	8 June, 2023—Revision 1	Intial Release Notes
Junos Space Security Director Release 23.1R1 Hot Patch V1	31 July, 2023—Revision 2	Added Resolved Issues
Junos Space Security Director Release 23.1R1 Hot Patch V2	14 September, 2023—Revision 3	Added the following in the Hot Patch: • New and Enhanced Features • Supported Devices • Resolved Issues
Junos Space Security Director Release 23.1R1 Hot Patch V3	14 December, 2023—Revision 4	Added the following in the Hot Patch: • New and Enhanced Features • Supported Devices • Resolved Issues
Junos Space Security Director Release 23.1R1 Hot Patch V4	21 February, 2023—Revision 5	Added Resolved Issues
Junos Space Security Director Release 23.1R1 Hot Patch V5	6 August, 2024—Revision 6	Added the following in the Hot Patch: • Resolved Issues • Known Issues

(Continued)

Release	Release Date	Updates
Junos Space Security Director Release 23.1R1 Hot Patch V6	2 September, 2024—Revision 7	Added Resolved Issues
Junos Space Security Director Release 23.1R1 Hot Patch V7	13 November, 2024—Revision 8	Added Resolved Issues and updated the Installation and Upgrade Instructions section.

> 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 © 2024 Juniper Networks, Inc. All rights reserved.