Engineering
Simplicity

Junos Space Security Director Release Notes 22.2R1

Published
2024-09-16

RELEASE

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 22.2R1.

- **Polymorphic address support in source and destination addresses for NAT rules**—Starting in Security Director Release 21.3R1 hot patch v3, while creating NAT rules for a group policy, you can select a polymorphic address as the source or destination address. The rule points to the default address if the device IP address does not match any of the context values in the polymorphic address. If there is a match, the address corresponding to the context value is considered as the source or destination address of the rule.

  NOTE: Polymorphic addresses are not supported in static NAT destination addresses.

- **Support for disabling service offload in Security Director**—Starting in Security Director Release 21.3R1 hot patch v3, we've provided options to delete the configured service and disable services offload for standard and unified firewall policies.

  You can select from the following options:

  - None—Select to delete the configured service from the device.
  - Enable—Select to enable services offload. When services offload is enabled, only the first packets of a session go to the SPU. The rest of the packets in services offload mode do not go to the SPU; therefore, some security features such as stateful screen are not supported. You can offload services only for TCP and UDP packets.
  - Disable—Select to disable services offload.

> **NOTE**: Both logical systems and tenant systems support the disable services offload feature.

- **Support to terminate CLI/J-Web edit mode user session**—Starting in Security Director Release 21.3R1 hot patch v3, when you retry the update job on devices that failed due to device lock failures, you can terminate CLI user sessions on a device from Security Director.

  To terminate the user session:

  1. Select **Monitor** > **Job Management**.
  2. Select the job, and then from the More list select **Retry on Failed Devices**.

     The Retry Update Failed Devices page is displayed.
  3. Select the **Evict CLI/J-Web edit mode users** option.

For new features and enhancements in Policy Enforcer, see Policy Enforcer Release Notes.

Supported Managed Devices

You can use Security Director Release 22.2R1 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 22.2 (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 22.2R1 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 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 6 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

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)
21.3R1	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

NOTE: For Policy Enforcer details, see Policy Enforcer Release Notes.

Supported Browsers

Security Director Release 22.2R1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Internet Explorer 11

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 22.2R1

Junos Space Security Director Release 22.2R1 is supported only on Junos Space Network Management Platform Release 22.2R1 that can run on the following devices:

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

For more information about installing and upgrading Security Director and Log Collector 22.2 (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 9.

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.			
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 10.

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 10.

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.			
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 11.

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.

- 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 22.2R1.

- 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 22.2R1.

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 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 unified threat management (UTM) 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 UTM custom objects without a UTM policy. PR1447779

  Workaround: Delete the UTM custom objects if they are not used in a policy, or assign a UTM 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 22.2R1:

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

- Security Log transport TLS-Profile is set incorrectly as NONE in Security Director. PR1665789

- Security Director API call does not work for NAT policies with more than 300 rules. PR1664941

- References do not work for dynamic address objects in Security Director. PR1664637

- The user is unable to push multiple configurations to the device. PR1664618

- Security Director updates an existing address book to the SRX Series device. PR1663898

- Unified Threat Management (UTM) custom categories gets deleted from the SSL proxy profile allowlist. PR1662493
- Security Director fails to export the filtered search for a rule to .pdf format. PR1660892
- Security Director fails to display the latest device configuration in the preview. PR1660583
- The user is unable to create route based VPN. PR1659421
- Security Director is unreachable when node 2 is the VIP node. PR1656449
- The policy update job fails. PR1655881
- The user is unable to delete unused dynamic objects created as a result of import. PR1655401
- The user cannot delete unused address objects. PR1655068
- Select and save functionalities in Intrusion Prevention System (IPS) policy fails in the firewall rule. PR1654241
- Incorrect fabric and control link status is displayed for logical systems. PR1651838
- Security Director pushes the same configuration to SRX Series device and then deletes it. PR1650529
- Search does not work for rules inside firewall policy. PR1649454
- The firewall policy update fails when you associate a dynamic address group. PR1649267
- The firewall policy update fails. PR1646550
- Address objects that are deleted from an address group does not show in delta. PR1684862

For resolved issues in Policy Enforcer, see Policy Enforcer Release Notes.

Hot Patch Releases

IN THIS SECTION

This section describes the installation procedure, features, and resolved issues in Junos Space Security Director Release 22.2R1 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 22.2R1 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 22.2R1 Patch v*X* from the download site.

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

2. Copy the **SD-22.2R1-hotpatch-v*X*.tgz** file to the **/home/admin** location of the VIP node.

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

   md5sum SD-22.2R1-hotpatch-v*X*.tgz.

4. Extract the **SD-22.2R1-hotptach-v*X*.tgz** file:

   ```
   tar -zxvf SD-22.2R1-hotpatch-vX.tgz
   ```

5. Change the directory to **SD-22.2R1-hotpatch-v*X***.

   ```
   cd SD-22.2R1-hotpatch-vX
   ```

6. Execute the `patchme.sh` script from the **SD-22.2R1-hotpatch-v*X*** 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-22.2R1-hotpatch-v*X***, 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

lists the resolved issues in the Security Director Release 22.2R1 hot patch.

Table 6: Resolved Issues in the Hot Patch

PR	Description	Hot Patch Version
PR1825791	The search functionality does not work properly in Security Director 22.2R1 HP v6.	V7
PR1817001	The user is unable to login to Security Director with a system generated password.	V7
PR1814140	The user is unable to push multiple metadata-base policies in custom LSYS from Security Director.	V7
PR1769834	UTM default configuration adds multiple unwanted configurations in Security Director.	V7
PR1775496	The search criteria show incorrect results in Security Director.	V6

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

PR	Description	Hot Patch Version
PR1786519	Device update fails with **statement not found** error while trying to delete the only rule from the rule group.	V5
PR1763709	User is unable to publish a policy from Security Director.	V4
PR1748252	Unable to import firewall rule in Security Director if the rule has DAG with missing category.	V3
PR1745412	Configuration for the address object in the SSL proxy associated with the firewall rule is missing.	V3
PR1744985	After upgrading Security Director to 23.1R1 release, report generation fails with an error.	V3
PR1743599	Security Director displays the Tunnel Status as **UNKNOWN** when user tries to create a VPN through the GUI.	V3
PR1742002	When you try to preview the changes done to a policy before publishing, it fails with `Calculating XML Edit Config` error message.	V3
PR1736563	Security Director modifies the device setup by adding an additional set of VPN configurations.	V3

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

PR	Description	Hot Patch Version
PR1731271	Security Director API displays internal server error during policy edit if the policy is locked.	V3
PR1728651	User is unable to import the group policies through zip file and snapshot roll back policy feature in Security Director.	V3
PR1728629	User is unable to sort the columns on the Logging Devices page in Security Director.	V3
PR1727372	The **VPN Monitoring** page does not load the data in Security Director Release 22.3R1.	V3
PR1723715	Save Comments does not work after upgrade to Security Director 22.3.	V3
PR1722324	Security Director is unable to import Firewall policy in SRX4200.	V3
PR1722117	Application visibility logs for the last eight hours and earlier are missing from the system.	V3
PR1716107	Security Director requires daily re-indexing for the search functionality to work properly.	V3

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

PR	Description	Hot Patch Version
PR1701645	SRX series devices do not show any data in the Intrusion Prevention System (IPS) report with log event `IDP_ATTACK_LOG_EVENT_LS`.	V3
PR1698920	Security Director shows invalid configuration in the update configuration preview.	V3
PR1659212	The search functionality in Security Director does not work properly when you search by port number.	V3
PR1746987	The VPN monitoring process hangs continuously, resulting in pile-ups.	V3
PR1735089	Security Director deletes the configurations for the policy-based VPNs that do not get imported to Security Director.	V3
PR1653054	The Auto Policy Sync in Security Director does not work.	V3
PR1754290	VPN publishing jobs fail.	V3
PR1741484	User is unable to change the local password from the Security Director GUI, **My Profile** > **Change Password**.	V3
PR1734133	When user performs snapshot rollback policy, Security Director creates a duplicate default IPS policy.	V3

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

PR	Description	Hot Patch Version
PR1664682	Geographical location report shows incorrect data in Security Director.	V2
PR1667530	The global search and column search functionalities do not work accurately in Security Director.	V2
PR1698572	Security director displays `An error occurred while requesting the data` error message while importing configuration from SRX4100 device.	V2
PR1702216	The application visibility feature does not show the log data for last eight hours and earlier.	V2
PR1709345	The Maximum Transmission Unit (MTU) is not visible during the edit workflow, when provided as default.	V2
PR1714846	When you add a new address to the address group, the GUI removes all the existing objects from the group.	V2
PR1568417	In Security Director, Security Director Insights shows the log source as 127.0.0.1 for all logs rather than the SRX IP address or the actual source from where the logs are originated.	V1

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

PR	Description	Hot Patch Version
PR1613930	The user is unable to edit the Policy-based VPN name or description in Security Director.	V1
PR1653687	Security Director does not display the correct time-zone when you change the time-zone using modify configuration.	V1
PR1662267	The search functionality in Security Director does not work for newly configured rules.	V1
PR1674701	The Security Director log filter does not work as expected for a particular timeframe.	V1
PR1676755	Security Director fails to import the security policies with the object address 0.0.0.0/0.	V1
PR1679106	Security Director updates the database with incorrect cyclic service group.	V1
PR1681035	There are issues with VPN profiles authentication algorithm after you upgrade Security Director.	V1
PR1683144	The search and find usage functionality in Security Director does not work as expected.	V1

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

PR	Description	Hot Patch Version
PR1683173	When the user configures a new IPsec VPN profile for route-based Hub and Spoke using the manual pre-shared key option, the output is set to multiple security IKE policies instead of only one security IKE policy.	V1
PR1687371	Security Director deletes the NAT and security intelligence settings from SRX Series Firewalls when the user uses DMI schema 22.1R1.10.	V1
PR1689302	Address object import from a CSV file fails.	V1
PR1689483	The search functionality in Security Director does not work for newly created address objects.	V1
PR1689638	When you view device changes, Security Director displays the Managed status as Device Changed for several devices.	V1
PR1691539	Security Director fails to import the policies using zip file.	V1
PR1694161	Security Director updates multiple policies even when you select only one policy for update.	V1

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

PR	Description	Hot Patch Version
PR1695528	Intrusion Detection and Prevention (IDP) signature continues to install the updates on SRX Series devices from IDP files even when the file transfer fails.	V1
PR1698840	Update to the Logical System (LSYS) fail at times in Security Director.	V1
PR1700163	User is unable to change the destination address for static NAT rules in Security Director.	V1
PR1701008	When you change the sequence of three or more set of rules in the Security Director, the changed order does not appear correctly after saving the changes.	V1
PR1703135	User is unable to search for an object in Security Director even when the objects exist in Shared Objects.	V1
PR1709403	Security Director fails to import the policy zip files with more than 20000 rules.	V1
PR1701645	SRX series devices do not show any data in the Intrusion Prevention System (IPS) report with log event *IDP_ATTACK_LOG_EVENT_LS*.	V1

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

PR	Description	Hot Patch Version
PR1707744	When you try to preview, publish, or update configuration in Security Director, it fails with an error.	V1
PR1710418	Security Director fails to publish the SRX series cluster policy with `UTM is not available in the device` error message.	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

30 August, 2022—Revision 1—Junos Space Security Director Release 22.2R1

2 February, 2023—Revision 2—Junos Space Security Director Release 22.2R1 Hot Patch V1

3 April, 2023—Revision 3—Junos Space Security Director Release 22.2R1 Hot Patch V2

15 September, 2023—Revision 4—Junos Space Security Director Release 22.2R1 Hot Patch V3

19 October, 2023—Revision 5—Junos Space Security Director Release 22.2R1 Hot Patch V4

7 March, 2024—Revision 6—Junos Space Security Director Release 22.2R1 Hot Patch V5

4 July, 2024—Revision 7—Junos Space Security Director Release 22.2R1 Hot Patch V6

16 September, 2024—Revision 8—Junos Space Security Director Release 22.2R1 Hot Patch V7