

# Junos<sup>®</sup> Space Security Director 13.3R2

## Release Notes

Release 13.3R2  
13 August 2014  
Revision 2

### Contents

Security Director Release Notes . . . . .	2
Installing Security Director . . . . .	2
Upgrade Prerequisites . . . . .	3
Upgrading Security Director . . . . .	3
Upgrading Log Collector . . . . .	4
Upgrading Log Director . . . . .	4
Supported Devices . . . . .	5
Supported Junos OS Releases . . . . .	5
Supported Browsers . . . . .	6
Management Scalability . . . . .	6
Features and Enhancements . . . . .	6
Known Issues . . . . .	7
Known Behavior . . . . .	11
Addressed Issues . . . . .	11
Junos Space Documentation and Release Notes . . . . .	12
Documentation Feedback . . . . .	12
Requesting Technical Support . . . . .	12
Self-Help Online Tools and Resources . . . . .	13
Opening a Case with JTAC . . . . .	13
Revision History . . . . .	13

## 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 IPS and application firewall licenses.)

- [Installing Security Director](#)
- [Upgrade Prerequisites](#)
- [Upgrading Security Director](#)
- [Upgrading Log Collector](#)
- [Upgrading Log Director](#)
- [Supported Devices](#)
- [Supported Junos OS Releases](#)
- [Supported Browsers](#)
- [Management Scalability](#)
- [Features and Enhancements](#)
- [Known Issues](#)
- [Known Behavior](#)
- [Addressed Issues](#)

### Installing Security Director

Security Director 13.3R2 requires Junos Space Network Application Platform Release 13.3R2.

When one of the following scenarios occurs, deployments using Junos Space Security Director 13.3R2 on the JA1500 hardware appliance or VMware virtual machine with 8 GB of RAM or less can incur significant degradation in system performance and memory.

- The number of firewall rules published simultaneously is 8,000 or more. The 8,000 threshold can be reached by a single user publishing or updating a single firewall policy that has 8,000 firewall rules, or two users simultaneously publishing or updating two firewall policies that each have 4,000 firewall rules.
- The number of firewall rules published or updated simultaneously is 4,000 or more, and several administrators make changes within Security Director or Network Application Platform at the same time. The 4,000 threshold can be reached by a single user publishing or updating a single firewall policy that has 4,000 firewall rules, or two users simultaneously publishing or updating two firewall policies that each have 2,000 firewall rules.

The issue is related to the number of simultaneous firewall rules published and not the number of devices managed by Security Director.

Network Management Platform Release 13.3 and Security Director Release 13.3 require more system memory to operate than earlier releases.

To avoid the issues stated, perform one of the following tasks prior to upgrading to Security Director Release 13.3R2:

- Migrate your Security Director installation from the JA1500 hardware platform to the new JA2500 hardware platform.
- Migrate your Security Director installation from the JA1500 hardware platform to a VMware virtual machine using a minimum of 16 GB RAM (32 GB RAM is recommended).
- Increase the RAM allocation for any VMware virtual machine deployments to a minimum of 16 GB RAM (32 GB RAM is recommended).

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

1. Install Network Application Platform Release 13.3R2.6.
2. Install Security Director Release 13.3R2.7.

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

## Upgrade Prerequisites

To upgrade Security Director, Log Collector, and Log Director, the following prerequisites must be met:

- Upgrade Network Management Platform Release 13.3R1.9 to Network Management Platform Release 13.3R2.6 before upgrading Log Collector and Log Director.
- Ensure that you follow the upgrade order mentioned.



**NOTE:** The procedure is same for virtual environments and JA2500 appliances.

## Upgrading Security Director

To upgrade Security Director Release 13.3R2, perform the following steps:

1. Download **Security-Director.13.3R2.7.img** file from [Download Site](#).
2. Select **Administration>Applications>Security Director**. Right-click and select **Upgrade Application**.

Upload the image using **Upload via HTTP** or **Upload via SCP** options.

3. Click **Upgrade**.

The Job Management tab shows the upgrade status.



**NOTE:** When the setup includes Log Collector, Log Director, and Security Director, upgrading Security Director automatically upgrades Security Director logging and reporting module.

Log Director is upgraded using Log Collector and Log Director component. Upgrade Log Collector followed by Log Director upgrade.

---

## Upgrading Log Collector

To upgrade Log Collector, perform the following steps:

1. Download **Log-Collector-Upgrade.13.3R2.X.img** file from [Download Site](#).
2. Select **Administration>Applications>Log Director**. Right-click and select **Upgrade Application**.

Upload the image using **Upload via HTTP** or **Upload via SCP** options.

3. Click **Upgrade**.

The Job Management tab shows the upgrade status.



**NOTE:** The Log Collector version is not displayed under **Applications>Log Director**. The Log Collector subsystem is upgraded in the background.

The upgrade package for Log Collector is same for both JA2500 appliance and virtual deployments.

---

## Upgrading Log Director

To upgrade Log Director R1.4 to Log Director R2.x application, perform the following steps:

1. Download **Log-Director-ESX.13.3R2.X.img** file from [Download Site](#).
2. Select **Administration>Applications>Log Director**. Right-click and select **Upgrade Application**.

Upload the image using **Upload via HTTP** or **Upload via SCP** options.

3. Click **Upgrade**.

The Job Management tab shows the upgrade status.



.....

**NOTE:** The Log Director version is displayed under Applications after the upgrade.

The same package is used for fresh install of Log Director in Virtual deployments.

The upgrade package is same for both JA2500 and virtual deployments.

.....

## Supported Devices

Security Director 13.3R2 is supported on the following SRX Series hardware devices and LN Series hardware device:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX550
- SRX650
- SRX1400
- SRX3400
- SRX3600
- SRX5400
- SRX5600
- SRX5800
- LN1000-V

## Supported Junos OS Releases

- Security Director 13.3R2 supports the following Junos OS branches:
  - 10.4
  - 11.4
  - 12.1
  - 12.1X44
  - 12.1X45

- 12.1X46
- 12.1X47
- SRX Series devices require Junos OS Release 12.1 and later releases to synchronize the Security Director description field with 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
- Chrome
- 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 and Enhancements

The Junos Space Security Director 13.3R2 application includes the following new features and enhancements:

- **Reports**—Beginning in Junos Space Security Director 13.3R2 logging and reporting provides reporting functionality. Using reports, you can schedule reports daily, weekly, or monthly, and configure them to include multiple criteria. You can also personalize the reports by adding company logo, footer, and so on. When the system generates a report, you and other designated recipients receive the report in PDF format via e-mail. Reports enable you to perform trend analysis of your network activities.
- **Enhanced Event Viewer support**—Event Viewer has the following enhancement:
  - Additional columns added.
  - Legends to event viewer graph added.

- Export to comma-separated file (CSV) option added to enable exporting event data into CSV format. You can feed this data to another system or tool for analysis.
- Options to create alerts, monitors, and reports are added.
- Time span selection enhanced.
- Capability to drag and drop columns to change the sequence added.
- Capability to save selected columns in filter added.
- **Enhanced dashboard support**—Dashboard has the following enhancement:
  - Capability to drag and drop dashboard added.
  - Legends to dashboard graph added.
- **Enhanced filter management**—Filter management has the following enhancement:
  - Address resolution capability for advanced filter.
  - Support for lower case key names and values in the drop down list.
  - Filter string validation and error or warning display.
- **Enhanced alerts support**—Alerts functionality now supports new **Groupby** fields for alert creation.
- **Junos OS Release 12.1X47 features**—The following Junos OS Release 12.1X47 features are supported in Security Director Release 13.3R2:
  - **Multiple firewall zones and multiple NAT ports with service**—Beginning in Junos OS Release 12.1X47, Security Director supports creation of multiple zones in the fromZone and toZone fields in match criteria. This is available for the Global firewall policy users. Also, Security Director supports creation of multiple destination ports and port ranges during the configuration of NAT rules. You have an option to specify services as part of the match criteria in a source and destination NAT rule.
  - **Application firewall enhancement-ngAppID2.0**—Security Director now supports a new application signature called ngAppID2.0 for application firewalls. With ngAppID2.0, the applications signature is enhanced to support both applications and nested applications signatures. Beginning in Junos OS Release 12.1X47 and later, the representation of nested applications is removed, and all nested applications are called applications.

## Known Issues

- Upgrading Log Collector sets the Log Director application to the undeployed state in the Junos Space Network Application Platform database. [PR 1002339]  
Workaround: Upgrade the Log Director application.
- In Event Viewer, when multiple filter criteria are used and the field value for the first criteria is invalid, then autosuggestion is not displayed for subsequent filter conditions. [PR 997069 ]

- Uninstalling Log Director or the Security Director Logging and Reporting module makes the Security Director Dashboard blank. [PR 1003353]

Workaround: Restart JBoss.

- Upgrading Security Director sets the logging and reporting module to the undeployed state in the Junos Space Network Application Platform database, even though the dependent Log Director is present. [PR 1002358]

Workaround: Upgrade the Log Director application.

- When you use the CLI to manually configure time settings (without using an NTP server) on Network Management Platform, rebooting the appliance retains the configured time zone but does not retain the correct time. Ensure that you manually configure the Space server time following a Space appliance reboot event. [PR 987118]
- Security Director is not upgraded if you select the Logging and Reporting option from the right-click menu. [PR 996632]

Workaround: Select the option Log Director.

- Reports module adds a set of default reports along with default event filters, but these filters are not be available in Event Viewer for the first time.

Workaround: Visit the Reports page first, for all the default event filters to be copied to the Event Viewer permanently.

- The create exempt rule displays zone information for logical systems. [PR 857554]
- The create exempt rule creates address object in the child domain even when a global domain address object exists. [PR 1004986]



**NOTE:** Logs of logical system assigned to the child domain is seen in the global domain as well as its child domain.

---

- Setting the report end time schedule to a past time, displays the following validation message **end date must be greater than or equal to start date**. [PR 1006969]

Workaround: Enter the end time greater than the start time.

- Scheduling a bi-weekly report does not schedule the report jobs at the appropriate bi-weekly time or date. [PR 1002508]
- The NSR rpd crashes when the mirror pipe boots up after the 8.4-20070326 software build has been installed. [PR 100469]
- Security Director deletes the predefined UTM profiles if they are modified in a device and not used in the firewall policy. Because this condition is not allowed on a device, the update fails.

Workaround: Revert the changes made for the predefined objects on a device. You can clone the predefined objects on Security Director and make the required changes. [PR 959961]

- The import OCR process shows a conflict with the global domain instead of with the child domain. [PR 983029]

- View Device Change shows older configuration changes along with the latest changes, even though the older changes were made before the Security Director update and latest device changes. [PR 969048]
- If UTM custom objects are used on a device, after an upgrade the device must be imported again and assigned to the imported policy.
- Security Director enables you to configure many global settings and all types of supported engines on SRX Series devices; however, you cannot set the active engine types through Security Director. You must manually configure the type of engine on SRX Series devices out of band. This applies to antivirus and webfiltering features which have multiple engine support.

Use the following CLI commands to configure the engine type:

- **set security utm feature-profile web-filtering type <web-filtering-engine-type>**
- **set security utm feature-profile anti-virus type <anti-virus-engine-type>**
- When you access the Security Director charts and Export to CSV jobs using IE8, if you click any chart the following message appears: **Statistics:I/O error.**

Workaround: Perform the following steps and try again:

1. Start the registry editor.
2. For a per-user setting, locate the following registry key:  
**HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings**
3. For a per-computer setting, locate the following registry key:  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings**
4. On the Edit menu, click **Add Value**.
5. To override the directive for HTTPS connections, add the following registry value:  
**BypassSSLNoCacheCheck"=Dword:00000001**
6. To override the directive for HTTP connections, add the following registry value:  
**BypassHTTPNoCacheCheck"=Dword:00000001**
7. Quit the registry editor.

[PR 986732]

This is a known issue in Microsoft IE8. Microsoft has published a KB article for this issue: <http://support.microsoft.com/kb/323308>.

- If the Security Director application running Release 13.1P1.2 is installed on the Junos Space Network Application Platform running Release 13.1P1.14, and if you upgrade Network Application Platform to Release 13.3R1, you cannot uninstall the Security Director application from the Platform. [PR 961862]

Workaround:

- Uninstall the Security Director application before upgrading Network Application Platform to Release 13.3R1.

OR

- If Security Director is in the disabled state when you upgrade Network Application Platform to Release 13.3R1, upgrade Security Director to Release 13.3R1 instead of uninstalling the application.
- If you expand a group policy that has more than 1,000 devices, a warning message is displayed stating that loading of these devices takes time. After some time, another warning message is shown, asking if you want to stop the script from running. This behavior is observed only in IE 8.0.

Workaround: To fix this problem for IE8 browsers, see <http://support.microsoft.com/kb/175500>. [PR 941609]

- In some browsers, if a monitor has many data points, the data in the graph has rendering issues the first time, and also when you manually refresh the browser window. [PR 963893]

Workaround: Refresh the monitor that has the rendering issue.

- Device monitors, VPN monitors, alerts, and EPS monitoring stop working if you cancel the following jobs:
  - **SystemPollForVPNsInLR**
  - **SystemPollForDevicesInLR**
  - **SystemPollForAlertsInLD**
  - **SystemPollForEPSsInLD**

- Adding special node might not build the cache on secondary node in a Platform fabric multi-node setup. If this is the case, the dashboard, and event viewer do not display any information. [PR 988077]

Workaround: Restart or reboot Jboss for the Platform node to rebuild the cache.

- Jump to Event Viewer options might not display the control plane logs.

Workaround: View complete data by unchecking the Security Logs Only option in Event Viewer.

- From the Junos Space Network Management Platform, uninstalling Log Director does not remove Log Collector, Reporting Devices, and Global Settings links under Administration > Logging. No action will be taken when you click these links.
- Route-based, site-to-site, and hub-and-spoke VPNs in aggressive mode are not displayed on the VPN monitor. [PR 976745]
- The VPN monitor does not update to display the deletion of a VPN from Junos Space Security Director. [PR 971453]
- The Security Director logging and reporting module displays policy rule changes only if you have not changed the policy after an update.
- VPN monitors do not display policy-based VPN information. [PR 971450]
- All logical system (LSYS) device logs are displayed in the parent device domain or global domain.

## Known Behavior

1. 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/bin/jboss-cli.sh --controller=<WEBIP>:9999 --connect</WEBIP> .`

You will get a new prompt `[domain@<WEBIP>:9999 /]`

2. Under this prompt enter the following command:

```
/profile=full-ha/subsystem=transactions/:write-attribute(name=default-timeout,value=8000).
```

The *value* parameter is configurable.

The Outcome tag in the output must read "success". The sample output is as shown in the following snippet:

```
{
  "outcome" => "success",
  "result" => undefined,
  "server-groups" => {"platform" => {"host" => {"dev" => {"server1" =>
{"response" => {
  "outcome" => "success",
  "response-headers" => {
    "operation-requires-restart" => true,
    "process-state" => "restart-required"
  }
}
}}}}}
}
```

3. Enter the following command again:

```
/profile=full-ha
/subsystem=transactions/:write-attribute(name=enable-statistics,value=true)
```

4. Once Step 2 and Step 3 are successful (the outcome shows "success"), restart the jboss by issuing the **service jboss restart** command.

## Addressed Issues

- When you retrieve data for a time range greater than 24 hours, occasionally data beyond the time range you have selected is displayed.
- In the fabric node for the Log Collector virtual machine, the status of App Logic and Database is always displayed as DOWN.
- The Security Director Logging and Reporting Alert Definition page does not refresh while switching between domains.
- Alert definitions are activated by default and disregard the disable flag when an alert definition is created.
- The **Show Policy** action does not display the following error for LSYS device policy logs: **No policy found Error.**
- Traffic-selector name must be restricted to 31 characters, else device update fails. [PR 999527]

- Publishing firewall policy fails if you use multiple address variables in firewall policy. [PR 1006042]
- The policy statement direct-term must not be generated if the selected protect-zone does not have any interface. [PR 1000093]

## 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 provide feedback by using either of the following methods:

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software 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: <http://kb.juniper.net/InfoCenter/>
- 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

---

13 August 2014—

Copyright © 2014, 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.