

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

## Release Notes

**Release 13.1**  
**30 May 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 .....	2
Supported Junos OS Releases .....	3
Supported Browsers .....	3
Management Scalability .....	3
New Features .....	3
Known Issues .....	6
Resolved Issues .....	9
Junos Space Documentation and Release Notes .....	10
Documentation Feedback .....	10
Requesting Technical Support .....	11
Self-Help Online Tools and Resources .....	11
Opening a Case with JTAC .....	11
Revision History .....	12

## 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](#)
- [New Features](#)
- [Known Issues](#)
- [Resolved Issues](#)

### Installing Security Director

Security Director 13.1 can be deployed only on Network Application Platform Release 12.3R1.3 with Network Application Platform Patch 12.3P2.8. Install Network Application Platform 12.3R1.3 and upgrade to Patch 12.3P2.8 before installing Security Director.

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

### Supported Devices

Security Director 13.1 is supported on the following SRX Series hardware devices:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX550
- SRX650
- SRX1400
- SRX 3400
- SRX 3600
- SRX 5600
- SRX 5800
- LN 1000

## Supported Junos OS Releases

- Security Director 13.1 supports the following Junos OS Release:
  - 10.4
  - 11.4 and later releases
  - 12.1X44-D10
- 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, it is recommended that the exact matching Junos OS schema is installed on the Junos Space 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.

## New Features

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

- **Scheduler**—You can create a scheduler for a policy to be active during a scheduled time. You can create a new scheduler for a policy or link the policy to an existing scheduler. When a scheduler timeout expires, the associated policy is deactivated and all sessions associated with the policy are also timed out.
- **IPS Import from the Device**—From Security Director Release 13.1 onwards, Security Director supports import of IPS policies along with firewall and NAT policies from a device. All objects supported by Security Director are imported during the policy import

process. Rules that contain objects not supported by Security Director are imported with the disabled rule state.

- **Certificate-Based VPN**—When creating a VPN profile, you can configure the authentication method; the available methods are pre-shared key, RSA, and DSA signatures. The IKE ID type selection is enabled for main mode as well, if the authentication is based on certificates.
- **NAT Policy Versioning**—NAT policy versioning can be performed by taking a snapshot of the policy. Snapshots for all types of policies can be created, including group and device exceptions. This feature also supports rolling back to a previous version, and comparing two arbitrary versions. A snapshot is captured automatically when a policy is published.
- **Policy Versioning - Overwrite Last Version**—The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you can delete the unwanted versions before taking a new version snapshot. Security Director automatically deletes the older version of snapshots. The Auto delete oldest version option facilitates this action. This option is enabled by default.
- **TCP Options in Policy Profile**—A new TCP session options are added in the Advanced Settings section of the new Policy Profile page. The available TCP sessions options are:
  - TCP-SYN Check
  - TCP Sequence Check
- **Push Disabled Rules**—You can optionally choose to push the disabled rules to a device by selecting the Update disabled rules to device option in the Security Director application setting, under Platform.
- **Rerun Failed Update Jobs**—Security Director allows you to rerun updates on failed devices. The Job Management framework gives you the option of retrying a job on all or a subset of the main objects, such as devices. You can retry a job more than once. The failed objects list reflects the jobs you choose to retry.
- **Custom VR Support**—The custom routing instance is now available for dynamic protocols (OSPF and RIP) similar to static or no-routing options. You can add the routing instance while creating a new VPN or modifying an existing VPN.
- **Import CLI Device Changes Only**—This feature allows you to import changes made in a device for firewall, NAT, and IPS policies, and to import the associated object changes back to Security Director.
- **Usability Improvements**—The following usability improvements are made in object builder, policies, search, and publish and update:
  - The newly added rule blinks a different color for a few seconds. The behavior is the same if you add a new rule before or after a rule, clone a rule, or paste a rule. This is applicable for firewall, NAT and IPS policies.
  - In all the group selector windows, you can select all addresses or services listed in the Available column by selecting Page and then copy them to the Selected column. If you want to unselect all, click **None**.

- You can now create an address group inline, in addition to the existing ability to create an address object inline.
- In the left pane of the policy, you can choose the Hide policies Without Devices assigned filtering option to filter out devices and group policies that are not assigned to any device. This is applicable for firewall, NAT, and IPS policies.
- You can perform advanced searches on the rule description for firewall, NAT, and IPS policies. For firewall policies, you can include custom columns in the advanced search.
- You can perform copying and pasting of rule groups similar to copying and pasting of rules. This feature is applicable for firewall, NAT, and IPS policies.
- You can cut rules in addition to copying rules. Save the policies prior to cutting and pasting the rules between two policies.
- You can reorder the rules across the Pre Rule and Post Rule of a group policy. This feature is applicable only for firewall policies.
- Whenever you make any changes to a firewall policy, a NAT policy, an IPS policy, or a VPN, you will have the option of entering the comments before saving these services. You can enable this option from Platform > Administration > Application. By default, this option is disabled.
- You can perform the following various rule operations on the filtered list of rules:
  - Add a rule before
  - Add a rule after
  - Paste a rule before
  - Paste a rule after
  - Clone a rule
  - Move a rule to top
  - Move a rule to bottom
  - Move a rule up
  - Move a rule down
- You can set an option to take a snapshot automatically after you have modified and saved a policy after a configured number of times. This setting is configurable in the Security Director application settings.
- You can use the available tooltip view to see information about VPN profiles. To see the tooltip for a VPN profile, move the mouse over the profile for which details are required. The tooltip displays the high-level information.
- If you have any cut or copied rules or rule groups, you will have a Paste Rules link, in addition to the Create Pre Rule and Create Post Rule links, to use to paste the rules or rule groups. This is applicable for firewall and NAT policies

- In the Job Details window, use the available filter box to search for any device by device name, tag name, or IP address. Filtering works only for the available devices. This feature is applicable for firewall, NAT, and IPS policies.
- You can validate a policy for any errors by clicking the Validate button, available next to the Save and Discard buttons. If any errors are found during the validation, a red warning icon is shown for the respective policies. This feature is available for firewall, NAT, and IPS policies.
- Security Director permits you to save policies that contain errors. Warning messages are displayed for policies that contain errors, but you can still save such policies as drafts. This feature is available for firewall, NAT, and IPS policies.
- You can sort IP addresses in ascending or descending order in the IP Address column. For address range and network type, IP addresses are sorted by the first two digits.
- You can now create the NAT pool object inline. You can perform the following operations on the NAT pool objects similar to Address and Service objects:
  - Displaying duplicate objects with merge option
  - Displaying unused objects with delete option
  - Finding usage of NAT pool objects
  - Replacing NAT pool objects
- During the policy import, in the Object Conflict Resolution window, you can copy the action value from one row, and paste to multiple or all rows.
- You can copy a cell from a firewall, IPS, or NAT rule and paste it into the same column in one or more other rules. This will result in copying the column value from one row to one or more selected rows. You can copy data only for the same column types.
- **REST APIs**—The following read and write REST APIs are supported by Security Director:
  - Firewall policy and Objects
  - VPN

## Known Issues

The following issues are still outstanding in the Junos Space Security Director Release 13.1.

- IPS compile check will not run when you push configuration through 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]
- After the upgrade, the policy IDs are shown in the Pending Services column instead of the policy names, and for VPNs, no VPN name is displayed.

Workaround: To display the policy and VPN names in the Pending Services, you must republish the published policies and VPNs. This is valid only when you upgrade Security Director Release 12.1 to Security Director Release 12.2.

- 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 Design 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 Security Design group policy representing 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 has the capability 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 end point. The command is configured on the SRX endpoint as "set routing-options static route", and update will pass. However, you must manually add the routing options.
- When you use a routing instance in the destination pool, update fail 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 possible. [PR 753733]
- In Security Design, the NAT Pool Objects ILP might not load with IE9 browser when the pool count is approximately 8192 imported from the device. [PR 754535]
- After upgrading from Security Design Release 12.1, a group policy with IPS mode None and a device exception of IPS mode Basic or Advanced, is not shown on the left pane of IPS policy.

Workaround: Modify the policy, change the IPS mode, and save.

- During the device import or the NSM migration of large policies, job failure might happen because of a transaction timeout.

Workaround:

- 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.jbossatx.jta.TransactionManagerService"
name="jboss:service=TransactionManager">
  <attribute name="TransactionTimeout">1800</attribute>
  <attribute
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.

- For a device, having firewall and NAT rules, that is newly added into Security Director, if you publish or update only firewall, Security Director deletes all the address objects that are referred 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 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 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]

- Modify or clone of a Nested Address Group having more than 800 Members throws Action Failure error pop-up and an Exception at server.log file. [PR 882102]
- Extra CLIs are displayed in the CLI view when previewing the firewall policy having a rule referring to a Scheduler object, even though there is no issue in XML configuration pushed to a device. [PR 869752]
- Import device changes is importing deactivated configuration even when there was no changes. [PR 874217]
- If you import firewall policies having inactive configuration nodes and then upgrade to Security Director Release 13.1, the nodes will get activated on update. To keep the node(s) inactive, you must import it again after upgrade to Security Director Release 13.1.
- When you push IPS policy to logical systems, Security Director will not generate CLIs for addresses and applications. For the root logical systems, the CLI gets generated for specific addresses or applications. In case of user logical systems address, application is configured as Any.
- The audit log generated from SDK-generated REST code is logging only HTTP details. Because the REST code does not have all the details required for generating the audit log, the generated code is not able to 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 is always having the value as zero. [PR 870931]
- If you do not have permission to any devices participating in the VPN, that VPN is still displayed in the GET ALL VPNs REST API.
- Security Director supports maximum of 1000 records for *getAll* APIs. If number of records are more than 1000, you must use pagination for the same.



## Resolved Issues

The following are the issues that have been resolved in Junos Space Security Director Release 13.1.

- The firewall Advance Search does not filter the expected results when you search with protocol number at Service field. [PR 874528]
- Preview on LSYS devices shows a warning saying the current number of rules or objects are exceeded even the device does not configured with any reserved quota.

Resolution: The warning message has changed to display appropriate message:  
[Warning] Reserved quota is not specified in the security-profile for <quota name as in CLI>. [PR 874578]

- Publish and Update Job management summary results of Failed and Passed states do not match with total number of devices. [PR 875870] [PR 878895]
- Create or Modify rule group header does not allow space and colon characters. [PR 880700]
- Double click details are not shown for Address group having more than 700+ members. [PR 881048]
- Security Director NSM DB migration is ignoring line breaks in the comments field. [PR 850260]
- Security Director adding an address to an address group does not result in the proper update on the next device update. [PR 854195]
- When the cluster device is deleted from Device Management without unassigning it from Device policy, the policy becomes invisible from Security Director GUI but still be available under Security Director database (sm\_db). [PR 858094]
- Enhancement request to add a scroll bar for Description field in firewall policy rules. [PR 865104]
- Device import fails when referred address in firewall rules is not created in address book (possible if rules are deactivated). [PR 866562] [PR 869745]
- The Junos Space VPN policy publish is randomly deleting routes and adding old VPN settings. [PR 868170]
- The source NAT rule with original destination address as Any and with Pool as translated address when upgraded from Security Director Release 12.1 to 12.2, publish fails. [PR 846314]
- Security Director Import Devices fails without a detailed reason. [PR 869745]
- Export of security policy in Security Director does not include UUID for MS-RPC Applications. [PR 880228]
- Policy rollback to an automatic snapshot taken earlier does not work. [PR 881540]
- While trying to change the *label* on an existing template, regular expression for this node cannot be modified error received. [PR 870478]
- In Security Director Patch Release 12.2P1.7, IPS push is failing. [PR 871224]

- Multiple issues with Job Details. [PR 878150]  
Resolution;
  - Sorting by status and device Name
  - Search by device IP, name and tag
  - Auto refresh the status for the devices
  - Resizing the table data along with the form
- Assign Devices to Service list is empty. [PR 878891]

#### Related Documentation

---

### 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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.