

# Junos<sup>®</sup> Space Security Director 13.1P1

## Release Notes

Release 13.1P1  
7 October 2013  
Revision 1

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
New Features . . . . .	4
Known Issues . . . . .	6
Known Behavior . . . . .	9
Resolved Issues . . . . .	9
Errata and Changes in Documentation for Security Director Release 13.1P1 . . . . .	10
Junos Space Documentation and Release Notes . . . . .	10
Documentation Feedback . . . . .	11
Requesting Technical Support . . . . .	11
Self-Help Online Tools and Resources . . . . .	11
Opening a Case with JTAC . . . . .	12
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](#)
- [Known Behavior](#)
- [Resolved Issues](#)
- [Errata and Changes in Documentation for Security Director Release 13.1P1](#)

### Installing Security Director

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

If you do not have Security Director deployed already, perform the following steps:

1. Install Network Application Platform Release 13.1R1.6 and upgrade to Network Application Platform Release 13.1P1.14.
2. Install Security Director Release 13.1P1.2

If you have Security Director deployed already, perform the following steps:

1. From Network Application Platform Release 12.3P2.8 and Security Director Release 13.1R1.4:
  - a. Upgrade to Network Application Platform Release 13.1R1.6 and Network Application Platform Release 13.1P1.14
  - b. After Step a is done, upgrade to Security Director Release 13.1P1.2.



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

---

2. From Network Application Platform Release 12.3R1.3 and Security Director Release 12.2P1.7:
  - a. Upgrade to Network Application Platform Release 12.3P2.8 and Security Director Release 13.1R1.4.

- b. After Step *a* is done, upgrade to Network Application Platform Release 13.1R1.6 and 13.1P1.14 respectively and Security Director Release 13.1P1.2.



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

3. From Network Application Platform Release 12.2P1.4 and Security Director Release 12.2R1.3:
  - a. Upgrade to Network Application Platform Release 12.3R1.3 and 12.3P2.8 respectively and Security Director Release 13.1R1.4.
  - b. After Step *a* is done, upgrade to Network Application Platform Release 13.1P1.14 and Security Director Release 13.1P1.2.



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

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

## Supported Devices

Security Director 13.1P1 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 13.1P1 supports the following Junos OS releases:

- 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, we recommend that you have the exact matching Junos OS schema 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 13.1P1 application includes the following new features:

- **Spoke-to-Spoke Communication for Static Routes**—Security Director provides an option at the VPN level to enable spoke-to-spoke communication with static routes. You can enable this option only for a hub-and-spoke VPN with static routing when you create or modify the VPN. By default, this option is not checked, and you can check or uncheck this option during the modify workflow.
- **Device Search Option in Assign Devices Window of Group Policy**—You have the option of searching for any devices in the Selected column (the right-hand side of the device selector) of the Assign Devices window. This is applicable only for Assigned Devices of the firewall and NAT group policies and IPsec VPNs..

- **Export of Security Director Devices Page**—You can export all the columns on the Security Director Devices page to a CSV file. You cannot select a device or devices and export only those devices to a CSV file. However, you can apply filters to the list of devices and export the filtered data to a CSV file.
- **Export of Job Details and Filtering Option**—You can export the job details of publish or preview and update jobs to a CSV file. The messages columns will also be captured in the exported CSV file. A filter option is available for all the columns in the Job Management workspace.
- **Mechanism for Showing the Policies Assigned and Installed on Devices and Exporting Them to CSV**—Two new columns are present on the Security Director Devices page: Assigned Services and Installed Services. Versioning information is added for the services listed under the Pending Services and Installed Services columns. The versioning information is available only for firewall and NAT policies.

Search options are available for the Assigned Services, Pending Services, and Installed Services columns, and for the type of services. The following search criteria are applicable for the search option that is available on the Security Director Devices page:

- Searching with an OR combination is not supported.
- Searching with compound negate is not supported.
- Compound search queries with AND and negate are supported.

Use the following keywords to search for a particular service:

- For an assigned service name, use the *assignedServices* keyword.

For example, use *assignedServices:storesrx* to list all the devices that are assigned to the *storesrx* firewall policy.

Use *-assignedServices:storesrx* to list all the devices that are not assigned to the *storesrx* firewall policy.

- For an assigned service type, use the *assignedServiceTypes* keyword. This finds all devices having minimum one firewall policy use. This keyword applies to firewall, NAT, IPS, and VPN policies.

For example, use *-assignedServiceTypes:FWPolicy* to list all the devices that are not assigned to any firewall policy.

Use *-assignedServiceTypes:FWPolicy AND assignedServiceTypes:NAT* to list all the devices that are not assigned to any firewall policy but that are assigned to any NAT policy.

- For pending service name, use the *pendingServices* keyword.

For example, use *pendingServices:(storesrx)* to find all devices where *storesrx* is published and the update is pending.

Use *-pendingServices:(storesrx)* To find all the devices that do not have policies with name having text *storesrx* published.

- For pending service type, use the *pendingServiceTypes* keyword. This keyword applies to firewall, NAT, IPS, and VPN services.

For example, use *pendingServiceTypes:FWPolicy* to list all the devices that have any firewall policy as a pending service.

The keyword *pendingServiceTypes:FWPolicy AND pendingServiceTypes:NAT* to list all the devices that have firewall and NAT policies as pending services.

- For installed service name, use the *installedServices* keyword.

For example, use *installedServices:storesrx* to list all the devices with firewall policy *storesrx* updated on it.

Use *-installedServices:storesrx* to find all devices where *storesrx* is not updated.

- For installed service type, use the *installedServiceTypes* keyword. This keyword applies to firewall, NAT, IPS, and VPN policies.

- **Deletion of all Firewall Policies**—Security Director does not allow deletion of all the firewall policies on a device. The Update job fails if all the firewall policies would be deleted on the device.

The warning messages are displayed during the update and preview workflow if you attempt to remove all firewall policies. For the preview workflow, the following warning message appears: *Device Update job will fail because the Update will remove all Firewall Policies from the device. Security Director does not support deleting all Firewall Policies.* For the update workflow, the following warning message appears: *Device Update failed because all Firewall Policies would have been deleted on device update. Security Director does not allow deleting all Firewall policies.*

- **Delete Unused Services and Service Groups**—A new option is available under Administration > Applications > Modify Application Settings > Update-Device for deleting all the unused services and service groups. Select the Delete unused Services and Service groups option to delete all the unused services and service groups. By default, this option is enabled whenever you perform a fresh install of Security Director or upgrade from the previous release.

If the option is enabled, Security Director will manage the services in the same way it manages addresses. Security Director will always delete the unused services (those services that are not referenced by any policy on the device) from the device during publish or update. If the option is disabled, Security Director will never try to delete services from the device, even if the service is unused on a device.



**NOTE:** A *service* in Security Director refers to an application on a device.

---

## Known Issues

- 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]

- 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. [PR 891368]
- 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]
- 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]

- 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 firewall (with IPS enabled), Security Director deletes all the service objects that are referred in IPS rules. Because IPS is not published, Security Director considers the service objects referred in IPS as unused and therefore attempts to delete them. Same is true if IPS is published without publishing firewall. Service objects referred in firewall are deleted.

Workaround: After importing policy and NAT configurations from the device, you must publish both the firewall and NAT policies. Similarly publish firewall and IPS together if firewall policy with IPS is imported. 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. [PR 887148]
- 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. [PR 857554]
- 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.
- 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 is not shown for any device in Security Director Devices page post upgrade from Security Director Release 13.1R1.4 to 13.1P1. [PR 902279]
- Intermittent issue with IPS signature and parsing. [PR 904606]
- Security Director Release 13.1 implementation of Consolidated Configuration is not fully compatible with Network Application Platform Release 13.1 Consolidated Configuration. [PR 896283]
- Security Director search: Issue with search when the search string has white space in between. [PR 909861]

Workaround: Search the substring of the service name within brackets to get all the matching services. if there are multiple services having the substring, use AND and – with service types to get particular service matching results.



The following example shows service names having space characters and substrings same that of multiple services. If there are services with names *Retail Store Policy* and *Store 06082013*:

- To search for devices assigned to service *Retail Store Policy*, use *assignedServices:(Retail) AND assignedServices:(Store)*.
- To search for the devices assigned to service *Store 06082013*, use *assignedServices:(Store) AND assignedServices:( 06082013)*.
- If a similar name exists for NAT and firewall services, use *assignedServiceTypes* to search for specific service assigned devices. Use *assignedServices:(Retail) AND assignedServices:(Store) AND assignedServiceTypes:(FWPolicy)*.
- To filter the devices which has matching service name *Store* and other than service type NAT, use *assignedServices:(Store) AND -assignedServiceTypes:(NAT)*.

## Known Behavior

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

## Resolved Issues

- Security Director wiped out security policies. [PR 886627]
- Reports mapping devices and policies. [PR 885787]
- The selection box to select or deselect devices added to a group policy does not order anything on the right hand side and does not permit searching. [PR 886630]
- Multiple issues with Job Details. [PR 878150]

- Hub and Spoke VPN Config pushed to the devices does not include routes for the spoke devices. [PR 874149]
- Refresh certificate does not work on cluster. [PR 892495]
- Cannot import config from SRX3600 cluster, Platform 12.3P2.8, and Security Director 13.1R1.4. [PR 896264]
- Security Director import devices fails without a reason. [PR 897210 ]
- Not able to import policies for one of two LSYS on SRX 3600 using Security Director. [PR 895030]
- Security Director Release 13.1 sends command to delete service object and causes update failure. [PR 889731]
- Network Application Platform failed to perform security policy update to SRX 5800. [PR 888775]
- The timeout value 129600 of a service object is rejected. [PR 892790]
- After upgrading to Security Director Release 13.1, the firewall policies do not load up. [PR 894456]
- Security Director Release 13.1 copy and paste of a rule seems to ignore changes to source-zone of the new rule and marks it as a duplicate. [PR 895826]
- Network Application Platform keep reverting zones to default after saving policy. [PR 891090]
- Security Director is creating multiple identical service group objects with identical services in the set. [PR 891867]

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

The following section provides the documentation errata for this release.

- In *Junos Space Security Director User Guide* the sections on Creating Static Signature Groups and Creating Dynamic Signature Groups incorrectly mentions 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

---

October 7, 2013—Revision 1

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.