

Release Notes

Published
2026-08-06

Junos Space Security Director Release Notes 26.1

Table of Contents

- Introduction3
- New and Changed Features3
- Supported Managed Devices3
- Supported Log Collection Systems4
- Supported Junos OS Releases.....4
- Threat Prevention (ATP) Cloud Releases5
- Supported Browsers5
- Installation and Upgrade Instructions6
- Supported Software Versions.....6
- Loading Junos OS Schema for SRX Series Firewalls6
- DMI Schema Compatibility for Junos OS Service.....6
- Management Scalability..... 10
- Known Behavior..... 10
- Known Issues 13
- Resolved Issues 13
- Finding More Information 16
- Revision History 17

Introduction

The Junos Space® Security Director application is a powerful and easy-to-use solution that enables you to secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and AppFW.



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

New and Changed Features

This section describes the new features and enhancements to existing features in Junos Space Security Director Release 26.1R1.

Enhanced VPN cryptographic options—Use this feature in Junos Space Security Director Release 26.1R1 to configure Diffie-Hellman (DH) groups 15, 16, and 21. You can also configure the Secure Hash Algorithm (SHA)-512 and Hash-based Message Authentication Code (HMAC)-384 and 512 in VPN profiles. These advanced cryptographic options protect your data, strengthen your VPN security, and safeguard your network traffic from evolving threats. See [Create VPN Profiles](#).

Support for selecting signature packages using service release and build parameters—Use service release, build, and release parameters to identify and map customized signature pack files to prevent release-specific failures in application identification (APPID) and intrusion detection/prevention (IDP).

Supported Managed Devices

You can use Security Director Release 26.1 to manage the following devices:

- SRX300, SRX320, SRX320-POE, SRX340, SRX345, SRX380
- SRX1500
- SRX4100, SRX4200, SRX4600
- SRX5400, SRX5600, SRX5800
- vSRX
- MX240

- MX480
- MX960
- MX2020

Supported Log Collection Systems

The following log collection systems are supported:

- Log Collector 26.1 (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 26.1 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, 22.3, 22.4
- 23.2, 23.4
- 24.2, 24.4
- 25.2, 25.4



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

The below table shows the supported Policy Enforcer and Juniper ATP Cloud releases.

Security Director Release	Compatible Policy Enforcer Release	Junos OS Release (Juniper ATP Cloud Supported Devices)
26.1R1	26.1R1	Junos OS Release 19.1R3 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 26.1 is best viewed on the following browsers:

- Mozilla Firefox
- Google Chrome

Installation and Upgrade Instructions

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

Supported Software Versions

Junos Space Security Director Release 26.1R1 is supported on Junos Space Network Management Platform Release 26.1R1.

Table 2: Supported Software Versions

Security Director Version	Compatible with Junos Space Network Management Platform Version	
	26.1R1 Hot Patch v1	
Security Director 26.1R1	Yes	
Security Director 26.1 R1 Hot Patch v1	Yes	

Installing and Upgrading Security Director Release 26.1

Junos Space Security Director Release 26.1R1 is supported only on Junos Space Network Management Platform Release 26.1R1 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](#).

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
18.4R1-S1	18.4R1.8 18.3R1.1 18.2R1.1	18.2R1.1	18.4R1.8

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

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

If a Junos OS Service Release is installed on your device without a matching DMI schema version in Junos Space Network Management Platform, then Junos Space chooses the nearest lower version of DMI schema installed, as shown in [Table 4](#).

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 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 5](#).

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 18.4R1.7 18.4R1.6 18.3R1.1	18.3R1.1	18.4R1.8

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

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

Juniper Business Use Only

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](#).

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 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 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 sub jobs 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 26.1.

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

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

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

- When you install a signature to a device, upgrade Application Signatures fail 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 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.

Known Issues

There are no known issues in Junos Space Security Director Release 26.1.

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

Resolved Issues

This section lists the issues fixed in Junos Space Security Director Release 26.1R1:

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

- Security Director can't import a firewall policy when the webClientAuthName field exceeds the character limit. [PR1908616](#)
- The VPN import job doesn't import protected networks from SRX Series Firewalls in Security Director Release 24.1R4. [PR1914107](#)
- Security Director shows the IKE identity as **Hostname** instead of none. [PR1915510](#)
- When filtering by rule name, the API returns the full payload instead of only the matching rule. [PR1917310](#)
- An error occurs when installing signatures on a device. [PR1919454](#)
- After upgrading to Junos Space 24.1R4, packet captures return 0 bytes. [PR1925044](#)
- Security Director continues to display the best match schema even after the **Allow Best Match Schema** option is disabled. [PR1931443](#)
- In Security Director Release 24.1R5, publishing fails for firewall and NAT policies on the root firewall. [PR1932446](#)
- After you edit a shared address object, the traffic selector doesn't update. [PR1936769](#)
- The route-based proxy ID updates to 0.0.0.0/32 instead of 0.0.0.0/0. [PR1938567](#)
- Firewall rules are reordered when you copy them from another policy. [PR1938575](#)
- Multiple users can't save VPN configurations in Security Director. [PR1939437](#)
- After applying the Security Director Release 24.1R5 Hot patch V2, the PFS group changes from 19 to 15. [PR1941206](#)
- When a traffic selector address changes, Security Director doesn't mark the VPN as re-publish required. [PR1931443](#)
- Security Director calculates incorrect CLI for an APBR (advanced policy-based routing) policy configuration. [PR1944946](#)
- An error occurs during signature installation, pushing files to the device fails. [PR1930074](#)
- Security Director shows an incorrect error when adding a static route to a routing instance. [PR1941735](#)
- Security Director fails to set up a VPN with st0 interfaces. [PR1951395](#)
- In Security Director Release 24.1R5, search doesn't work in a subdomain for an IP address or object name. [PR1952644](#)
- Unable to import IPsec VPNs into Junos Space Network Management Platform. [PR1943212](#)
- The Security Director GUI doesn't support a dns-name address object longer than 69 characters, although you can create it on the SRX Series CLI. [PR1954328](#)
- SD Does Not Recognize OOB Changes for After Performing Update. [PR1925154](#)

Hot Patch Releases

Junos Space Security Director Release 26.1R1 Hot Patch Release

This section describes the installation procedure and resolved issues in Junos Space Security Director Release 26.1R1 hot patches.

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.
- 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 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 26.1R1 Patch vX from the [download site](#).

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

2. Copy the SD26.1R1-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 SD26.1R1-hotpatch-vX.tgz.
```

4. Extract the SD26.1R1-hotpatch-vX.tgz file:

```
tar -zxvf SD26.1R1-hotpatch-vX.tgz
```

5. Change the directory to SD26.1R1-hotpatch-vX.

```
cd SD26.1R1-hotpatch-vX
```

6. Execute the patchme.sh script from the SD26.1R1-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/.SD26.1R1-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

Resolved Issues in the Hot Patches

Table 7 on page 23 lists the resolved issues in Security Director Release 26.1R1 hot patch.

Table 7: Resolved Issues in the Hot Patch

PR	Description	Hot Patch Version
1952155	Security Director Packet Capture "No data available" error	v1
1960741	Inconsistent API response: 'rule-order' field is missing after install SD 24.1 R5 HPv3	v1
1966098	[Confidential]-Policy enforcer backup scheduled jobs are not working as expected.	v1
1952644	Security Director Search not working in subdomain (for IP object-name) running 24.1R5	v1

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/>.

Revision History

Table 8: Revision History Table

Release	Release Date	Updates
Junos Space Security Director Release 26.1R1 Hot Patch V1	6 August 2026—Revision 2	Updated the following: • New and Changed Features in Junos Space Security Director 26.1R1 V1 hot patch • Resolved Issues
Junos Space Security Director Release 26.1R1	4 June 2026—Revision 1	Initial Release Notes

Copyright © 2026 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2025 Juniper Networks, Inc. All rights reserved.