

# Junos<sup>®</sup> Space Security Director 13.1P2

## Release Notes

Release 13.1P2  
25 September 2013

The Junos Space Network Application Platform provides the essential tools the network administrator needs for automating network operations, including device discovery and management, topology visualization, deploying device images and scripts, network monitoring, job operation management, user account management, audit logging, and network administration. Network administration tasks include managing the Junos Space fabric (comprising one or more IP-connected nodes), databases, licenses, applications, authorization servers, tags, permission labels, DMI schemas, and troubleshooting.

### Contents

|   |    |
|---|----|
| Security Director Release Notes . . . . .                         | 2  |
| Installing Security Director . . . . .                            | 2  |
| Supported Devices . . . . .                                       | 3  |
| Supported Junos OS Releases . . . . .                             | 3  |
| Supported Browsers . . . . .                                      | 4  |
| Management Scalability . . . . .                                  | 4  |
| Features . . . . .  | 4  |
| Known Issues . . . . .  | 6  |
| Known Behavior . . . . .  | 8  |
| Resolved Issues . . . . .   | 9  |
| Errata and Changes in Documentation for Security Director Release |    |
| 13.1P1 . . . . .  | 9  |
| Junos Space Documentation and Release Notes . . . . .             | 9  |
| Documentation Feedback . . . . .                                  | 10 |
| Requesting Technical Support . . . . .                            | 10 |
| Self-Help Online Tools and Resources . . . . .                    | 10 |
| Opening a Case with JTAC . . . . .                                | 11 |
| Revision History . . . . .  | 11 |

## Security Director Release Notes

---

The Junos Space Security Director application is a powerful and easy-to-use solution that lets you secure your network by creating and publishing firewall policies, IPsec VPNs, NAT policies, IPS policies, and application firewalls. (To push IPS and application firewall signatures to a device, you also need an IPS and application firewall licenses.)

- [Installing Security Director](#)
- [Supported Devices](#)
- [Supported Junos OS Releases](#)
- [Supported Browsers](#)
- [Management Scalability](#)
- [Features](#)
- [Known Issues](#)
- [Known Behavior](#)
- [Resolved Issues](#)
- [Errata and Changes in Documentation for Security Director Release 13.1P1](#)

### Installing Security Director

Security Director 13.1P2 requires Network Application Platform Release 13.1P1.

If you have Security Director deployed already, first upgrade to Security Director 13.1R and then perform the following steps:

- a. From Security Director Release 13.1R1.4:
  1. Upgrade to Network Application Platform Release 13.1R and Network Application Platform Release 13.1P1.
  2. After Step 1 is done, upgrade to Security Director Release 13.1P2.



**NOTE:** Once Step 1 is completed, Security Director might be disabled in the Junos Space GUI. This is an expected behavior.

---

- b. If you have already deployed Security Director Release 13.1P1, you can directly upgrade to Security Director Release 13.1P2.
- c. If you do not have Security Director deployed already, perform the following steps:
  1. Install Network Application Platform Release 13.1R and upgrade to Network Application Platform Release 13.1P1.
  2. Install Security Director 13.1P2.

For more information about installation, refer to [Managing Junos Space Applications](#).

## Supported Devices

Security Director 13.1P2 is supported on the following SRX Series hardware devices, LN Series hardware device:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX550
- SRX650
- SRX1400
- SRX3400
- SRX3600
- SRX5600
- SRX5800
- LN1000-V

## Supported Junos OS Releases

- Security Director 13.1P2 supports the following Junos OS releases:
  - 10.4
  - 11.4 and later releases
  - 12.1X44-D10
  - 12.1X45
- SRX Series devices require Junos OS Release 12.1 and later releases to sync the Security Director description field to the device.
- The logical systems feature is supported on devices running Junos OS Release 11.4 and later.
- Junos OS Release 11.4 or a later release is required for AppFW feature support.



**NOTE:** Before you can manage an SRX Series device using Security Director, we recommend that you have the exact matching Junos OS schema installed on the Junos Space Network Application Platform. If there is a mismatch, a warning message is displayed during the publish preview workflow.

## Supported Browsers

Security Director is best viewed on the following browsers:

- Mozilla Firefox 20
- Chrome 26
- Internet Explorer 8.0 and 9.0

## Management Scalability

Security Director has been tested with a variety of customer configurations. A retail or branch configuration was tested with 10,000 devices and 100 firewall rules per device. Similarly, a data center scenario was tested with 10,000 rule policies, 20,000 address objects, and 3,000 custom service objects. Object Builder scale testing was performed with 50,000 address objects.

## Features

The Junos Space Security Director 13.1P2 application includes the following new features:

- **Junos OS Release 12.1X45 Features**—The following Junos OS Release 12.1X45 features are supported in Security Director Release 13.1P2:

- **Excluding Addresses or Address Group in a Firewall Policy**—Beginning in Junos OS Release 12.1X45, firewall policies have the option of excluding the source and destination addresses. The selected address list is considered excluded, and the device permits traffic from addresses other than the excluded address.

The following two new radio buttons are available to allow you to include or exclude the source and destination addresses in a firewall rule:

- Include Addresses
- Negate Addresses

The exclude address option is not supported for the address types IPv6, wildcard, unresolved DNS, and any. No more than 10 addresses per rule can be excluded. If more than 10 addresses are excluded, Security Director flags this during the preview or publish.

- **Configuration of Single IP Non-PAT Pool**—You can now create a source NAT pool with a single IP and no port translation. Two new parameters, Address Pooling and Address Sharing, are available. You can choose Address Pooling for all types of translations, but you can enable address sharing only when you select No Translation. If you select Host Address Base, the Address Pooling or Address Sharing options are not shown.
- **Logical Systems Support for Group NAT Policy**—All logical systems are now available for selection for a group NAT policy. These logical systems support the Translated Packet Source match type as Interface.

- **DDNS ALG**—All new ALGs supported by Junos OS Release 12.1X45 appear in the ALG drop-down box when you are creating a new protocol. These new ALGs are supported only if the Type selected is TCP, UDP, or Other .
- **3K Applications Support Per Policy**—For high-end SRX Series devices, instead of 128 services, 3072 applications per policy are now supported.
- **Original Packet Source Port for a Source NAT Rule**—Source NAT supports a source port for the original packet source. For all rules, the source port is added to the original packet source. The Source Port field is disabled for the destination NAT. The port numbers must be separated by commas, and a maximum of eight entries is allowed, including ports and port ranges.
- **Original Packet Source Port for Static NAT Source Address**—In the Original Packet Source field of Static NAT, the Address and Port fields are added.
- **Suite B Implementation for IPsec VPN**—The advanced encryption and authentication algorithms are available for the IPsec VPNs. The set of algorithms is collectively designated by the NSA as Suite B cryptography.

The following new encryption and authentication algorithms are available for IPsec VPN:

- IKE proposals
  - Group19, 20, and 24 to Diffie-Hellman groups list
  - DSA, EC-DNA-Signature-256, and EC-DNA-Signature-384 to authentication method lists
  - SHA-256 and SHA-384 to authentication algorithms list
- IPsec proposals
  - Group19, 20, and 24 to Diffie-Hellman groups list
  - AES-GCM-128, AES-GCM-192, and AES-GCM-384 to encryption methods list
- Custom proposals
  - SuiteB-GCM-128 IKE proposal set for SuiteB-GCM-128
  - SuiteB-GCM-256 IKE proposal set for SuiteB-GCM-256

You can configure the authentication method; the available methods are preshared key and RSA signatures. The IKE ID type selection is enabled for main mode and also for authentication that is based on certificates. For the certificate-based authentication method, the predefined proposal sets such as standard, basic, and compatible are not applicable. You must create a custom proposal for certificate-based authentication.

You can configure an IKE ID for the main mode VPN proposals using the available Hostname, User@hostname, and IPAddress IKE ID options.

- **Auto VPN**—Auto VPN, also known as Zero Touch Hub (ZTH), is an SRX Series feature that enables administrators to add or remove spoke devices dynamically without performing any configuration changes on the hub devices.

Security Director Release 13.1P2 includes support for the design and provisioning of Auto VPN on devices running Junos OS Release 12.1X45. During the creation of a hub and spoke VPN, a new option is available for creating an Auto VPN. This option applies only to route-based VPNs with PKI certificate-based authentication. Because this feature is supported only on devices running Junos OS Release 12.1X45, all other devices will not be available for spoke or hub selection.



**NOTE:** The Auto VPN feature is not supported on logical systems or extranet devices. Therefore, these systems and devices are filtered out from device association during Auto VPN design or modification.

- **Local ID or Remote ID Configuration**—Prior to Security Director Release 13.1P2, there was no option for customizing IKE addresses and local or remote IKE IDs for preshared key-based VPNs. In this release, a new column, IKE Address, is available during the VPN creation process. When you create a new VPN, the IKE Address column lists the selected external interface IP address; this is the default value, which you can modify. The Main Mode profile has been enhanced to support IKE ID types such as IP address, hostname, and user-at-hostname, similar to Aggressive mode. Using these configuration options, you can modify the IKE ID of each endpoint in the VPN.

## Known Issues

- IPS compile check will not run when you push the configuration using the consolidated configuration.
- In the firewall policy workspace, the preview configuration for a published policy that includes IPS does not show that IPS configuration. [PR 748307]
- In the NSM global domain pre-rules and post-rules, if the install-on setting is configured for any other subdomains, those firewall policy rules will be migrated to Security Director as rules in the group policy for the NSM global policy.

Rules that have the install-on settings for subdomains are not created within the respective migrated group policy but instead are created within the Security Director group policy that represents the NSM global policy. [PR 773985]

- Domain rule migration of NAT is not supported. In NSM, domain rules are used only for firewall policies, although NSM is capable of creating NAT policies.
- Updating NAT policies imported from a device that has proxy-ARP configured deletes the proxy-ARP configuration
- The static route command is not complete for the route-based VPN that has an extranet device as an endpoint. The command is configured on the SRX endpoint as “set routing-options static route”, and the update will pass. However, you must manually add the routing options. [PR 891368]
- When you use a routing instance in the destination pool, update fails for a device running Junos OS Release 12.1. This behavior is inconsistent with Junos OS Releases 10.3 and later. [PR 771449] [Device side PR 773264]

- Enabling auto proxy-ARP at the policy level, and disabling any specific rule, is not supported. [PR 753733]
- In Security Director, the NAT Pool Objects ILP might not load with the IE9 browser when the pool count is approximately 8192 imported from the device. [PR 754535]
- For a device that has firewall and NAT rules and that is newly added into Security Director, if you publish or update only the firewall configuration, Security Director deletes all the address objects that are referenced in NAT rules. Because NAT is not published, Security Director considers the address objects referred in NAT as unused and therefore attempts to delete them.

Workaround: After importing policy and NAT configurations from the device, you must publish both the policy and NAT. Then the update is successful. [PR 774904]

- If the Security Director application setting Delete Unused Services and service groups under Update-Device is enabled, and if you try to publish or update only the firewall configuration (with IPS enabled), Security Director deletes all the service objects that are referenced in IPS rules. Because IPS is not published, Security Director considers the service objects referenced in IPS as unused and therefore attempts to delete them. The same is true if the IPS configuration is published without the firewall configuration. Service objects referenced in the firewall configuration are deleted.

Workaround: After importing policy and NAT configurations from the device, you must publish both the firewall and NAT policies. Similarly, you must publish firewall and IPS policies together if the firewall policy with IPS is imported. Then the update is successful. [PR 774904]

- In the left pane of the firewall and NAT workspaces, the draft icon for a Device Exception policy does not appear when the policy is saved as draft. However, on collapsing or expanding the Group policy to which the Device Exception policy belongs, you can see the draft icon.

This behavior is the same for IPS device exception policies. However, the tooltip for the device exception policies shows whether or not the policy is in the draft state. [PR 870226]

- Modifying or cloning a nested address group that has more than 800 members results in an Action Failure error pop-up, and an exception is written to the server.log file. [PR 882102]
- Extra CLI output is displayed in the CLI view when you are previewing a firewall policy that includes a rule that references a Scheduler object, even when there is no issue in the XML configuration that is being pushed to a device. [PR 869752]
- Import device changes import a deactivated configuration even when there have been no changes. [PR 874217]
- If you import firewall policies that have inactive configuration nodes and then upgrade to Security Director Release 13.1, the nodes will be activated on update. To keep the node(s) inactive, you must import the node or nodes again after upgrading to Security Director Release 13.1. [PR 887148]
- When you push IPS policy to logical systems, Security Director will not generate CLI commands for addresses and applications. For the root logical systems, the CLI output

gets generated for specific addresses or applications. The user logical systems address application is configured as Any. [PR 857554]

- The audit log generated from SDK-generated REST code logs only HTTP details. Because the REST code does not have all the details required for generating the audit log, the generated code cannot create a meaningful audit log entry. [PR 878414] [PR 873589]
- Schema validation fails when you are validating the schema generated from the SDK wizard against the input XML. [PR 870905]
- If you get a resource by its ID and the resource has a collection, the total attribute always has the value as zero. [PR 870931]
- If you do not have permission to modify any devices participating in the VPN, that VPN is still displayed in the GET ALL VPNs REST API.
- The right-click preview configuration shows non-Security Director changes after a non-Security Director device change is made directly on the device. [PR 882371]
- The Pending Services information is not shown for any device on the Security Director Devices page after an upgrade from Security Director Release 13.1R1.4 to 13.1P1. [PR 902279]
- Intermittent issues occur with IPS signatures and parsing. [PR 904606]
- The Security Director Release 13.1 implementation of Consolidated Configuration is not fully compatible with the Network Application Platform Release 13.1 Consolidated Configuration. [PR 896283]
- IPv6 addresses are allowed for exclusion or negation through REST.

Workaround: Do not input IPv6 addresses with *source-address-excluded* or *destination-address-excluded* set to true. If set already, remove them from Security Director UI. [PR 917387]

## Known Behavior

- Security Director supports a maximum of 1000 records for *getAll* APIs. If there are more than 1000 records, you must use pagination to view the extra records.
- During the device import or the NSM migration of large policies, a job failure might happen because of a transaction timeout. Select the number of devices such that the total number of rules is not more than 10,000.

Workaround:

- To import more devices at a time, increase the transaction timeout using the following instructions. In the Junos Space server console, go to `/usr/local/jboss/server/all/conf/jboss-service.xml`. In this file, navigate to the following snippet:

```
<!-- JBoss Transactions JTA -->
<mbean code="com.arjuna.ats.jbosstx.jta.TransactionManagerService"
name="jboss:service=TransactionManager">
  <attribute name="TransactionTimeout">1800</attribute>
</mbean>
```



```
name="ObjectStoreDir">${jboss.server.data.dir}/tx-object-store</attribute>
</mbean>
```

- Increase the transaction timeout value to 3600 (depending upon the number or size of the imported or migrated policies).
- Restart the jboss by issuing the **service jboss restart** command.

## Resolved Issues

- During the provisioning of a full-mesh IPsec VPN, the VPN publish fails with the message *The specified area Id 0 is already used in device*. [PR 912541]
- Proxy-ARP statements are sent to a device even when NAT rules are disabled. [PR PR 905310]
- Ability to configure *local-identity* and *remote-identity* parameters for Main mode in the Junos Space GUI. [PR 880622]
- Issue with search when the search string has white space in between the lines. [PR 909861]
- While creating a destination NAT rule, you are given the option to specify a port range. This is confusing, because destination NAT does not support the original destination packet port range configuration. [PR 884341]

## Errata and Changes in Documentation for Security Director Release 13.1P1

The following section provides the documentation errata for this release.

- In the *Junos Space Security Director User Guide* the sections “Creating Static Signature Groups” and “Creating Dynamic Signature Groups” incorrectly state that static and dynamic signature groups can be created from the Actions drawer. To create a static signature or dynamic signature groups, right-click the signature and select **Create Static Group** or **Create Dynamic Group**.

## Junos Space Documentation and Release Notes

---

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security,

reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

## Documentation Feedback

---

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>

- Join and participate in the Juniper Networks Community Forum:  
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

## Revision History

---

—

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.