

Junos[®] Space Security Director 14.1R2

Release Notes

Release 14.1R2
January 2015

Contents

Security Director Release Notes	2
Installing Security Director	2
Instructions for Validating the Log Collector OVA Image	2
Upgrading Prerequisites	5
Upgrading Security Director	5
Installing Virtual Log Collectors	6
Installing JA2500 Appliance as a Log Collector	6
Installing the Integrated Log Collector on JA2500 Appliance	7
Upgrading the Log Collector	8
Supported Devices	9
Supported Junos OS Releases	10
Supported Browsers	10
Management Scalability	10
New Features	11
Known Issues	12
Known Behavior	15
Addressed Issue	15
Junos Space Documentation and Release Notes	16
Documentation Feedback	17
Requesting Technical Support	17
Self-Help Online Tools and Resources	17
Opening a Case with JTAC	18
Revision History	18

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](#)
- [Instructions for Validating the Log Collector OVA Image](#)
- [Upgrading Prerequisites](#)
- [Upgrading Security Director](#)
- [Installing Virtual Log Collectors](#)
- [Installing JA2500 Appliance as a Log Collector](#)
- [Installing the Integrated Log Collector on JA2500 Appliance](#)
- [Upgrading the Log Collector](#)
- [Supported Devices](#)
- [Supported Junos OS Releases](#)
- [Supported Browsers](#)
- [Management Scalability](#)
- [New Features](#)
- [Known Issues](#)
- [Known Behavior](#)
- [Addressed Issue](#)

Installing Security Director

From Junos Space Security Director 14.1R2 onward, a single image [Security-Director.14.1R2.6.img] installs Security Director, Log Director, and the Security Director Logging and Reporting module. Installing Security Director Release 14.1R2 installs all three applications. You must deploy the Log Collector add then add the Log collector to Junos Network Management Platform fabric to view the log data in Dashboard, Event Viewer, Reports, and Alerts.

Instructions for Validating the Log Collector OVA Image

From Junos Space Security Director 14.1R1.5 onward, Log Collector open virtual appliance (OVA) image is securely signed. You can validate the image by performing the following tasks:

**NOTE:**

- Validating the OVA image is optional; you can install or upgrade Log Collector without validating the OVA image.
- Before you validate the OVA image, ensure that the PC on which you are performing the validation has the following utilities available: tar, openssl, and ovftool (VMWare Open Virtualization Format [OVF] Tool). You can download the VMWare OVF Tool from the following location:
<https://my.vmware.com/web/vmware/details?productId=353&downloadGroup=OVFTOOL351>

- Download the Log Collector OVA image and the Juniper Networks Root certificate file (**JuniperRootRSACA.pem**) from the Junos Space Security Director 14.1R1 download page at <http://www.juniper.net/support/downloads/?p=spacesecdir#sw>.



NOTE: You need to download the Juniper Networks Root certificate file only once; you can use the same file to validate OVA images for future releases of Junos Space Network Management Platform.

- (Optional) If you download the OVA image and the certificate file to a PC running Windows, copy the two files to a temporary directory on a PC running Linux or UNIX. You can also copy the OVA image and the certificate file to a temporary directory (**/var/tmp** or **/tmp**) on a Junos Space node.



NOTE: Ensure that the OVA image file and the Juniper Networks Root certificate file are not modified during the validation procedure. You can do this by providing write access to these files only to the user performing the validation procedure. This is especially important if you use a generally accessible temporary directory, such as **/tmp** or **/var/tmp**, because such directories can be accessed by several users. Make sure to take precautions to ensure that the files are not modified by other users during the validation procedure.

- Navigate to the directory containing the OVA image.
- Unpack the OVA image by executing the following command:

```
tar xf ova-filename
```

where *ova-filename* is the filename of the unpacked OVF file contained within the previously downloaded OVA image.

- After the unpacked OVF file is validated, validate the signing certificate with the Juniper Networks Root CA file by executing the following command:

```
openssl verify -CAfile JuniperRootRSACA.pem -untrusted Certificate-Chain-File  
Signature-file
```

where **JuniperRootRSACA.pem** is the Juniper Networks Root CA file, *Certificate-Chain-File* is the filename of the unpacked certificate chain file (extension **.pem**), and *Signature-file* is the filename of the unpacked signature file (extension **.cert**).

If the validation is successful, a message indicating that the validation is successful is displayed.

A sample of the validation procedure is as follows:

```
[user@host ~]# ovftool /root/Log-Collector.14.1.ovf
OVF version: 1.0
VirtualApp: false
Name: Log-Collector.14.1
```

```
Download Size: 1.22 GB
```

```
Deployment Sizes:
```

```
Flat disks: 564.00 GB
```

```
Sparse disks: 2.98 GB
```

```
Networks:
```

```
Name: VM Network
```

```
Description: The VM Network network
```

```
Virtual Machines:
```

```
Name: Log-Collector.14.1
```

```
Operating System: centos64guest
```

```
Virtual Hardware:
```

```
Families: vmx-07
```

```
Number of CPUs: 2
```

```
Cores per socket: 1
```

```
Memory: 8.00 GB
```

```
Disks:
```

```
Index: 0
```

```
Instance ID: 8
```

```
Capacity: 64.00 GB
```

```
Disk Types: SCSI-lsilogic
```

```
Index: 1
```

```
Instance ID: 9
```

```
Capacity: 500.00 GB
```

```
Disk Types: SCSI-lsilogic
```

```
NICs:
```

```
Adapter Type: E1000
```

```
Connection: VM Network
```

```
Adapter Type: E1000
```

```
Connection: VM Network
```

```
Adapter Type: E1000
```

```
Connection: VM Network
```

```
[root@NWAPPLIANCE24079 ~]# openssl verify -CAfile JuniperRootRSACA.pem
-untrusted junos-space-certchain.pem Log-Collector-ESX.14.1R1.9.cert
Log-Collector-ESX.14.1R1.9.cert: OK
```

6. (Optional) If the validation is not successful, perform the following tasks:
 - a. Determine if the contents of the OVA image have been modified. If the contents have been modified, download the OVA image from the Junos Space Network Management Platform downloads page.

- b. Determine whether the Juniper Networks Root CA file is corrupted or modified. If it was corrupted or modified, download the certificate file from the Junos Space Network Management Platform downloads page.
- c. Retry the preceding validation steps using one or both new files.

Upgrading Prerequisites

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

- Upgrade Network Management Platform Release 13.3R2.6 to Network Management Platform Release 14.1R2.9 before upgrading Security Director, Log Collector, and Log Director.
- From Junos Space Security Director 14.1R2 onward, a single image upgrades Security Director, Log Director, and Security Director Logging and Reporting module. Upgrading to Security Director Release 14.1R2, upgrades all three applications.



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

Upgrading Security Director

To upgrade Security Director Release 14.1R2, perform the following steps:

1. Download the **Security-Director.14.1R2.x.img** file from the [Download Site](#).
2. Select **Administration > Applications > Security Director**. Right-click and select **Upgrade Application**.

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

3. Click **Upgrade**.

The Job Management tab shows the upgrade status.

You can directly upgrade to Security Director Release 14.1R2 from the following earlier Security Director releases:

- 13.3R1 (Security Director running on the Network Application Platform Release 13.3R1)
- 13.3R2 (Security Director running on the Network Application Platform Release 13.3R2 or 13.3R4)
- 14.1R1 (Security Director running on the Network Application Platform Release 14.1R1)



NOTE: When the setup includes Log Collector, Log Director, and Security Director, upgrading Security Director automatically upgrades the Security Director Logging and Reporting module. Log Director is upgraded using Log Collector and the Log Director component. Upgrade Log Collector first; then upgrade Log Director.

Installing Virtual Log Collectors

1. Download the **Log-Collector-ESX.14.1R2.12.ova** file from the [Download Site](#).
2. Install the OVA image to deploy a Log Collector or Log Concentrator on to ESX server.
3. Add the Log Collector subsystem as a specialized node on the Junos Space Network Management Platform Fabric. For more information, see Chapter 2 of the [Getting Started Guide](#) for instructions on adding the Log Collector nodes as a specialized node.



NOTE: The virtual logging nodes can be added to Junos Space Network Management Platform running on both a virtual and a JA2500 environment.

Installing JA2500 Appliance as a Log Collector

Beginning with Release 14.1R2, you can use a JA2500 appliance as a Log Collector and a Log Concentrator.

To install JA2500 appliance as a Log Collector or a Log Concentrator, perform the following steps:

1. Create a bootable USB drive. You can use any third party conversion software tool (for example, Rufus) to perform image conversion.



NOTE: DISCLAIMER: Juniper does not endorse any particular conversion tool. Juniper disclaims any and all assurances, representations and warranties of any kind, express or implied, including without limitation any warranty as to quality, merchantability or non-infringement, as to any third party software tools. Your use of such software is entirely at your own risk.

- . For more information, see Chapter 2 of the [Getting Started Guide](#) for instructions on Installing a JA2500 Log Collector appliance image using a USB drive.
2. Ensure that the appliance's BIOS boots from the USB drive instead of the appliance's hard disk.
3. Download the **Log-Director-JA2500.14.1R2.2.iso** file from the [Download Site](#) and then install the ISO image on the JA2500 appliance.

4. Select the node type as a Log Collector or a Log Concentrator.
5. Add the Log Collector subsystem as a specialized node on the Junos Space Network Management Platform Fabric. For more information, see Chapter 2 of the [Getting Started Guide](#) for instructions on adding the Log Collector nodes as a specialized node.



NOTE: The JA2500 logging nodes can be added to Junos Space Network Management Platform running on both virtual and JA2500 environment.

Installing the Integrated Log Collector on JA2500 Appliance

In this section, the JA2500 as an integrated deployment runs Junos Space, Security Director, Log Director, and Log Collector VM.

To install the Log Collector VM application on the Junos Space Network Management Platform:

1. Log in to the Junos Space Network Management Platform user interface.
The box at the top of the task tree displays Junos Space Network Management Platform by default.
2. Select **Network Management Platform > Administration > Applications**.
3. Click the **Add Application** icon.
4. Upload the Log Collector VM image (Log-Collector-JA.14.1R2.X-VM.img) by performing either of the following steps:
 - a. Click **Upload via SCP**.

The Upload Software via SCP dialog box appears. You must provide the following Secure Copy remote machine credentials:

- Add your username.
- Add your password.
- Confirm by adding your password again.
- Add the host IP address.
- Add the local pathname of the Junos software application file.
- Click **Upload**.

5. To verify that the Upload Application job is complete, click **Job ID** on the Jobs > Job Management inventory page. Wait until the job is completed and to ensure that the job is successful.



NOTE: If the upload is successful, Log Collector VM is displayed on the Add Application page. The details of the application title, filename, version, release type, and the required Junos Space Network Management Platform version are also displayed.

6. Click the Add Application icon to install the Log Collector VM application.
7. Select the Log Collector VM image.
8. Click **Install**.

The Application Configuration dialog box is displayed.

9. Enter the IP address, subnet mask, default gateway, and the password for the Log Collector VM application. You are also prompted to configure the IP address for eth1 and eth2 interfaces.



NOTE: You will be prompted twice to enter the password. Use this password while adding a Log Collector virtual machine as a specialized node in the Junos Space Fabric.

10. Click **OK** to proceed.

The Application Management Job Information dialog box appears.

11. In the Application Management Job Information dialog box, click **Job ID** to see the Add Application job on the Jobs > Job Management inventory page. Wait until Log Director is fully deployed to ensure that the job is successful.
12. Log out from and log in to the Junos Space Network Management Platform for the changes to take effect.



NOTE: Ensure that you can ping the Log Collector subsystem using the configured IP address.

Upgrading the Log Collector

You can upgrade the Log Collector nodes by installing the Log Collector upgrade package. The procedure is the same for both the virtual and hardware space environments. The support for hardware-based Log Collectors is available from Release 14.1R2. You must upgrade log collection on VM nodes and hardware-based nodes (JA2500) by following the steps as listed below.

Note that all the nodes that are present in the system will be upgraded with this upgrade package.

To upgrade Log Collector, perform the following steps:

1. Take a backup of log data from the Log Collector. For more information, see Chapter 6 of [Getting Started Guide](#) for instructions on backing up the data for Log Collector.
2. Download the **Log-Collector-Upgrade.14.1R2.3.img** file from the [Download Site](#).
3. Select **Network Management Platform > Administration > Applications** and then click the **Add Application** icon.

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

4. Select Log Collector. For example: **Log-Collector-Upgrade.14.1R2.3.img**. The option to install is displayed.
5. Click the Add Application icon to install the Log Collector upgrade application.
6. Select the Log Collector upgrade and then click **Install**.

The Job Management tab shows the image upgrade status. To validate the upgrade status of Log Collector nodes, select Logging > Log Collectors > Version.

**NOTE:**

- If the upgrade fails on any of the nodes, you must the reinstall the upgrade image.
 - If you are using multiple Log Collectors and have changed your Log Collector Password (using “Change Password” in Log Collectors page) in Release 14.1R1, then you have to "reset the password" after the upgrade of Log Collectors to Release 14.1R2 .
-

Supported Devices

Security Director 14.1R2 is supported on the following SRX Series hardware devices and LN Series hardware device:

- SRX100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX240H
- SRX550
- SRX650
- SRX1400
- SRX3400
- SRX3600
- SRX5400
- SRX5600
- SRX5800
- LN1000-V
- LN2600

Supported Junos OS Releases

- Security Director 14.1R2 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.

New Features

The Junos Space Security Director 14.1R2 application includes the following new features:

- **Policy analysis**—Policy analysis helps you analyze the firewall rule base for policies managed by Security Director, and identifies the firewall rules that contain shadowing and redundant anomalies. Policy analysis also identifies anomalies in the addresses and services that are assigned to rules. The policy analysis report is generated in PDF format; you can configure the report to be e-mailed to multiple recipients. The reports contain a summary and a pie chart showing all anomalies. You can schedule the report generation.
- **Importing an existing VPN environment**—Junos Space Security Director lets you import your existing large and complex VPN configurations into Security Director. You do not have to recreate the same VPN environment to allow Security Director to manage it. During the VPN import, all VPN-related objects are also imported along with the VPN. This workflow imports VPN configuration settings from the individual devices into Security Director for centralized management. It does not change any settings on the individual devices. Once the process is completed, all VPN settings are manageable centrally from the VPN page.
- **Tracking the utility rate of security firewall policies**—You can track the utility rate of firewall policies by analyzing the number of hits they receive from Security Director. You can also determine the policy rules that are currently used on the device, the hit levels of the policy rules that are hit by the traffic, and the usage frequency of the policy rules. Using hits data, you can identify the important and less important policy rules, and take further action to optimize the policy rules by deleting the unwanted policy rules.
- **Drag and drop of policy rules**—You can select one or more objects to drag and drop into the respective columns in the policy tabular view. Security Director ensures that objects can be dropped only into the columns that support dragging and dropping. Columns that support this function are the Source Address, Destination Address, and Service columns. Before dropping any object into the policy rules, you must first lock the affected policy.

You can drag and drop the objects across the rules. The new object is copied to the rule. This feature is supported for firewall, NAT, and IPS policies.
- **UTM wizard**—Unified Threat Management (UTM) consolidates several security features into one device to protect against multiple threat types. The advantage of UTM is streamlined installation and management of these multiple security capabilities. With the existing functionality, you must create the policies for the security features you require before you create the UTM policy. The new UTM wizard guides you through the step-by-step process of creating the new policies. Each individual security feature creation will launch its own wizard.
- **Viewing a NAT policy for a corresponding log and logs generated by the NAT rule**—When a log is generated for a source, destination, or static NAT rule in the Event Viewer workspace, you can view the corresponding NAT policy. For a log generated for a source or destination rule, you are given the option to view either the source NAT rule or the destination NAT rule, or both. If you choose to view a static NAT rule, both the

source and the destination NAT rule logs are shown. Similarly, you can view the corresponding logs generated by any NAT rule. You are automatically redirected to the Event Viewer workspace to view the log.

- **Hardware-based Log Collectors and Log Collector Management**—Beginning in Junos Space Security Director Release 14.1R2, you can deploy a JA2500 appliance as a Log Collector and a Log Concentrator.
- **Enhanced Event Viewer support**—Event Viewer has the following enhancements:
 - **Comparison charts**—You can use a bar chart to compare the number of events of a particular type for the current time period to the number of events of that type for the previous time period.
 - **Filtering on multiple string values**—You can select multiple string values for filtering by selecting the required column cell from the Event Viewer. This feature enables you to create a filter string to view specific information.
 - **Create an alert, report, and monitor**—You can create an alert, report, and monitor from Event Viewer.
- **Enhanced filter management**—Filter management has the following enhancement:
 - **Create a local filter**—You can create a local filter in the Event Viewer or on the Alerts page. For example, changes to a filter in the dashboard do not affect a filter in the Event Viewer or on the Alerts page.
- **Enhanced alerts support**—You can navigate to the Event Viewer from the Alerts page and then view the list of logs that generated the alert.
- **Enhanced troubleshooting**—Log Collector management has the following enhancements:
 - You can select Action > Show Statistics from the Log Collector page to view the log collection statistics or to troubleshoot issues with the Log Collector.
 - You can view the log messages if there are any issues with Log Collector and Log Concentrator.

Known Issues

- The Network Application Platform enables users to manage objects from all the allowed domains in the aggregated view. However, Security Director does not support this functionality. [PR 1053883]
- On upgrading Security Director from the Release 13.1 to 14.1R1, the Compare Snapshots shows the domain diff for almost all the rules even though the rules are same. [PR 1025719]
- The hub-and-spoke numbered (P2P) are imported as multiple S2S VPNs unlike UnNumbered HnS VPN. [PR 1026290]
- Dual hub-and-spoke VPN import is not supported. If the spoke has identical configuration pointing to both the hub devices, such as same IKE IDs, dual hub-and-spoke might not be imported completely. [PR 1058451]

- The End-Point Tunnel settings additional columns selection for view is not saved; moved to another endpoint or you must select them again. [PR 1028744]
- Security Director ignores the import of certain VPNs when the IKE ID combination is local or remote DN, and remote or local hostname for RSA Authentication and Main Mode. [PR 1028849]
- The Select Devices page during the VPN import does not scroll down completely till the end; it goes up automatically in Firefox and IE browsers. [PR 1048727]
- Not able to delete the special node when one of the nodes in two node setup is down. [PR 1047967]
- Not able to upgrade the Network Application Platform from the Release 14.1R1 to 14.1R2 in JA1500 appliance because of the constraints in /tmp directory in the Platform. [PR 1050091]
- Modifying a hub-and-spoke or full-mesh VPNs which were imported with different external Interfaces will not be able to change the external Interface. [PR 710963]
- Adding a new Log Concentrator to a setup with an existing Log Collector shows a backlog of logs on the Log Concentrator from the Log Collector. [PR 1057423]
- When alert definitions are defined without a filter condition, you will see a backlog of logs on the Log Concentrator at high EPS rates. [PR 1057425]
- If the reports page is not visited even once and an upgrade is performed from Release 14.1R1 to 14.1R2, then the default reports do not appear. [PR 1027361]
- 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]
- A Log Collector added after the EPS threshold is exceeded will not be functional.
- A user with only Modify Report permission cannot reschedule an already scheduled report. [1026515]

Workaround: To update the schedule, you must have both Modify Report and Job Management permissions.

- A user with Send Report permission cannot send e-mail if the e-mail address is not present. [1027359]

Workaround: To add an e-mail address and send a report, the user must have both Send Report and Modify Report permissions.

- For Security Intelligence filters in the Event Viewer, all the applicable columns are displayed in the Event Viewer table but the column set is shown as default. [PR 1025152]
- After a predefined filter is selected in Event Viewer, non-aggregated mode will not show the following three columns when all columns are selected. [PR 1058410]

Workaround: Clear Filter Settings > Select All Columns > Refresh the page.

- Logging and Reporting feeds do not get updated in case of more than 1000 managed devices while upgrading from 14.1R1 to 14.1R2. [PR 1058702]



NOTE: Issue is applicable only if managed devices in SD is more than 1000 and you are upgrading from older versions of SD to 14.1R2.

Follow the below steps, after upgrading space platform & Log Director, Security Director, Security Director Logging & Reporting to 14.1R2.

1. Delete all the existing Log Collectors from **Network Management Platform > Administration > Fabric**
 2. Log in to Space Console through SSH as user "admin"
 3. Navigate to /var/cache/jboss/ECM
 4. Delete all contents in this folder `rm -rf *`
 5. Add all the collectors which were deleted in step 1.
- Audit logs shows a message "User does not have API Access" while loading Dashboard, Event Viewer and Alerts, if user does not have permission for User management or Device management. [PR 1058675]
 - Scenario: In 14.1R1 version, there are more than one Log Collector [with a Log Concentrator] and the Log Database Password was changed.

Issue: Upgrading Log Collectors from 14.1R1 to 14.1R2 by installing the "Log-Collector-Upgrade.14.1R2.2.img" image, Log Concentrator will not aggregate logs from Log Collectors.

While upgrading the Log Collectors using **Log-Collector-Upgrade.14.1R2.2.img** from Release 14.1R1 to 14.1R2 sometimes the Log Concentrator will not aggregate logs from Log Collectors. [PR 1057416]

Workaround: Select **Network Management Platform > Administration > Global Settings > Change Password**— Change the Log Database Password after the upgrade of Log Collectors.

- 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]
- VPN monitors do not display policy-based VPN information. [PR 971450]
- When multiple log collectors and one log concentrator is added and all the log collectors go down, dashboard and event viewer does not show message indicating the same. [PR 1053795]

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 Issue

- User with a role having only View Security Director Devices can still import devices. [PR 1035742]
- After importing Xdiff from NSM, few NAT policies with 0.0.0/0 source address are deleted. [PR 1014991]
- Security Director does not check for a valid license before pushing new a Signature database. [PR 1017123]
- The Security Director Devices page did not display the SRX cluster to assign a policy after manual failover. [PR 1029057]
- Security Director is showing *Failed to check current download job, so cancel it* error message. [PR 1030921]
- Some of Network Application Platform Restful APIs for Security Director are not working. [PR 1031047]
- Security Director API not working with Tacacs+ accounts. [PR 1032837]

- On Security Director Release 13.1R2.7, import policy is failing. [PR 1039502]
- While defining a new NAT pool under Security Director, the asterisk (*) mark must be removed from the Device field under Routing Instance. [PR 1041480]
- The Network Application Platform does not push the Routing Instance value which is configured in the destination NAT pool. [PR 1043651]
- The import from SRX Series devices failing in NYC HRA setup when OCR is present. [PR 1045993]
- Error thrown when a NAT policy is published with a third NAT pool in SRX Series logical system. [PR 1047996]
- Importing SRX NAT policy from a customer database fails. [PR 1049706]
- The icons are missing in the Create role page on the Network Application Platform GUI. [PR 1041360]
- Users with role having only View Security Director Devices rights can still import devices. [PR 1035742]
- Security Director Devices allows Update to an Unmanaged Device. Job State and Status shows Success, but Message displays [Warning]: Device is unmanaged. Update is skipped on this device. [PR 949521]
- Security Director is not listed after installation because of a conflict with QoS Design. [PR 1042980]
- Security Director does not provide the Advanced Filters options when the user has only a read-only role for firewall, IPS, and NAT policies. [PR 1021634] [PR 1041360] [PR 1049355]
- Uninstalling Log Director or the Security Director Logging and Reporting module makes the Security Director dashboard blank. [PR 1003353]
- After an upgrade of an existing Log Collector, the version is not shown correctly unless it is deleted from special node and re-added.
- During upgrade SECI might not get deployed. [1027363]
- Adding a special node might not build the cache on the 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]
- Jump to Event Viewer options might not display the control plane logs.
- 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]

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 of the Juniper Networks TechLibrary 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 <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to 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 Partner Support Service 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

—

Copyright © 2016, 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.