

Junos[®] Space Network Management Platform 13.3R1 Release Notes

Release 13.3R1
13 June 2016

Contents

Junos [®] Space Network Management Platform Release Notes	2
Upgrade Instructions	2
Application Compatibility	4
Supported Junos Space Applications and Adapters	4
Supported Devices	4
New Features in Junos Space Network Management Platform Release 13.3R1	5
Operational Notes	8
Known Behavior	9
Known Issues	11
Resolved Issues in Junos Space Network Management Platform Release 13.3R1	16
Junos OS Compatibility	24
Junos Space Documentation and Release Notes	24
Requesting Technical Support	24
Self-Help Online Tools and Resources	24
Opening a Case with JTAC	25
Revision History	26

Junos® Space Network Management Platform Release Notes

- [Upgrade Instructions](#)
- [Application Compatibility](#)
- [Supported Junos Space Applications and Adapters](#)
- [Supported Devices](#)
- [New Features in Junos Space Network Management Platform Release 13.3R1](#)
- [Operational Notes](#)
- [Known Behavior](#)
- [Known Issues](#)
- [Resolved Issues in Junos Space Network Management Platform Release 13.3R1](#)
- [Junos OS Compatibility](#)

Upgrade Instructions



CAUTION: During the Junos Space Network Management Platform installation or upgrade process, do not modify the filename of the software image that you download from the Juniper Networks support site. If you modify the filename, the installation or upgrade fails.



WARNING: Due to enhanced password restrictions introduced in Junos Space Network Management Platform 13.3R1, you are prompted to change the administrator password on first login after the upgrade. Arrange for a new password for the admin user before the upgrade.

After upgrading to Junos Space Network Management Platform 13.3R1 which also includes an upgrade to Jboss EAP 6.1, old Jboss 4.2.3 logs that were previously under /var/log/jboss are removed. New Jboss EAP 6.1 logs can be found under /var/log/jboss/servers/server1/server.log. It is recommended to backup the logs by using the Space Troubleshooting feature before attempting the upgrade.

You can upgrade Junos Space Network Management Platform to version 13.3 from the following versions:

- 13.1R1.6
- 13.1P1.14
- 13.1P5.3
- 13.1P6



NOTE: Upgrade to Junos Space Network Management Platform 13.3 from 13.1 may take up to 3 hours depending on the size of the database in 13.1. Do not interrupt or restart the setup without contacting the Juniper Support team first.

When you upgrade to Junos Space Network Management Platform 13.3R1 on a multi-node setup and initiate a reboot request, the nodes are rebooted in the following sequence:

1. The master node reboots first. Although, the other nodes on the Junos Space fabric are in the UP state, all services such as jboss, mysql, jmp-watchdog, and heartbeat are stopped.
2. The master node completes the reboot process, deploys all the .ear files, and completes the initialization process.
3. The master node then issues a reboot command to all other nodes in the Junos Space fabric. Concurrently, the Junos Space user interface is available on the master node and you can log-in to the setup. User can schedule and execute jobs but it is not recommended to run jobs until all other nodes in the Junos Space fabric are in the UP state.

Before you schedule and execute jobs, check the status of all other nodes in your Junos Space fabric from the Junos Space user interface by accessing Network Management Platform -> Administration -> Fabric.

4. The other nodes in the Junos Space fabric reboot, deploy the .ear files, and start the initialization process.

The total time for all nodes to completely initialize is longer than the previous releases.



NOTE: Before starting the upgrade process, ensure that none of the nodes on the Junos Space fabric have a large number of database backups in the /var/cache/jboss/backup directory. Large number of database backups may delay the initialization process. It is recommended to only retain the last two database backups before starting the upgrade process. Delete all other database backups before starting the upgrade process.



NOTE: After the upgrade process is complete, check the status of all nodes in the Junos Space fabric and ensure that they are UP before you start upgrading a Junos Space application. Otherwise, the software upgrade may fail across all nodes.



NOTE: During the upgrade process, do not manually reboot the nodes if the Junos Space user interface does not come up for an extended period of time. Please engage Juniper Support team to help resolve the issue.

Application Compatibility

Before you upgrade to Junos Space Network Management Platform 13.3R1, ensure that compatible versions of Junos Space applications are available for upgrade. If you upgrade to Junos Space Network Management Platform Release 13.3R1 and the compatible version of a Junos Space application is not available, the current version of the Junos Space application is deactivated and cannot be used until Juniper Networks releases a compatible version of the Junos Space application.

For example, Junos Space Network Management Platform Release 13.3R1 is not compatible with any of the previous releases of Junos Space Security Director. If you upgrade to Junos Space Network Management Platform Release 13.3R1, Junos Space Security Director is deactivated and cannot be used.

Check the [Junos Space Application Compatibility Matrix](#) for the latest information.

Supported Junos Space Applications and Adapters

This release of Junos Space Network Management Platform supports the following Junos Space applications:

- Service Insight 13.3R1.7
- Service Now 13.3R1.7
- WW Junos OS Adapter

Supported Devices

This release of Junos Space Network Management Platform supports the following additional Juniper Networks devices running Junos OS:

- EX4300
- MX-VC
- PTX3000
- QFX5100
- QFX-VC
- SRX5400

For the complete list of supported devices, see the FAQ topic [Which Juniper Networks Platforms Does Junos Space Network Management Platform Software Support?](#).



NOTE: When Junos Space Network Management Platform discovers EX Series switches running Layer 2 next generation (L2NG) software, the device family for these devices is displayed (in the Device Management page) as “junos” and not as “junos-ex”. This behavior is currently observed on EX4300 and EX9200 switches running Layer 2 next generation software.

New Features in Junos Space Network Management Platform Release 13.3R1

Junos Space Network Management Platform Release 13.3R1 introduces the following features:

- **Running applications in separate server instances** – You can run applications in separate server instances, which allows you to have a better control over resource allocation as well as manage each application, individually.
- **Rebooting devices** – You can reboot individual devices, virtual chassis setups, dual Routing Engine (RE) setups, and cluster setups from Junos Space Network Management Platform by navigating to Device Operations > Reboot Devices in the Devices workspace. You cannot reboot Logical System (LSYS) devices from Junos Space Network Management Platform.
- **Reporting enhancements** – The reporting feature is enhanced to enable you to generate a Device Inventory report. When editing filter conditions in a report definition, you can define multiple filter values as well as filter criteria using comma-separated values.
- **Quick templates** – Use a CLI-based template editor or a form-based editor to push configurations to multiple devices. You can switch between the two editors to specify the configuration that you want to push to a device. You can set default values for and reorder variables in the configuration elements. You can save the variable settings in a CSV file and download the file to your local system. Before deploying the configuration, resolve these variables manually or by uploading a CSV file that contains information about how to resolve the variables.
- **Negative device templates** – Create device templates with delete commands. When this negative device template is deployed to a device, the delete commands erase the specific configuration on the device.
- **Device name visible on top of the logical and physical inventory pages** – View the name of the device in the physical inventory, physical interfaces, logical interfaces, software inventory and license inventory views. You can also view the name of the device when you want to view the scripts associated with the device, the scripts executed on the device, and the inventory changes on the device.
- **Model devices to enable rapid deployment** – From Junos Space Network Management Platform, you can create configlets that can be downloaded offline to devices. The devices can then connect back to Junos Space Network Management Platform. You can specify the mode of authentication for deployed devices: password-based or key-based. When the devices connect back, the devices can be validated on the basis of their hostname or serial number. You can deploy schema-based configuration to devices or upgrade or downgrade the Junos OS version on the devices through a single workflow. Currently, you can deploy ACX Series, EX Series, and SRX Series devices to Junos Space Network Management Platform using this feature.
- **User-defined alarm filters and event filters** – Create persistent alarm filters and event filters in the Network Monitoring workspace that you can access at any time to view alarms and events based on the defined filtering criteria. Filters are user specific.
- **Read-only Network Monitoring role** – A Junos Space user assigned the FMPM Read Only User role can view devices in the selected domain and view network monitoring

reports, but cannot administer devices, access the Network Monitoring > Admin workspace, nor perform actions on alarms or events in the Network Monitoring workspace.

- **Enhanced topology support** – Improved topology zooming control, support for automatic refresh, and ability to search by device categories are now provided. View nodes by category type (routers, switches, security devices, Media Flow controllers, fabric). You can also view nodes that are one or more hops away from the selected nodes and click to go back or forward to view topology history.
- **Exporting job details to a CSV file** – Export details about the following jobs as a comma-separated file (CSV) to your local system, which allows you to process the data offline. Use this data to identify devices on which staging or deployment of the image has failed.
 - Discover devices
 - Stage image on devices
 - Verify the checksum
 - Deploy images on devices
 - Stage scripts on devices
 - Execute scripts on devices
 - Execute an operation on devices
- **Reassigning jobs to other users** – Exclude users who are owners of scheduled or recurring jobs from deletion when you delete users from the Role Based Access Control workspace. A new “Exclude users who have jobs in progress or scheduled” check box is introduced on the Delete Users Confirmation dialog box, which when selected excludes these users from deletion. This is the default behavior. You can clear this check box to delete these users as well. However, before deletion, you may want to reassign the scheduled or recurring jobs owned by these users to other users. The new “Reassign Jobs” feature in the Job Management workspace enables you to reassign any scheduled or recurring jobs from one user to another user within the same domain. This reassignment ensures that the new user can monitor these jobs and ensure their successful completion.
- **Enhancements to the global search feature** – The global search feature is extended to objects in the Audit Log and Job Management workspaces. Using this enhancement, you can perform a full-text search for objects in the Audit Log and Job Management workspaces. You can search for objects in the device inventory, physical inventory, software inventory, physical interfaces, logical interfaces, tag categories, audit logs, and job categories.
- **Domains** – The domains feature replaces the Permission Labels feature. Using this feature, you can achieve a logical grouping of objects and assign specific administrators to manage objects within a specific domain. You can use the domains feature to define the network structure of your organization.

- **Configuring a specialized or network monitoring node** – Decouple the OpenNMS functionality from the Junos Space VIP node and run it on separate nodes (or specialized nodes). This feature helps you optimize the performance of a fabric.
- **Clearing all your jobs** – When you no longer need to view your jobs on the My Jobs report page, click the newly added “Clear All My Jobs” icon on this page to clear all your jobs. After this operation, though your jobs are no longer listed on the My Jobs report page, you can still view these jobs on the Job Management page.
- **Tags view** – The Tags view is added to the Device Management and Job Management inventory landing pages using which you can view the number of objects that are associated with a specific tag. The total number of assigned objects is displayed along with the tag name in the Tags view. In this view, the tags are organized into Public and Private categories. You can click a private or a public tag under the Private or Public category to view objects that are associated with the specific tag and relevant to the inventory page that you are currently on. In addition to these categories, you can click the Untagged category to view objects that are untagged (that is, objects that are not associated with any tags). From the Tags view, you can create both public and private tags.
- **Viewing objects that are tagged** – View the list of objects that are assigned to a specific tag using the newly added “View Tagged Objects” task on the Tags inventory landing page.
- **Enhancements to image management** – The staging and deployment image inventory landing page displays the staged and checksum statuses of an image on various devices, which helps you decide whether to stage or deploy an image on a specific device.
- **Enhancements to user management** – The Locked Out column on the User Accounts inventory landing page displays locked and unlocked users.
- **Deleting staged images from devices** – Remove images that are staged on devices from the Device Management and Images inventory landing pages.
- **Assigning a temporary or random password to a user** – As an administrator, you can generate a temporary password and send it by e-mail to a new user or an existing user whose password has expired. A user who logs in with the temporary password must change the password before its expiry.
- **Enhancements to local database backup operations** – When you initiate a local database backup operation in a multinode setup, Junos Space backs up the database on the secondary node and then copies the backed-up database file from the secondary node to the primary node. If one of the nodes crashes or is corrupted, this feature enables you to restore the system from the other node.
- **Enhancements to job management** – The newly added Parameters column on the Job Management page displays the name of the objects or provides a link to the objects on which a job is executed.
- **Enhancements to the Modify Script workflow** – Modify and save the script to the Junos Space Network Management Platform database without staging the modified (or the latest) script version on devices. However, you can still continue to stage the modified script on to the devices as in previous releases, if needed.

- **Enhancements to staging of images** – Junos Space Network Management Platform checks whether there is sufficient disk space to stage an image on the device. If there is insufficient disk space, you cannot stage the image on the device.
- **Enhancements to the Configuration File management workspace**
 - The newly added “Export Diff” option on the View Diff page enables you to export the differences in configuration between two configuration files to your local system.
 - Timestamp information is displayed along with the version number on the following inventory landing pages using which you can determine when a specific version of the configuration file was created on the Junos Space server:
 - View Config File Details page
 - Edit Config File page
 - Export Config File(s) page
 - Restore Config File(s) page
 - Compare Config Files page
 - View Diff page
 - You can now manage the number of lines of configuration that must be displayed on the Edit Config File page and View Config File Details page
- **User interface enhancements** – When you select objects and perform an action on them from an inventory landing page, the objects remain selected even after the action is performed.
- **Enhancements to the Job details page** – The Description column on the Job details page displays a short message to indicate that a job is successfully executed.

Operational Notes

The following are the operational notes for Junos Space Network Management Platform:

- In Junos Space Network Management Platform Release 13.1R1, an API POST query **/api/space/device-management/devices/change-credentials** was used to change the device credentials. The POST BODY contained the following:

```
<change-credentials>
<devices href="/api/space/device-management/devices">
<device href="/api/space/device-management/devices/{ID}">
</device>
</devices>
<userName>username</userName>
<password>password</password>
<changeTo>credential(or)Key</changeTo>
</change-credentials>
```

In Junos Space Network Management Platform Release 13.3R1, the REQUEST BODY format contains the following:

```
<change-credentials>
<devices>
```

```

<device href="/api/space/device-management/devices/{ID}">
</device>
</devices>
<userName>username</userName>
<password>password</password>
<changeTo>credential(or)Key</changeTo>
</change-credentials>

```

- The "Users" workspace is renamed "Role Based Access Control" in Junos Space Network Management Platform Release 13.3R1.
- If you want to perform a global search on a device inventory landing page, jobs inventory landing page, or audit logs inventory landing page using partial keywords, append "*" to the search keywords.
- Job Administrator privileges are required to cancel auto-generated Resync Network Elements jobs.
- Internet Explorer slows down because some scripts may take an excessive amount of time to run. The browser prompts the user to decide whether to continue running the slow script. Refer to <http://support.microsoft.com/kb/175500> to fix this issue.
- When you switch from "Space as system of record" mode to "Network as system of record" mode, devices with the "Managed Status: 'Device Changed' or 'Space & Device Changed'" status are automatically synchronized after a period of 900 seconds. To reduce this time period, modify the "Polling time period secs:" setting for Network Management Platform on "Administration > Applications > Modify Application Settings" to a lower value such as 150 seconds.
- In Space as System of Record (SSoR) mode on Junos Space, when a new authentication key is generated, devices discovered and managed using RSA keys whose management status is Device Changed move to a status of Key Conflict Authentication. To resolve the conflict on the devices and bring them back to a key-based state, upload keys manually (Devices > Upload Keys to Devices).
- Devices such as the BX Series and MCG5000 devices that do use the BX Series, and MCG5000 devices are not supported in Space as System of Record (SSoR) mode.
- When Junos Space Network Management Platform discovers EX Series switches running Layer 2 next generation (L2NG) software, the device family for these devices is displayed (in the Device Management page) as "junos" and not as "junos-ex". This behavior is currently observed on EX4300 and EX9200 switches running Layer 2 next generation software.

Known Behavior



CAUTION: To avoid a BEAST TLS 1.0 attack, whenever you log in to Junos Space through a browser tab or window, make sure that the tab or window was not previously used to surf a non-HTTPS website. Best practice is to close your browser and relaunch it before logging in to Junos Space.

- HTML report generation and viewing is not supported in Junos Space Network Management Platform Release 13.3R1. Use CSV and PDF report formats.
- SNMP monitoring of JBoss parameters is not supported due to the lack of snmp-adapter for JBoss version 7. (PR/968233)
- Device-initiated connections to Junos Space might cause an inconsistency with the IP addresses listed in Junos Space. For example, if you use a loopback address to discover the devices, the devices might end up sourcing their SSH session from their interface address (Junos OS default behavior is to select the default address), which can lead to firewall conflicts.
- In a fabric with specialized FMPM nodes, the disaster recovery feature is applicable only to the main Junos Space nodes. The disaster recovery feature is not applicable to FMPM nodes and the data.
- When you upgrade Junos Space Network Management Platform 3.3R1 and reboot the Junos Space appliance, the static routes added are lost. The workaround is to manually add the static route. This limitation is not seen when you perform a fresh installation of Junos Space Network Management Platform 13.3R1. (PR/952030)
- When a remote user with the FMPM Manager role uses the API to access Junos Space Network Management Platform, the user details are not updated in the `/opt/opennms/users.xml` file.
- You may observe the following limitations with the topology feature:
 - Node tooltip always displays Status as Active/Managed even though the node is down.
 - For SRX cluster, topology links are displayed only for the primary member of the cluster and not for the secondary member.
- When Unified ISSU is performed from the Manage Operations workflow, the Routing Engines are not rebooted. The Routing Engines must be manually rebooted for the image to be loaded.
- If there are pending out-of-band changes (Device Managed Status: Device Changed) and, from Config Editor, a change request is created and deployed (Device Managed Status: Space & Device Changed), the deployment fails. This is appropriate and expected behavior, since pending out-of-band changes must be resolved first. Note that the Device Managed Status does not change back from Space & Device Changed to Device Changed because the failed change request is saved in the Junos Space database and can be redeployed.
- For LSYS (logical, nonroot) devices, when there are pending out-of-band changes on the root device, the Resolve out-of-band changes menu option is disabled for those child LSYS devices, even though Device Managed Status is shown as Device Changed. This is by design.
- Network Monitoring does not support Alarms/Performance Management using SNMPv3.
- RMA is not supported for devices running WW Junos OS, and non-Junos OS devices.
- Script Manager supports only Junos OS Release 10.x and later.

- Stage device script or image supports only devices running Junos OS Release 10.x and later.
- For unified ISSU support for both device-initiated and Junos Space-initiated dual Routing Engine connections, we strongly recommend that you configure the Virtual IP (VIP) on the dual Routing Engine device. Dual Routing Engine devices without VIP configuration are not fully supported on Junos Space.
- In a single node or multiple nodes, changes to the user (for example, password, roles, and disable or enable user) will take effect only on the next login.
- Looking Glass functionality is not supported on logical systems.

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 13.3R1. For each entry, the identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- For devices with permission labels assigned to them, corresponding subdomains are automatically created when you upgrade to Junos Space Network Management Platform Release 13.3R1. Devices are moved from the global domain to the subdomains. All configuration files associated with the devices should be moved to the subdomains.

However, during the upgrade, devices are correctly moved from the global domain to the corresponding subdomains but the associated configuration files are not moved. Also, performing a configuration file backup in a subdomain updates the associated configuration file version incorrectly as global instead of the subdomain.

Workarounds:

- After upgrading to Junos Space Network Management Platform Release 13.3R1, move the device to the global domain and then back to the subdomain. This moves the configuration files associated with that device to the subdomain and updates the configuration file version correctly as the subdomain.
- After upgrading to Junos Space Network Management Platform Release 13.3R1, delete the configuration file for that device in the global domain before you back up the associated configuration file in the subdomain
- Before upgrading to Junos Space Network Management Platform Release 13.3R1, detach the permission labels from devices that have configuration files associated with them. This way, those devices are not automatically moved to the subdomains during the migration. (PR/971376)
- In Junos Space Network Management Platform Release 13.3R1, from the Physical Inventory view for SRX Series devices, the shortcut menu item View Physical Interfaces always appears dimmed. This is a regression from Junos Space Network Management Platform Release 13.1P2.6. (PR/961266)
- If you restart the Network Monitoring service from the Administration > Applications > Manage Services page, remote users who are currently logged in cannot access the Network Monitoring workspace. This is the default behavior if you restart the Network Monitoring service.

Workaround: Remote users should log out from the Junos Space user interface session and then log in. (PR/969268)

- When you upgrade the device image on some devices using the Rapid Deployment workflow, a device-platform mismatch occurs. (PR/939078)
- SRX Series devices added by using the Rapid Deployment workflow do not connect to Junos Space. (PR/946019)
- After upgrading from Junos Space Network Management Platform Release 13.1 to Junos Space Network Management Platform Release 13.3R1, newly added or deleted devices are not automatically updated in the Network Monitoring workspace. To update Network Monitoring after the upgrade, select Network Monitoring > Node List > Resync Nodes from the Junos Space user interface. (PR/969856)
- On the tabular view of the Device Configuration editor, the text in the Comments field does not indicate whether the configuration option has a comment. The color of the text in the Comments field is the same for all configuration options. When you delete a comment for a configuration option, the color of the text in the Comments field changes to white. (PR/968896)
- If you apply a filter on the columns displayed on the Devices inventory landing page search results, the column entries are not filtered correctly. (PR/948865)
- Timestamp-related columns in the Job Management and Audit Logs inventory landing pages display time in PST (local browser time) but require the user to input the search string in the equivalent UTC time. Search for audit logs or jobs using the PST timestamp does not return any search results. (PR/946327)
- Global search and searching from the inventory landing page are not supported on all columns in the Job Management and Audit Logs workspaces. (PR/935765)
- Using the Retry on Failed Devices option on the Job Management page displays devices assigned to different domains. (PR/950050)
- Report definitions cannot be moved across domains. The Report Definition inventory landing page does not contain the Assign to Domain option on the shortcut menu. (PR/950150)
- The firewall blocks SNMP access to the external SNMP manager added from the Administration > Fabric > SNMP Manager page.

Workaround: Manually add firewall rules to allow SNMP access. (PR/966142)

- If you modify the subnet mask of the device management interface using the jmp_setup menu options on the Junos Space Appliance, the routes in the devint table are deleted. (PR/965250)
- MIB groups added to a system definition from the Junos Space user interface are not saved.

Workaround: Manually add the collection MIB group to the data collection file from the backend and restart the Network Monitoring service. (PR/967705)

- When you upgrade to Junos Space Network Management Platform Release 13.3R1 and reboot the Junos Space Appliance, the static routes added are lost.

Workaround: Manually add the static routes.

This limitation is not seen when you perform a fresh installation of Junos Space Network Management Platform Release 13.3R1. (PR/952030)

- In a multi-node cluster, the notifications are not displayed after the failover.

Workaround: Refresh the Web browser manually. (PR/955498)

- The remote users assigned to a domain via a remote profile, are not listed on the Assigned Users tab for that domain in the Domains inventory landing page. (PR/946323)
- On the Devices inventory landing page, the tool tip for Show Relevant Tags in the Tag view includes the count and breakup of all tagged objects instead of only the associated tagged devices. (PR/936108)
- Performance graphing of too many values or interfaces at the same time may result in the URI length limit exceeded error.

Workaround: Reduce the number of values or interfaces for graphing. (PR/951620)

- If you navigate to the Network Monitoring > Topology page, click the Default Focus, and then click **Click to go back** multiple times, you are redirected to the Junos Space > Dashboard page. (PR/940907)
- A user assigned to the global domain can view the devices assigned to a subdomain in the Network Monitoring workspace. (PR/943385)
- A user with super administrator privileges and access to a subdomain cannot perform the Rescan Admin, Update SNMP, Schedule, and Outage actions in the Network Monitoring workspace. (PR/945491)
- Role Based Access Control privileges assigned to a custom user role for Quick templates do not work effectively. (PR/940294)
- If you click a chart on the Junos Space Network Management Platform user interface using Internet Explorer 8, you receive the following error message: "Statistics:I/O Error."

Workaround: Perform the following steps and try again:

1. Start Registry Editor.
2. For a per-user setting, locate the following registry key:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

For a per-computer setting, locate the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

3. On the Edit menu, click **Add Value**.

To override the directive for HTTPS connections, add the following registry value:

"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:

"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit Registry Editor.

For more information, refer <http://support.microsoft.com/kb/323308>. (PR/933633)

- When accessing the Junos Space Network Management Platform user interface from Internet Explorer 8, you cannot export and download files such as inventory details, backup configuration files, and troubleshooting logs.

Workaround: Perform the following steps and try again:

1. Start Registry Editor.
2. For a per-user setting, locate the following registry key:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

For a per-computer setting, locate the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

3. On the Edit menu, click **Add Value**.

To override the directive for HTTPS connections, add the following registry value:
"BypassSSLNoCacheCheck"=Dword:00000001

To override the directive for HTTP connections, add the following registry value:
"BypassHTTPNoCacheCheck"=Dword:00000001

4. Quit Registry Editor.

For more information, refer <http://support.microsoft.com/kb/323308>. (PR/933656)

- You may view the "Junos Space is Starting...." message on the Junos Space user interface for some time (approximately two minutes) in the following instances:
 - Uploading the CA Root Certificate or Certificate Revocation List
 - Deleting the CA Root Certificate or Certificate Revocation List(PR/937970)
- You cannot filter the device templates by the Deployment Status column on the Templates page. (PR/938517)
- You can stage device images from the Junos Space user interface on a Dual Routing Engine device even if there is no sufficient space on the backup Routing Engine. (PR/933302)
- Filters are not enabled on the Staged Images and Deploy Images page. You cannot filter these pages to view the devices on which the software is already staged. (PR/932442)
- You cannot sort by the Device Name Column in the Physical Interfaces view on the Device Management page. (PR/931925)
- Zombie user from the former standby node appears after a switchover of the Junos Space nodes. (PR/858198)
- Devices with the connection-type "Reachable Device initiated" do not connection back after performing disaster recovery. (PR/919433)

- User receives an email from ?root@host? from the disaster recovery setup. (PR/919436)
- The FMPM special node contains irrelevant rpms installed. (PR/883610)
- Changing the network settings using the CLI menu does not work for the FMPM node. (PR/893184)
- The SPACE-PLATFORM-MIB does not differentiate the space node and fmpm node. (PR/909382)
- In a multi-node fabric, SNMP v2 settings configured in the Fabric > SNMP Manager page are not updated properly in the /opt/opennms/etc/snmp-config.xml file.
Workaround: Provide the IP address and set the "community" string manually for nodes in the Network Monitoring > Admin section. (PR/909643)
- The Generated Reports page can be viewed even if the View Generated Report privilege is not selected for a custom user role. (PR/889084)
- A domain name cannot be set up for a QFabric device through the Basic Setup Wizard. (PR/895442)
- Script execution on a device fails if the device returns a warning message. (PR/856224)
- When group settings are applied on the device, these settings are not displayed in the Basic Setup Wizard. (PR/884068)
- When a node is set up as "Inactive" in the device configuration, the Basic Setup Wizard incorrectly displays the node as "Active". (PR/884074)
- If you change the Authentication mode through the CLI using the setSpaceAuthMode script, this change is not displayed in the user settings on the Junos Space user interface. (PR/888220)
- The last row of the page is truncated for all generated reports. (PR/889088)
- Some events are lost in the alarm history when duplicate events are received from different service interfaces of the same device. (PR/891369)
- The LmSensors and UCD-SNMP MIB should be compiled by default in Network Monitoring to monitor hardware parameters such as fan, temperature, and voltage of the Junos Space appliance. (PR/893557)
- When the VIP and Node-IP are modified using the menu options in the CLI, the devices are moved to the sync-failed state. (PR/889572)
- The Internet Explorer browser may display issues such as script errors, longer response times, and slower refresh times. (PR/882729)
- When the VIP and Node-IP settings are modified using the CLI menu options, all the device are moved into the sync-failed state. (PR/889572)
- Unified ISSU support or CLI-command modification is needed from TXP-3D. (PR/880614)
- Device Discovery fails if the tags mentioned in the CSV file are the private tags in Junos Space. (PR/860854)

- Topology layout does not display the link associated with a peer-to-peer service between a Juniper Networks device and an unmanaged device. (PR/836790)
- Although M Series, MX Series, and ACX Series devices do not support PPP as an encapsulation type, configuration editor in Junos Space Network Management Platform allows you to configure the PPP encapsulation. (PR/833612)
- For a Junos Space initiated connection, the Platform > Manage Devices inventory page fails to switch to the new master Routing Engine on the dual Routing Engine on a Junos OS device. (PR/563648)
- Old SNMP trap targets are not removed from the device when the network settings on the Junos Space appliance are modified. (PR/689042)
- The LSYS feature does not support deletion of both root and LSYS at the same time. Delete them one at a time. (PR/754683)
- The RMA feature does not currently work for devices running WW Junos OS. (PR/791987)
- Users without Assign/Unassign Template permissions are allowed to add and delete templates from the View Assigned Shared Objects wizard. (PR/816788)

Resolved Issues in Junos Space Network Management Platform Release 13.3R1

The following are the issues that have been resolved in Junos Space Network Management Platform Release 13.3R1. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- Upgrading from Junos Space Network Management Platform Release 13.1 to Junos Space Network Management Platform 13.3R1.3 fails if the Network Monitoring database is larger than 5 GB. (PR/973618)
- Global search option is displayed for Junos Space applications such as Security Director and Network Activate. Global search option is currently supported only on Junos Space Network Management Platform. Global search option is not supported on Junos Space applications. (PR/912743)
- The Switch Option and Dynamic profile options are not supported in the device configuration but are enabled in Junos Space due to the device (LN2600) schema issue. (PR/850531)
- Using the Internet Explorer browser, you can create configlets only from the first line of the configlet editor and not from any other intermediate line. (PR/889181).
- Changes to customized attributes are not retained. (PR/894863).
- You cannot execute scripts on the physical inventory of an SRX Series cluster. (PR/865274)
- When you log in to the single-node Junos Space setup, navigate to the Administration > Fabric page, right-click the node, and select Restart SNMP, SNMP restarts successfully but the following message appears on the user interface: "Failed to Start/Stop SNMP." (PR/919424)

- You cannot export an audit log to obtain all records of the audit log if filters are enabled on the audit log. (PR/917443)
- On the Topology page, the Group functionality does not work because the shortcut menu options are not available. (PR/914476)
- Global search results display incorrect count for some search queries. For some global search queries such as "SRX AND NOT '650'", the correct search results are shown but the counts are incorrect on the Search Results panel. (PR/899296)
- The Utilization Report for the device interface does not show any statistics. (PR/884326)
- The aggregation links between EX Series switches and SRX 3600 devices cannot be discovered using the Topology Discovery feature. (PR/880569)
- When you generate a report in CSV format, the columns are misaligned in the generated report. (PR/907518)
- RSA-based authentication does not work on QFabric devices. (PR/895887)
- When you deploy a configuration on a device, the job details do not show the summary of the configuration pushed to the device. The summary of the configuration is shown on the View Configuration Change Log page. (PR/895824)
- The Encapsulation column on the Physical Interface report cannot be filtered. (PR/891829)
- The Reports dashboard displays information about system health. It does not display information about reports or report definitions. (PR/892172)
- Although the Auto-resync Device check box is not disabled in Space as System of Record (SSoR) mode, automatic resynchronizing of devices is not supported in this mode. (PR/813078)
- You cannot create configlets on the CLI Configlets > Configlets > Create CLI Configlet page if you are accessing the Junos Space user interface through Internet Explorer 9. (PR/889181)
- Changes to customized attributes on the Configuration page are not retained. (PR/894863)
- When you select a device from the topology layout, the filtered view of the alarms specific to the selected device is not displayed. All alarms are displayed. (PR/895262)
- In the Basic Setup Wizard, a configuration made without saving to Consolidate Configuration is recorded in the audit log. (PR/894140)
- The option to select multiple devices for "Resolve Out-of-Band Changes" is disabled even if all the selected devices are in the "Device Changed" state. This is because one or more of the selected devices that are in the "Device Changed" state have the "Resolve Out-of-Band Changes" option disabled. For example, when both the primary and secondary nodes of a cluster are discovered in the same or different discovery jobs, one of the nodes frequently goes into the "Device Changed" state, but the Resolve Out-of-Band Changes option is disabled. (PR/894552)

- Global search does not support special characters such as "+," "~," and "!" for private tags, public tags, and other fields. The device management search does not support special characters such as "+," "~," and "!" for public tags. (PR/893289)
- When you modify the SNMP node settings on the **Fabric SNMP settings** page, you need to update the `/opt/opennms/etc/snmp-config.xml` file manually with the new SNMP node settings. (PR/881120)
- The **Sort-By** field takes precedence over the **Group-By** field in a generated report. This displays inaccurate data in the generated report. (PR/888510)
- When you upgrade from Junos Space Network Management Platform Release 12.3 to Junos Space Network Management Platform Release 13.1, the SNMPv3 settings are preserved and migrated if only one SNMP manager is configured. If there are multiple SNMP managers configured, you need to re-configure the SNMPv3 settings manually after the upgrade. (PR/888710)
- In CLI mode, the Junos Space authentication mode does not change to password based when you modify the Junos Space authentication mode by using the `setSpaceAuthMode` script from the non-VIP node. (PR/892630)
- The string filter using the **starts with** operator does not work on all reports. (PR/892360)
- You cannot filter a report by using the date-and-time filter as expected. (PR/891797)
- When adding unmanaged devices by using a CSV file, enter **N/A** in the loopback address column if you do not want to add a valid loopback address. (PR/893424)
- The following columns cannot be filtered on the Device Inventory Report: IP address, Connection status, AIS install and Event profile, Connection type, and Schema version. (PR/892074)
- Fabric-node SNMP settings that are configured through the Fabric SNMP Settings page are not updated in the `/opt/opennms/etc/snmp-config.xml` file. (PR/888071)
- The "When" option is not supported in the device configuration but is enabled in Junos Space due to the device (LN2600) schema issue. (PR/849396)
- The IP table of the Junos Space server does not work if a TACACS server is used for user authentication. (PR/843248)
- When you create a new organization in Service Now, the Device Group Name field does not accept a continuous string with spaces. (PR/918474)
- Junos Space should save the Junos Space Network Management Platform database on the standby node in a multi-node Junos Space setup. (PR/883604)
- The Add and Delete buttons to add or delete scripts to or from a script bundle are not available on the Junos Space user interface. (PR/920668)
- If you modify a role (end with "Modify," not "Cancel") and then try to create a new role while having another role entry selected, only the new settings are displayed but no role is created. (PR/929596)
- Intermittent outages of Junos Space Network Management Platform 13.1R1.6 was seen on two-node JA1500 Fabric systems. (PR/901645)

- Adding or removing an IP address to or from the SNMP Manager page in the Junos Space user interface freezes the user interface in the "Processing please wait" state. (PR/926608)
- When you try to downgrade the Junos OS, a job error message "Failed to execute RPC get-software-information-backup" is displayed. (PR/915369)
- If you filter two or more columns on the View Physical Interface page, a white screen is displayed. (PR/914215)
- The My Jobs view on the Junos Space user interface should have an additional Clear All button to delete multiple jobs simultaneously. (PR/861124)
- The Detailed Jobs view (double click on a finished job) should display the details of the job. (PR/861635)
- The Tag Administration page does not display the assigned devices for the tags. (PR/861650)
- On the Apply Tags page, the full name of the tag should be entered for auto-completion(search) to work successfully. (PR/901230)
- Private tags are visible and can be deleted or changed only on the Tags Administration page. (PR/861640)
- You cannot assign read-only access to objects in the Network Monitoring workspace. (PR/857952)
- A Junos Space user must be forced to change the initial password after the first successful login. (PR/861659)
- The operational status of all components (also the laser modules) should be shown directly in the Physical Inventory view. (PR/883597)
- The operational status of all components (also the laser modules) should be shown directly in the Physical Inventory View for SFP or XFP from other vendors. (PR/883625)
- The Resync Nodes function does not obey the checked state of the "Add SNMP configuration during device discovery" check box in the Platform Application settings page. When the Resync Nodes operation is performed from the Network Monitoring workspace, a "space" trap-group is added to the managed devices. (PR/905446)
- You cannot re-import a downloaded configlet containing umlauts to Junos Space Network Management Platform because umlauts are encoded incorrectly. (PR/901069)
- XPath functions are not supported on the XPath manager. (PR/922703)
- The tabs on the Configuration View page are too small and the title of the tabs is missing. (PR/917399)
- Information about the switchover of Junos Space nodes is not displayed as an outage in the Network Monitoring workspace. (PR/858195)
- The SNMPv3 authentication and privacy password used for discovering a new network element does not comply with the password policy of the SNMP Manager trap forwarding functionality. (PR/905192)

- If you click the Topology link in the Network Monitoring workspace, an "Internal Error" is displayed. (PR/931453)
- Closing or crashing the browser leads to a locked user session. (PR/915024)
- Auto-showing of search results works only if the search name is fully written in the Search field. (PR/925667)
- When you replace an FPC card for a device and try to sort the Inventory View, the replaced FPC card entry is always listed at the bottom of the inventory page. (PR/858337)
- The automatic refresh functionality is required for all inventory pages in Junos Space Network Management Platform. (PR/883600)
- In the Physical Interfaces and Physical Inventory views for SFP or XFP, the range of the modules (distance, wavelength, and so on) and the Port Type access or network should be displayed. (PR/883631)
- For asynchronous REST method calls where a queue has to be attached to the request, the error message "400 Passed QueueUrl is either invalid or queue does not exist" is displayed when the call is executed. (PR/860485)
- API requests (GET, POST, and so on) on `/api/hornet-q/` can be executed without any user authentication (username and password). (PR/861485)
- A user who logs in to Junos Space Network Management Platform via the API is not registered in the audit logs. (PR/863797)
- Different HornetQ REST API actions lead to error messages at the EMS in N|rnberg. (PR/926961)
- When certificate-based authentication mode is activated in Junos Space Network Management Platform, multiple client sessions can be opened with the same user account though only one session is allowed. (PR/932808)
- When certificate-based authentication mode is activated in Junos Space Network Management Platform, a user with only API rights can connect to Junos Space Network Management Platform from the user interface. (PR/932810)
- Performance of the Junos Space setup worsens when it is a single node setup. (PR/887544)
- An unpurged job is incorrectly displayed as a purged job. (PR/860476)
- If you generate a report from a report definition, the Job Management page does not display details of the generated report. (PR/931458)
- A user with the "Create / Modify Report Definition" permissions but with no permissions to view the audit logs can generate audit trail reports. (PR/931924)
- A user with the ""View Generated Reports" permissions can view and download the reports related to workspaces or privileges that are not assigned to the user. (PR/931935)
- When you resize the pop-up windows in Junos Space Network Management Platform, the contents of the pop-up windows are not resized. (PR/856110)

- Horizontal scroll bars are not available on multiple pages on Junos Space Network Management Platform. (PR/856495)
 - The previously applied filter should be cleared when you try to view a new job ID on the Job Management page. (PR/858257)
 - The name of the network equipment (NE) is not visible at the top of the Physical Inventory and Logical Inventory views. (PR/861544)
 - A user object should remain selected after an action is performed on the user. (PR/879056)
 - In the pop-up windows displayed on the Junos Space user interface, the OK button should correspond to the Enter key on the keyboard. (PR/861539)
 - If a page is refreshed, irrespective of whether it is initiated by an automatic user interface update or by the Refresh button, the view (scroll bar) jumps to the top of the page. (PR/915036)
 - The passphrase used for Public and Private Key authentication between Junos Space and the device is stored in cleartext. (PR/879982)
 - The Apache server is not configured according to database requirements. Several vulnerabilities were observed. (PR/879986)
 - The following security requirement for UNIX systems should be met:
 - Detailed user and role concepts for individual components of the system — for example, "no remote access for root," "each user of each application and/or database must have credentials," "functional accounts for the applications," and "no administrative accounts on databases for the application." Currently, all accounts used in Junos Space are administrative accounts.
 - Authorizations for users and applications must be reduced to the minimum required for the tasks to be performed. UNIX system administrators should always use functional accounts.
- (PR/880014)
- The following updates to the CentOS are required:
 - The operating system and all its components must be kept up to date from initial setup through the entire lifetime.
 - The software and hardware components that are no longer supported by the vendor must not be used.
 - The software and hardware components with a known vulnerability should not be used. However, their use is permitted if a measure exists to remedy the vulnerability, which must be implemented additionally in this case.
 - The installed operating system version should be the current version of the operating system that has the currently released patch status.
- (PR/880025)
- Harden the operating system by configuring it according to the *CIS Hardening Guide for RedHat*. (PR/880019)

- Default passwords on database systems must be changed. (PR/880620)
- A JBoss vulnerability is found in a Junos Space Platform 12.2P1.4 setup during a vulnerability scan. (PR/863272)
- The Session ID calculated does not meet the security requirement for Web applications. (PR/879980)
- Update JBoss packages to the current patch level 7.1. (PR/879984)
- MySQL does not write and send binary log files to the remote system log server. (PR/880000)
- The user accounts of processes (junospace, centos, mysql, postgres, apache, and jboss) are administrative accounts that have more rights assigned than needed. All user accounts should have only those rights assigned that are needed. (PR/880001)
- Harden the PostgreSQL database by configuring it according to specific database requirements. (PR/880002)
- The PostgreSQL packages are not updated to the current patch level provided by the vendor. (PR/880004)
- All SUID and GUID permissions are not removed from the operating system. (PR/880008)
- Configure and test a remote system log server for the operating system and application log data. Check the log data related to CentOS, MySQL, PostgreSQL, Apache, and JBoss. (PR/880016)
- Each instance of the Web server must not be executed with system privileges. Apache permissions should be changed. (PR/880228)
- System output and messages should not contain internal information. JBoss configuration should be modified to hide default server headers. (PR/880629)
- SFTP should be hardened to comply with security requirements. (PR/884122)
- The MySQL database should run in a chroot environment. (PR/884125)
- Configure the SSH server according to specific security requirements. (PR/884128)
- The application and system log files are stored on a dedicated file system, which has been solely created for this purpose. (PR/884354)
- All the processes running on a UNIX system must be launched with the minimum rights required for the process to function. (PR/884427)
- The host parameters used for user authentication must not contain wildcards. (PR/884428)
- The risk of a service failure due to denial-of-service attacks must be mitigated by suitably modifying the configuration. (PR/884431)
- The following issues related to XSS need to be addressed:
 - User sessions must be protected against unauthorized hijacking by other users. The Web server is vulnerable to cross-site scripting (XSS).

- System services must be robust against unexpected input. The Apache Web server does not validate input sufficiently. This can lead to XSS attacks.

(PR/884469)

- The system does not ensure that passwords meet a minimum length of eight characters and contain uppercase and lowercase letters, numerals, and special characters. The passwords and passphrases do not comply with the password policies. (PR/884481)
- A registration process used for a Web application should be created on Junos Space Network Management Platform. (PR/884504)
- The SSH server service is not linked to a specific IP address at which it fulfills its function. (PR/892801)
- Information about the Web server in HTTP headers is not minimized. (PR/892816)
- SSH Agent Forwarding is not prohibited on the server side. (PR/894943)
- The user accounts for the processes (opennms and postgres) must have only those rights assigned that are needed. Administrative accounts should not be used. (PR/898548)
- MySQL must be executed within a chroot environment. (PR/898550)
- Using X509 Certificate auth mode with a smart card slows down the system tremendously. (PR/905515)
- X509 client certificate authentication does not apply to the NBI. (PR/905555)
- A warning message should be displayed to the user when the user opens another active Web browser session. (PR/905642)
- Directory listings (indexing) must be deactivated to prevent misuse of information about files and directory structures. (PR/905655)
- The following requirements related to Postgres hardening need to be met:
 - Access to database among various database systems must comply with the least privilege principle. Rights of the Network Monitoring user must be restricted if possible.
 - Accesses to database systems, as well as critical database procedures and database content, should be logged. Enable access logs for Postgres.

(PR/909574)

- Upgrade to Apache 2.2.25. (PR/910651)
- Enable the required flags to authenticate users on server systems by using asymmetric cryptographic algorithms, such as Public key, and OTP. (PR/912757)
- Disable mounting of cramfs, freevxfs, jffs2, hfs, hfsplus, and squashfs file systems in the CentOS. (PR/912795)
- Install and configure Advanced Intrusion Detection Environment (AIDE) on the CentOS. (PR/912797)
- Enable audit logging for specific items on the CentOS. (PR/912801)
- The CentOS should be hardened. (PR/912804)

Junos OS Compatibility

For compatibility information, see the FAQ [What Junos Releases Are Supported in Different Junos Space Applications?](#).

- Related Documentation**
- *Junos Space Frequently Asked Questions*

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>.

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

12 March 2014—Revision 1, Junos Space Network Management Platform Release 13.3R1

16 June 2014—Revision 2, Added Junos Space Network Management Platform Release 13.1P6 as a supported upgrade path to Junos Space Network Management Platform Release 13.3R1.

15 July 2014—Revision 3, Added note about supported devices

13 June 2016—Revision 4

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.