

Junos® Space Network Management Platform Release 14.1R1 Release Notes

Release 14.1R1
13 June 2016

Contents

Junos® Space Network Management Platform Release Notes	2
Upgrade Instructions	2
Instructions for Validating the Junos Space Network Management Platform OVA Image	3
Upgrading from Prior Releases of Junos Space Network Management Platform	5
Reboot Sequence After Upgrading on a Multinode Setup	5
Upgrade Notes	6
Application Compatibility	6
Supported Junos Space Applications and Adapters	6
Supported Devices	7
New and Changed Features	7
Operational Notes	13
Changes in Default Behavior	15
Known Behavior	16
Known Issues	17
Resolved Issues in Junos Space Network Management Platform Release 14.1R1	24
Documentation Updates	28
Junos OS Compatibility	28
Junos Space Documentation and Release Notes	28
Requesting Technical Support	29
Self-Help Online Tools and Resources	29
Opening a Case with JTAC	30
Revision History	31

Junos® Space Network Management Platform Release Notes

These release notes accompany Junos Space Network Management Platform Release 14.1R1.

- [Upgrade Instructions on page 2](#)
- [Application Compatibility on page 6](#)
- [Supported Junos Space Applications and Adapters on page 6](#)
- [Supported Devices on page 7](#)
- [New and Changed Features on page 7](#)
- [Operational Notes on page 13](#)
- [Changes in Default Behavior on page 15](#)
- [Known Behavior on page 16](#)
- [Known Issues on page 17](#)
- [Resolved Issues in Junos Space Network Management Platform Release 14.1R1 on page 24](#)
- [Documentation Updates on page 28](#)
- [Junos OS Compatibility on page 28](#)

Upgrade Instructions

This section includes instructions to upgrade to Junos Space Network Management Platform Release 14.1R1. Read these instructions before you begin the upgrade process.



.....

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.

.....

- [Instructions for Validating the Junos Space Network Management Platform OVA Image](#)
- [Upgrading from Prior Releases of Junos Space Network Management Platform](#)
- [Reboot Sequence After Upgrading on a Multinode Setup](#)
- [Upgrade Notes](#)

Instructions for Validating the Junos Space Network Management Platform OVA Image

From Junos Space Network Management Platform Release 14.1R1 onward, the Junos Space Platform open virtual appliance (OVA) image is securely signed.



NOTE:

- Validating the OVA image is optional; you can install or upgrade Junos Space Network Management Platform 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 VMWare OVF Tool from the following location:
<https://my.vmware.com/web/vmware/details?productId=353&downloadGroup=OVFTOOL351>.

To validate the Junos Space Network Management Platform OVA image:

- Download the Junos Space Platform OVA image and the Juniper Networks Root CA certificate file (**JuniperRootRSACA.pem**) from the Junos Space Network Management Platform - Download Software page at
<https://www.juniper.net/support/downloads/?p=space>.



NOTE: You need to download the Juniper Networks Root CA 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 downloaded the OVA image and the Root CA 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 Root CA 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 CA 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.

- 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 downloaded OVA image.

5. Verify that the unpacked OVA image contains a certificate chain file (**junos-space-certchain.pem**) and a signature file (**.cert** extension).
6. Validate the signature in the unpacked OVF file (extension **.ovf**) by executing the following command:

```
ovftool ovf-filename
```

Where *ovf-filename* is the filename of the unpacked OVF file.

7. Validate the signing certificate with the Juniper Networks Root CA certificate 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 certificate 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:

```
-bash-4.1$ ls
JuniperRootRSACA.pem  space-14.1R1.316085.ova
-bash-4.1$ mkdir tmp
-bash-4.1$ cd tmp
-bash-4.1$ tar xf ../space-14.1R1.316085.ova
-bash-4.1$ ls
junos-space-certchain.pem  space-14.1R1.316085.cert
space-14.1R1.316085-disk1.vmdk.gz  space-14.1R1.316085.mf
space-14.1R1.316085.ovf
-bash-4.1$ ovftool space-14.1R1.316085.ovf
Opening OVF source: space-14.1R1.316085.ovf
Warning: Could not verify certificate (possibly self-signed)
Warning: Not all files referred in the OVF package is accounted for in the
manifest file
OVF version: 1.0
Name: space-14.1R1.316085

Download Size: 1.53 GB

Deployment Sizes:
Flat disks: 32.00 GB
Sparse disks: 3.76 GB

Networks:
Name: VM Network
Description: The VM Network network

Virtual Hardware:
Family: vmx-04
Disk Types: SCSI-lsillogic

Completed successfully
-bash-4.1$ openssl verify -CAfile ../JuniperRootRSACA.pem -untrusted
```

```
junos-space-certchain.pem space-14.1R1.316085.cert
space-14.1R1.316085.cert: OK
```

8. (Optional) If the validation is not successful, perform the following tasks:
 - a. Determine whether the contents of the OVA image are modified. If the contents are modified, download the OVA image from the Junos Space Network Management Platform - Download Software page.
 - b. Determine whether the Juniper Networks Root CA certificate file is corrupted or modified. If it is corrupted or modified, download the Root CA certificate file from the Junos Space Network Management Platform - Download Software page.
 - c. Retry the preceding validation steps by using one or both of the new files.

Upgrading from Prior Releases of Junos Space Network Management Platform

You can upgrade to Junos Space Network Management Platform Release 14.1R1 from the following prior versions:

- 13.3R4.4
- 13.3R2.6
- 13.3R1.9
- 13.1R1.6
- 13.1P6.3
- 13.1P5.3
- 13.1P1.14

Reboot Sequence After Upgrading on a Multinode Setup

When you upgrade to Junos Space Network Management Platform Release 14.1R1 on a multinode setup and initiate a reboot request, the nodes are rebooted in the following sequence:

1. The primary node reboots first. Although, you can ping or connect (using SSH) to the other nodes in the Junos Space fabric, all services on the other nodes such as jboss, mysql, jmp-watchdog, and heartbeat are stopped.

You can check the status of a service by executing the following command: **service *service-name* status**, where *service-name* is the name of the service; for example, mysql.

2. The primary node completes the reboot process, deploys the component files, and completes the initialization process.
3. The primary 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 primary node and you can log in and access the Junos Space GUI.

Before you schedule and execute jobs, check the status of all other nodes in your Junos Space fabric. To do this, access the Fabric page (**Administration > Fabric**) from

the Junos Space GUI and ensure that the **Status** for all nodes is **UP** and that the **App Logic** is also **UP**.

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

As explained in the preceding step, check that the status of all nodes is up.

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

Upgrade Notes



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. Contact the Juniper Networks Support team for help in resolving this issue.



NOTE: Before starting the upgrade process, ensure that none of the nodes on the Junos Space fabric contains a large number of database backups in the `/var/cache/jboss/backup` directory. Large number of database backups may delay the initialization process. We recommend that you retain only the previous 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 (in the **Administration > Fabric** page) and ensure that the **Status** is **UP** for all nodes *before* you start upgrading a Junos Space application. Otherwise, the software upgrade may fail across all nodes.

Application Compatibility

Before you upgrade to Junos Space Network Management Platform Release 14.1R1, ensure that compatible versions of Junos Space applications are available for upgrade. If you upgrade to Junos Space Network Management Platform Release 14.1R1 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.

Supported Junos Space Applications and Adapters

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

- Service Insight releases 13.3R1, 13.3R2, and 14.1R1
- Service Now releases 13.3R1, 13.3R2, and 14.1R1
- ww Junos OS Adapter

For the latest information, see the [Junos Space Application Compatibility](#) knowledge base article.

Supported Devices

Junos Space Network Management Platform Release 14.1R1 supports the following additional Juniper Networks devices running Junos OS:

- EX9204
- EX9208
- QFX5100-96S

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 (on 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 and Changed Features

This section describes new features and the enhancements to existing features in Junos Space Network Management Platform Release 14.1R1.

- **Change in release numbering**—Starting from Junos Space Network Management Platform Release 14.1R1, the release numbering has changed to the *m.nRb.s* format, where *m* is the major release number, *n* is the minor release number, *b* is the build number (*b*=1 indicates an FRS release and *b*>1 indicates a maintenance release), and *s* is the (optional) spin number.
- **Enhancements to the global search feature**—Global search is extended to objects on the following inventory landing pages:
 - Configlets
 - Configuration Files
 - Configuration Views
 - Device Templates
 - Generated Reports
 - Images
 - Report Definitions
 - Scripts
 - User Accounts
 - XPath and Regex

You can perform a full-text search for objects on these inventory landing pages.

- **Checking before a node is added to a fabric**—Junos Space Network Management Platform displays a warning message if you delete a node from an existing fabric and try to add it to another fabric without reimaging the node. When you delete a node from a fabric, you must reimage the node before adding the node to another fabric.
- **Cloning a user role**—A Super Administrator or a User Administrator can clone a predefined or a user-defined role from the Roles inventory landing page. Cloning a role creates a copy of the role. You can modify the cloned role to suit your requirements.
- **Configuring a proxy server**—A Super Administrator or User Administrator can configure a proxy server that Junos Space Network Management Platform and its installed applications can use.
- **Deleting unused schemas**—From the Administration workspace, a user with Super Administrator or System Administrator privileges can delete any unused Device Management Interface (DMI) schemas that do not need to be managed by Junos Space Network Management Platform.
- **Support for the administrative interface on Junos Space Virtual Appliance and Junos Space hardware appliances**—Junos Space Virtual Appliance and Junos Space hardware appliances (JA1500 appliance and JA2500 appliance) support the configuration of the eth1 Ethernet interface as an administrative interface. This helps in providing data security by separating the administrative traffic of the nodes in a Junos Space fabric from the GUI traffic and the device management traffic. For more information, refer to the Junos Space Virtual Appliance, JA1500, or JA2500 documentation available at http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html.
- **Restricting users to view only their own jobs**—From Junos Space Network Management Platform Release 14.1R1 onward, users can view only their own jobs on the Job Management page; only users with the Super Administrator or the Job Administrator role can view jobs initiated by all users.
- **Enhancements to schema updates**—From Junos Space Network Management Platform Release 14.1R1 onward, you can download the list of DMI schemas for one or more device families, instead of downloading the list of all DMI schemas from the Juniper Networks Subversion repository. You can then select schemas from the list and install the selected schemas. You can also schedule the installation of DMI schemas for a future date. From Junos Space Network Management Platform Release 14.1R1 onward, the installation of schemas is a job.
- **Enhancements to viewing tagged objects**—The following objects are now supported for viewing on the View Tagged Objects page (in the Administration workspace):
 - Config Files Management (Configuration Files workspace)
 - Configuration Views, XPath and Regex, and Configuration Filters (CLI Configlets workspace)
 - DMI Schemas, Fabric Node, Applications (Administration workspace)

- **Enhancements to informational messages on the Junos Space UI**—Informational messages are displayed when a new domain is created, when a user with access to more than one domain logs in, or when search results are displayed.
- **Load-balancing devices across Junos Space nodes**—From Junos Space Network Management Platform Release 14.1R1 onward, you can rebalance devices evenly (by clicking the **Device Load Balancer** icon in the **Fabric** page within the **Administration** workspace) across Junos Space nodes in the fabric, if the devices being managed by Junos Space Network Management Platform are not evenly distributed.
- **Verifying and executing a job on the basis of user roles**—From Junos Space Network Management Platform Release 14.1R1 onward, a job is executed only if the job owner has permissions to execute the job. When an administrator reassigns a job to a user, Junos Space Platform checks whether the user has the permissions needed to execute the job; if the user does not have the permissions, the job is not reassigned. In addition, when an administrator modifies a user account, a notification is displayed if the removal of role affects any previously scheduled jobs.
- **Automatically detecting and dynamically updating network topology changes**—After the topology is discovered by Junos Space Network Monitoring Platform, any changes to the topology are automatically detected and the data related to the topology changes is updated dynamically. In addition, only nodes or node links that are updated are redrawn, not the entire topology.
- **Color-coding and dynamically updating the node link status**—The Network Monitoring Topology page provides an option to display a color-coded link status: a green link indicates that the link is up and a red link indicates that a link is down. When an SNMP trap is received indicating that the link status has changed, the node link status is dynamically updated in the topology.
- **Enhancements to the Network Monitoring UI**—The Network Monitoring UI has been updated to make it consistent with the rest of the Junos Space Network Management Platform UI.
- **Support for specifying devices by using tags or a CSV file in the Operation workflow**—You can select devices on which you want to run an operation by using tags or a comma-separated values (CSV) file.
- **Retrying failed or canceled jobs**—You can retry jobs that failed or were canceled on all devices or on the devices on which the job was not executed. In addition, you can schedule the jobs to be retried later. You can retry the following job types:
 - Backup or restore configuration files
 - Validate or deploy configuration
 - Stage or execute a script
 - Execute an operation
 - Undeploy template
 - Deploy template
 - Deploy device image
 - Stage device image

- Verify device image
- Stage or execute a script bundle
- Backup database
- Resynchronize network elements
- **Changing the target for scheduled jobs**—You can reschedule and modify the recurrence settings of previously scheduled jobs. For jobs that use dynamic tags for device selection, click the **Parameters** column on the Job Management page to view the dynamic tags.
- **Enhancements to the CLI Configlets and the Images and Scripts workspaces**—With the enhancements to the CLI Configlets and the Images and Scripts workspaces, you can perform the following tasks:
 - Filter CLI Configlets by tags when applying the CLI Configlets to devices
 - Filter CLI Configlets by tags when executing the CLI Configlets to devices
 - Search all columns related to CLI Configlets on the **Apply Configlets** page
 - Use the **Reference Number** field to provide a unique reference to CLI Configlets
 - Create CLI Configlets with the **Password Field** or **Password Confirm Field** parameter types.
 - Use the "password" option for the variable context script annotation to specify that input parameters (on the Junos Space Platform UI) are obscured for operational scripts.
 - Mark CLI Configlets, scripts, and script bundles as favorites.
 - All objects marked as favorites are associated with the My Favorite tag.
- **Domain and User Account enhancements**—With the enhancements to the Domain and User Accounts feature in the Role-Based Access Control workspace, you can perform the following tasks:
 - Domain hierarchy—Create up to five levels of subdomains below the Global domain.
 - You can perform the **Assign to Domain** action on more than one object (of the same type) at the same time.
 - **Assigned Domains** column—Use the **Assigned Domains** column in the Domain creation workflow to filter users who are assigned to a specific domain and assign these users to the domain.
 - Absolute path for domain names on all inventory landing pages—Domains are displayed with an absolute path representing the hierarchy of the domain with which the object is associated.
 - Unique namespace for objects across domains—You can create objects with the same name across domains. You can create the following objects with the same name across domains: Templates, Template Definitions, CLI Configlets, Configuration Views, XPath and Regex, Configuration Filters, Report Definitions, Images, Script Bundles, and Operations.

- Progress bar to view the progress of object assignment to domains—A progress bar displays the progress of the task to assign multiple objects to the domain. You can view the progress bar when you assign objects from all supported workspaces.
- **Use Same Roles Assigned to** and **Use Same Domains Assigned to** settings—Use the **Use Same Roles Assigned to** and the **Use Same Domains Assigned to** settings in the User Account creation workflow to search for and filter existing users and copy the roles or domains assigned to them. This allows you to assign to a new user the same roles and domains that are assigned to an existing user quickly.
- **Enhancements to quick templates**—The following enhancements are added to quick templates:
 - Export and import quick templates in XML format.
 - Add comments in the CLI-based template editor.
- **Enhancement to job details**—View fuller descriptions of the status for the following jobs:
 - Backup configuration files
 - Delete configuration files
 - Restore configuration files
 - Execute script
 - Disable scripts on devices
 - Enable scripts on devices
 - Remove scripts on devices
 - Stage scripts on devices
 - Run operation
- **Enhancements to exporting and importing tags, user accounts, roles, and domains**—With enhancements to exporting and importing tags, user accounts, roles, and domains in several workspaces, you can perform the following tasks:
 - Export public and private tags from the Administration workspace in CSV format.
 - Export user accounts from the Reports workspace in CSV, PDF, and HTML formats.
 - Export user-defined roles from the Role-Based Access Control workspace in CSV format.
 - Import new roles to Junos Space Network Management Platform from the Role Based Access Control workspace by using an XML file.
 - Export a domain and its associated subdomains from the Role Based Access Control workspace in CSV format.
- **Viewing the device configuration in alphabetical order**—Click the **Custom Settings** icon, and select the **Enable Alphabetic Ordering** check box on the **View Active Configuration** page to view the configuration options for a device in alphabetical order. You can also enable this feature for the filtered view of the device configuration.

- **Support for the Junos OS confirmed-commit feature**—From Junos Space Network Management Platform Release 14.1R1 onward, by default, Junos Space Network Management Platform uses a confirmed-commit for all commit operations on all devices that are discovered by Junos Space and that support the **confirmed-commit** NETCONF capability. The default timeout is ten minutes. To perform confirmed-commit operations from Junos Space Platform, you must publish the configurations that were created using templates.
- **Enhancements to the Model Device workflow**—With the enhancements to the Model Device workflow, you can perform the following tasks:
 - Activate modeled devices by using Junos Space–initiated or device-initiated discovery methods depending on whether the devices are reachable or unreachable.
 - Model and activate a device by using the Create Modeled Instance workflow.
 - Modify the configuration on a modeled device by using the schema-based device configuration editor.
 - Assign and deploy configuration templates and quick templates to modeled devices automatically during activation or manually by using the deployment workflows.
- **Cloning Devices**—You can clone a modeled or real device managed by Junos Space Network Management Platform by using the Clone Device workflow; the clone can be activated and managed using the Activate Modeled Device workflow.
- **Enhancements to Looking Glass**—You can execute a wider range of **show**, **ping**, and **traceroute** commands on devices. You can configure a timeout to allow more time to execute commands that take a longer time to execute on devices. You can also export the results of the executed commands in CSV and DOC formats.

To view the list of commands that are supported, type the first few letters of the command in the **Execute Command** text box in the **Looking Glass** page; for example, typing **sh** lists the supported commands that start with **sh**.

- **Enhancements to the Secure Console**—You can resize, minimize, and maximize the Secure Console terminal window by using standard mouse and keyboard controls. You can also copy and paste CLI commands in the terminal window by using standard keyboard shortcuts.
- **Warnings to logged-in users before reboot or shutdown**—Administrators can specify a time after which nodes are rebooted or shut down and specify a customized notification for logged-in users. When the reboot or shutdown workflow is initiated, the users logged in to the nodes being rebooted or shut down receive a warning message on their consoles and browsers; nodes are rebooted or shut down after the previously specified time elapses.
- **Creating versions of a device template**—A new version of a device template is created when you modify a device template that is assigned or deployed to the devices. You can select a device template version to assign, deploy, undeploy, unassign, and audit template configuration on the devices.
- **Cloning and comparing device templates**—Compare two versions of device templates to view the differences in configuration between the templates by using the Compare Template Versions workflow. In addition, you can compare a the configuration in a

device template with the configuration on the device by using the Compare Template Against Device workflow. You can also clone device templates by using the Clone Templates workflow.

- **Connecting to devices by using SSH from the Network Monitoring workspace**—On the Topology page (in the Network Monitoring workspace), you can connect to one or more devices by using SSH. You can also connect to the same device one or more times; a new SSH window is created for each connection.
- **Progress bar for adding or upgrading Junos Space applications**—When you add a Junos Space application or upgrade an existing Junos Space application, a progress bar is displayed.
- **Enhancements to the Junos Space startup page**—When Junos Space Network Management Platform is starting up, the startup page displays a progress bar indicating the percentage of startup completed, the estimated time left for completing the startup, and a list of tasks to complete (with the current task pointed out). When a task is successfully completed, a message is displayed; if a task fails, an error message is displayed indicating why the task failed.
- **Support for MS-CHAP v2**—Starting from Junos Space Network Management Platform Release 14.1R1, Junos Space Network Management Platform supports the use of Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) for RADIUS authentication.
- **Enhancements to hosted virtual machines**—The IP address of the hosted virtual machine is displayed on the Fabric and Space Node Settings pages (in the Administration workspace). In addition, for a hosted virtual machine, you can modify the IP address, subnet mask, and gateway IP address. Additional warnings are displayed when nodes that are being shut down or rebooted include hosted virtual machines.

Operational Notes

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

- If you select the **Add SNMP configuration during device discovery** check box on the **Administration > Applications > Modify Network Management Platform Settings** page and discover a device whose trap target is updated, clicking Resync Node from the Network Monitoring workspace does not reset the trap target for the device.
- If you clear the **Add SNMP configuration during device discovery** check box on the **Administration > Applications > Modify Network Management Platform Settings** page, the trap target is not set for the device during device discovery and resynchronizing node operations.
- If you select the **Add SNMP configuration during device discovery** check box on the **Administration > Applications > Modify Network Management Platform Settings** page, stop the Network Monitoring service from the **Administration > Applications > Manage Services** page, and discover a device, the trap target is not added to the device. To set the trap target for the device, start the Network Monitoring service from the **Administration > Applications > Manage Services** page and resynchronize the node list by using the **Network Monitoring > Node List > Resync Nodes** workflow. The newly

discovered device is added to the Network Monitoring node list and the trap target is added to the device.

- If you want to perform a global search on a device, jobs, or audit logs inventory landing page by 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 you to decide whether to continue running the slow script. Refer to <http://support.microsoft.com/kb/175500> for instructions on 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 900 seconds. To reduce this time period, modify the **Polling time period secs** setting for Network Management Platform (**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 the Key Conflict Authentication status. To resolve the conflict on the devices and bring them back to a key-based state, upload the RSA keys manually (**Devices > Upload Keys to Devices**).
- Devices such as the BX Series and MCG5000 devices that do not use system status log files 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.
- The **EnterpriseDefault** (uei.opennms.org/generic/trap/EnterpriseDefault) event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the **EnterpriseDefault** event.

For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic in the *Junos Space Network Management Platform User Guide*.

- When a physical hard drive is removed from a Junos Space hardware appliance (JA1500 or JA2500) or a logical hard drive is degraded, the corresponding SNMP traps (`jnxSpaceHardDiskPhysicalDriveRemoved` and `jnxSpaceHardDiskLogicalDeviceDegraded` respectively) are generated and displayed as events in the Network Monitoring workspace. Later, when the physical hard drive is reinserted, the corresponding events (`jnxSpaceHardDiskPhysicalDriveAdded` and `jnxSpaceHardDiskLogicalDeviceRebuilding`) are generated and displayed in the Network Monitoring workspace; however, the alarms previously raised for the removal of the physical hard drive are not cleared automatically. You can clear these alarms manually,

if required. The alarms for the reinsertion of the physical hard drive are automatically cleared after a few minutes because they are of the **Normal** type.

- If the administrator password for a Fault Monitoring and Performance Monitoring (FMPM) node is modified using the Junos Space CLI, the disaster recovery with the FMPM node fails and new users added in Junos Space (after the password is modified) are not synchronized to the FMPM node. This is because the modified administrator password is not automatically updated in the Junos Space MySQL database.

To ensure that the synchronization to the FMPM node takes place, you must run the `/var/www/cgi-bin/changeSpecialNodepassword.pl` script so that the modified FMPM node password is updated in the Junos Space MySQL database. The syntax for the script is as follows: `/var/www/cgi-bin/changeSpecialNodePassword.pl fmpm-node-ip fmpm-node-password`, where `fmpm-node-ip` is the IP address of the FMPM node, and `fmpm-node-password` is the modified password for the FMPM node.

- Junos Space Network Management Platform Release 14.1R1 uses OpenSSL version 0.9.8e-27.el5_10.3. Although this version is based on the older 0.9.8e branch, it contains all relevant security updates and fixes (current up to the June 2014 release) provided by OpenSSL and CentOS. For further details regarding fixes and CVEs included in this OpenSSL version, execute the following command on the Junos Space debug shell: `rpm -q openssl-0.9.8e-27.el5_10.3 -changelog`.

Changes in Default Behavior

- From Junos Space Network Management Platform Release 13.3R1 onward, the Users workspace is renamed Role Based Access Control.
- On the Fabric page, the application logic status of Junos Space nodes is shown as UP only after all the Enterprise Archive (EAR) files for the Junos Space node are deployed and the schemas are processed. [PR/951985]
- The name of the sample comma-separated values (CSV) file downloaded from the Images and Scripts workspace is changed to **DeviceSelectSample.csv**. [PR/1002481]
- The **Linkd** menu item on the **View** menu on the Network Monitoring Topology page is renamed to **EnLinkd**.
- In Junos Space Network Management Platform Release 14.1, the SNMP polling time for discovering links between devices is set using the **rescan_interval** parameter in the **Enhancedlink.xml** file. In prior releases, this SNMP polling time for discovering links between devices was set using the **snmp_polling** parameter in the **linkd.xml** file. The default value for the **rescan_interval** parameter is 86,400,000 milliseconds
- Changes have been made to the following Network Monitoring Topology layouts:
 - D3 layout—This layout is added.
 - ISOM layout, KK layout, and Spring layout—These layouts are deprecated.
 - FR layout—This layout is modified.
- When you expand the drive size of the virtual machine (for a Junos Space Virtual Appliance) by using the Junos Space CLI, the following warning message is displayed before you select the partition that you want to expand: **Warning: As part of expanding**

disk partition, all disk space allocated for Junos Space instance will completely be allocated to the chosen partition. To add more disk space to other partitions, additional disk space needs to be allocated to the Virtual Machine, prior to doing so in Junos Space. [PR/1016882]

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 access a non-HTTPS website. The best practice is to close your browser and relaunch it before logging in to Junos Space.

- : Device-initiated connections to Junos Space may have different IP addresses from those listed in Junos Space. For example, if you use a loopback address to discover a device, you may source the SSH session of the device from its interface address (Junos OS default behavior is to select the default address) instead. This can lead to firewall conflicts.
- 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 in the Topology page:
 - The tooltip on the node displays the status as **Active/Managed** even when the node is down.
 - For an SRX Series 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 a change request is created and deployed (Device Managed Status: Space & Device Changed) using the configuration editor, the deployment fails. This is an appropriate and expected behavior because 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 displays Device Changed. This is by design.
- RMA is not supported on devices running ww Junos OS, and devices that are not running Junos OS.
- Script Manager supports only Junos OS Release 10.x and later.

- A 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) take effect only at the next login.
- Looking Glass functionality is not supported on logical systems.
- For devices running Junos OS Release 12.1 or later, the following parameters do not display any data in the Network Monitoring workspace because the corresponding MIB objects have been deprecated:
 - jnxJsSPUMonitoringFlowSessIPv4
 - jnxJsSPUMonitoringFlowSessIPv6
 - jnxJsSPUMonitoringCPSessIPv4
 - jnxJsSPUMonitoringCPSessIPv6
 - jnxJsNodeSessCreationPerSecIPv4
 - jnxJsNodeSessCreationPerSecIPv6
 - jnxJsNodeCurrentTotalSessIPv4
 - jnxJsNodeCurrentTotalSessIPv6

Known Issues

The following issues are still outstanding in the Junos Space Network Management Platform Release 14.1R1. For each entry, the identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- If you assign a device to a different domain and there are dependencies, Junos Space correctly blocks the assignment but sometimes the Junos Space user interface does not display an error message. [PR/1003361]
- If you uninstall the Log Director application from Junos Space Network Management Platform Release 14.1R1, the Security Director dashboard displays a blank page.

Workaround: Restart the JBoss service on all nodes in the Junos Space fabric by entering the **service jboss restart** command on the Junos Space debug shell. After all the nodes restart, widgets are displayed on the Security Director dashboard. [PR/1003353]

- If you modify the node management IP address (eth0) or the virtual IP address of a node using the Junos Space CLI, the IP address of the device management interface (eth3) of the node is also reset.

Workaround: Modify the node management IP address (eth0) or the Virtual IP address(eth0:0) on the **Administration > Fabric > Space Node Settings** page from the Junos Space GUI. [PR/1000931]

- When you upgrade to Junos Space Network Management Platform Release 13.3R2, the SNMP configuration to monitor the power supply of a Junos Space Appliance is not automatically added to the `/etc/snmp/snmpd.conf` file.

Workaround:

1. Navigate to the **Administration > Fabric** page.
2. Right-click the Junos Space Appliance and select **SNMP Configuration**.

The SNMP Configuration page for the Junos Space Appliance is displayed.

3. Wait for the page to load. When the page loads, the default SNMP configuration is displayed. Click **Cancel**.

The code required to monitor the power supply of the Junos Space Appliance is added to the `/etc/snmp/snmpd.conf` file.

[PR/997938]

- 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]

- The remote users assigned to a domain through a remote profile are not listed on the Assigned Users tab for that domain on the Domains inventory landing page. [PR/946323]
- 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]
- 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:

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

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

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

3. From the Edit menu, select **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 the Registry Editor.

For more information, refer to <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:

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

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

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

3. From the Edit menu, select **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 to <http://support.microsoft.com/kb/323308> . [PR/933656]

- You may see the **Junos Space is Starting...** message on the Junos Space user interface for 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]
- 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 physical interfaces using the **Device Name** column in the Physical Interfaces view on the Device Management page. [PR/931925]
- You receive an email from ?root@host? from the disaster recovery setup. [PR/919436]

Workaround: Move the **mcelog.cron** file from the **/etc/cron.hourly** directory to the **/var/tmp** directory. This stops the notification.

- The FPM node contains irrelevant RPMs installed. [PR/883610]

- For FMPM nodes, you cannot change the network settings using the Junos Space CLI. [PR/893184]
- The SPACE-PLATFORM-MIB cannot differentiate between a Junos Space node and an FMPM node. [PR/909382]
- A user with the custom user role can view the Generated Reports page even if the View Generated Report privilege. The Generated Reports page can be viewed even if the View Generated Report privilege is not selected for a custom user role. [PR/889084]
- You cannot set a domain name for a QFabric device through the Basic Setup Wizard. [PR/895442]
- Group settings that are applied on the device are not displayed in the Basic Setup Wizard. [PR/884068]
- When a node is set as "Inactive" in the device configuration, the Basic Setup Wizard incorrectly displays the node as "Active." [PR/884074]
- The last row of the page is truncated for all generated reports. [PR/889088]
- The LmSensors and UCD-SNMP MIBs 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 address and node IP settings are modified using the Junos Space CLI, all the devices 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 private tags in Junos Space. [PR/860854]
- Although M Series, MX Series, and ACX Series devices do not support PPP as an encapsulation type, you can use the configuration editor in Junos Space Network Management Platform to configure the PPP encapsulation. [PR/833612]
- Old SNMP trap targets are not removed from the device when the network settings on the Junos Space Appliance are modified. [PR/689042]
- The RMA feature does not currently work for devices running Junos OS. [PR/791987]
- Users without Assign/Unassign Template permissions are allowed to add templates to and delete templates from the View Assigned Shared Objects wizard. [PR/816788]
- When you discover devices on Junos Space Network Management Platform Release 14.1R1 by using device-initiated connections and modify the node management IP address of the Junos Space node, the **outbound-SSH** configuration on the discovered devices is not updated with the modified node management IP address.

Workaround: Use the template editor or configuration editor to update the modified node management IP addresses on the discovered devices. [PR/869846]

- Changes made to the candidate configurations in prior releases of Junos Space Network Management Platform are discarded when you upgrade to Junos Space Network Management Platform Release 14.1R1.

Workaround: Deploy all configuration changes made through the candidate configuration on the **Review/Deploy Configuration** page (under **Devices > Device Management**) before upgrading to Junos Space Network Management Platform Release 14.1R1. [PR/887739]

- When a physical hard drive is removed from a Junos Space hardware appliance (JA1500 or JA2500) or a logical hard drive is degraded, the corresponding SNMP traps (jnxSpaceHardDiskPhysicalDriveRemoved and jnxSpaceHardDiskLogicalDeviceDegraded respectively) are generated and displayed as events in the Network Monitoring workspace. Later, when the physical hard drive is reinserted or the logical hard drive is regenerated, the corresponding events (jnxSpaceHardDiskPhysicalDriveAdded and jnxSpaceHardDiskLogicalDeviceRebuilding respectively) are generated and displayed in the Network Monitoring workspace; however, the alarms previously raised for the removal of the physical hard drive or the degradation of the logical hard drive are not cleared automatically. You can clear these alarms manually, if required. The alarms for the reinsertion of the physical hard drive and the regeneration of the logical hard drive are automatically cleared after a few minutes. [PR/888166]
- If the domain ID is not specified in the POST query parameters, all resources or jobs are created in the domain (within the permission tree) to which the user is assigned. If the user is assigned to more than one domain, you must specify the domain for which the API is scoped using the query parameters **domainContext=(currentDomainId eq id)**. For example, **POST on URL**
/api/template-management/templates?domainContext=(currentDomainId eq 3453). [PR/975576]
- When you upgrade to Junos Space Network Management Platform Release 14.1R1, some scheduled jobs are canceled or cannot be retried if they failed. This is because job parameters may have changed in Release 14.1R1 due to bug fixes and enhancements.

Workaround: Re-create and reschedule the jobs after the upgrade to Junos Space Network Management Platform Release 14.1R1 is completed. [PR/978232]

- Recurring jobs created in previous releases of Junos Space Network Management Platform Release do not run after you upgrade to Junos Space Network Management Platform Release 14.1R1.

Workaround: After the upgrade, re-create the recurring jobs on Junos Space Network Management Platform Release 14.1R1. [PR/995934]

- After you upgrade to Junos Space Network Management Platform Release 14.1R1, the **Reports > Generated Reports > View/Download** page does not display reports generated using Junos Space Network Management Platform Release 13.3R1 or earlier.

Workaround: Back up previously generated reports on an external system by downloading the reports (in CSV, HTML, or PDF) *before* performing the upgrade. After

the upgrade, regenerate the new reports by using the existing report definitions from the **Reports > Report Definitions** page. [PR/1002281]

- On the **Device Management > Device Configuration > View/Assign Shared Objects** page, only the latest version of a previously created template can be assigned to the device. [PR/1003810]
- When Junos Space Network Management Platform is configured to use remote authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2), the authentication fails when you enter the username in the *domain\username* format.

Workaround: Enter the username in the *domain@username* format. [PR/1005943]

- The EnterpriseDefault (uei.opennms.org/generic/trap/EnterpriseDefault) event appears on the Events page in the Network Monitoring workspace only if there is no associated event definition for a received event. To create the required event definition, compile the MIB corresponding to the object ID (OID). You can find the OID by reviewing the details of the EnterpriseDefault event. For more information about compiling SNMP MIBs, refer to the [Compiling SNMP MIBs](#) topic in the *Junos Space Network Management Platform User Guide*. [PR/1006133]
- When you connect to a device by using SSH, you can edit the contents of the file in the vi editor; however, only limited vi editor functionality is supported. You cannot use the left, right, up, and down arrow keys to navigate within the file, but you can use the vi editor's standard keys—H (left arrow), J (down arrow), K (up arrow), and L (right arrow). [PR/1009106]
- When Junos Space Network Management Platform is configured to use remote local authentication with a RADIUS server that uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2) and the RADIUS server is integrated with an RSA Authentication Manager Server, the Access Challenge requests between the RSA server and the RADIUS server do not work correctly.

Workaround: Use RADIUS servers configured with the Password Authentication Protocol (PAP) when you are using an RSA Authentication Manager Server. [PR/1009543]

- Though Firefly devices are displayed on the Network Monitoring Topology page, the links between such devices are not displayed. [PR/1011207]
- In the Network Monitoring Topology page, the display of bridge links between devices is not supported. [PR/1011230]
- If a report definitions is created in a prior release of Junos Space Network Management Platform and a Generate Report recurring job is scheduled, the job is deprecated when you upgrade to Junos Space Network Management Platform Release 14.1R1.

Workaround: Re-create the job you upgrade to Junos Space Network Management Platform Release 14.1R1. [PR/1012568]

- After a Junos Space application is installed on Junos Space Network Management Platform and you select the application from the Applications list box, only the application's dashboard is displayed. The application's workspaces might not be displayed in the navigation tree, or if they are displayed, you cannot access the tasks because of an error.

Workaround: After the application is installed successfully, log out of Junos Space and log in again to fix this issue. [PR/1016463]

- On the Network Monitoring Topology page, when you clear the existing nodes in focus and click Use Default Focus (in the Node Display Warning dialog box), the names of the nodes in focus are not displayed. [PR/1017453]
- In some cases, when you use Mozilla Firefox version 31.0 to access the Junos Space GUI, the Junos Space Login page does not load. This issue has been observed on PCs running both Mac OS X and Microsoft Windows. (For more information about this issue, refer to the following links on the Mozilla Firefox Support website:
<https://support.mozilla.org/en-US/questions/1012728#answer-616338> and
<https://support.mozilla.org/en-US/questions/1012765>.)

Workaround:



NOTE: The following steps are for Mozilla Firefox version 31.0 running on Microsoft Windows; the procedure for Mac OS X might differ.

1. On the Mozilla Firefox menu bar, click **Tools** and select **Options**.
The Options dialog box is displayed.
2. Click the **Advanced** icon and then select the **Certificates** tab.
3. Click **View Certificates**.
The Certificate Manager dialog box is displayed.
4. Select the **Authorities** tab.
5. On the **Authorities** tab, select the entries for one or more Junos Space Platform virtual IP (VIP) addresses that you are unable to access in Firefox.
6. Click **Delete or Distrust**.
A dialog box lists the previously selected entries.
7. Click **OK**.
The entries that you selected are deleted.
8. Click **OK** in the Certificate Manager dialog box, and then click **OK** in the Options dialog box.
9. (Optional) Restart Firefox.
10. In the Mozilla Firefox address bar, type the VIP address that you want to access.
You should now be able to access the Junos Space Login page.

[PR/ 1017999]

- M Series, MX Series, and T Series device images that are imported into Junos Space Network Management Platform are not filtered and displayed on the Images page

when you click the bar for **M** or **MX** or **T** on the **Device Image Count by Platform Group** chart (in Images and Scripts page). [PR/1018176]

- In Internet Explorer versions 8, 9, 10, and 11, after you switch a domain using the domain switcher, the domain switcher list box automatically expands and cannot be minimized.

Workaround: Click elsewhere on the page to minimize the domain switcher list box. If you switched domains from the Network Monitoring workspace, click the navigation tree or the header bar, or navigate to another page. [PR/1018804]

- When you retry a failed Stage Script job, the Script(s) tab in the Job Target dialog box, which appears when you click the Script(s):*no* link in the Parameters column (on the Job Management page), displays the version of the script as null. However, when you double-click the job, the script version is displayed correctly in the dialog box. [PR/1018742]

- When you select a category on the Topology page, log out of Junos Space and log in, the nodes in the previously selected category are added to the focus along with the category; in addition, you cannot remove the category from the focus by clicking the Remove from focus (x) button.

Workaround: To remove the category from the focus, search for and select the same category on the Topology page, and then click the Remove from focus (x) button. [PR/1019193]

- For device templates, the **Compare Template Against Device** task fails when you specify that the task should recur. The sequence of steps that lead to this error are as follows:

1. Select a device template from the **Device Templates > Templates** page.
2. Select **Compare Template Against Device** from the Actions menu.
The Compare Template Against Device page appears.
3. Select the devices to be compared and click **Next**.
4. Select the **Recurrence** check box and click **Finish**.
The Audit Log dialog box displays an internal server error message.
5. Click **OK**.

The error is also recorded in the server log. [PR/1019856]

- When you configure eth3 as the device management interface and monitor a device that is in a different subnet than that of the eth3 interface, Network Monitoring fails to monitor the device.

Workaround: Add an FMPM node and configure the eth0 interface on the FMPM node with the same information as the eth3 interface on the Junos Space node. [PR1137980]

Resolved Issues in Junos Space Network Management Platform Release 14.1R1

The following issues are resolved in Junos Space Network Management Platform Release 14.1R1. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- 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 device running Junos OS. [PR/563648]
- The LSYS feature does not support the deletion of both root and LSYS at the same time. Delete them one at a time. [PR/754683]
- The contents of pop-up windows in Junos Space Network Management Platform cannot be resized. [PR/856110]
- Script execution on a device fails if the device returns a warning message. [PR/856224]
- A zombie user from a former standby node appears after a switchover to a different Junos Space node. [PR/858198]
- The Manage CSV Files task (**Device Templates > Definitions**) now supports single quotation mark and comma. [PR/867131]
- If you change the authentication mode through the CLI by using the **setSpaceAuthMode** script, the change is not displayed in the user settings on the Junos Space user interface. [PR/888220]
- In a multinode fabric, SNMP v2 settings configured on the **Fabric > SNMP Manager** page are not updated properly in the `/opt/opennms/etc/snmp-config.xml` file. [PR/909643]
- Devices with the connection type "Reachable Device initiated" do not reconnect after disaster recovery. [PR/919433]
- You can perform a search operation on the landing page only if you enter the full keyword or use "*" before and after the keyword to be searched. [PR/925667]
- In the Network Monitoring workspace, you can now search for events that occurred in the past 1 hour, 4 hours, 8 hours, and 12 hours without providing text parameters for the event. [PR/933295]
- You can stage device images from the Junos Space user interface on a dual Routing Engine device even if sufficient space is not available on the backup Routing Engine. [PR/933302]
- Global search and searching from the inventory landing page are not supported on some columns in the Job Management and Audit Logs workspaces. [PR/935765]
- 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]
- When you upgrade the device image on some devices using the Rapid Deployment workflow, a device-platform mismatch occurs. [PR/939078]
- Role Based Access Control privileges assigned to a custom user role for Quick templates do not work effectively. [PR/940294]
- 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]
- Log files cannot be retrieved from the Junos Space CLI if the file size is smaller than 1 GB. [PR/944970]

- Timestamp-related columns on 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 by using the PST timestamp does not return any search results. [PR/946327]
- Junos Space Network Management Platform is not able to discover and manage TXP series devices if **netconf ssh** is not configured on the device. [PR/946422]
- 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]
- Clicking 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]
- From the Device Access page, you cannot connect to a device using SSH (**SSH to Device**) because of the comma character in the device password. [PR/952661]
- In a multinode cluster, the notifications are not displayed after the failover. [PR/955498]
- In some cases, if you search for content on a page before the page has completely loaded, the filters do not provide the correct results. [PR/959467]
- The Generate Key passphrase is visible on the Junos Space Network Management Platform UI. [PR/960187]
- Junos Space Network Management Platform does not validate schemas uploaded in offline mode, which leads to errors. [PR/960802]
- 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]
- The firewall blocks SNMP access to the external SNMP manager added from the **Administration > Fabric > SNMP Manager** page. [PR/966142]
- 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. [PR/961266]
- On the Authentication Servers page, modifying the TACACS+ entry causes the **Port Number** field to be automatically changed to 49 even if a different value was specified previously. [PR/962448]
- During JBoss initialization, the error message file **Exception is: For input string: "18446744073709551615"** is logged in the **server.log** file. [PR/962861]
- Junos Space is unable to perform database backups to a remote server running OpenSSH version 6.2p2. [PR/966212]
- Junos Space incorrectly provides an **Upgrade Platform** option during software image upload. [PR/967417]

- MIB groups added to a system definition from the Junos Space user interface are not saved. [PR/967705]
- SNMP monitoring of JBoss parameters is not supported due to the lack of snmp-adapter for JBoss version 7. [PR/968233]
- In 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]
- In some cases, the child LSYS status is not updated correctly if the root LSYS status changes from UP to DOWN or vice versa. [PR/969420]
- For devices with permission labels assigned to them, the 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. In addition, when you back up a configuration file in a subdomain, the associated configuration file version is incorrectly updated as global, rather than with the name of the subdomain. [PR/971376]
- A configuration with the **route-filter with prefix-length-range** command that is pushed to the device through a template fails. [PR/971688]
- After changes are made to the RADIUS server, the Junos Space UI grays out intermittently. [PR/972413]
- On the Templates page, the **Sort Ascending** and **Sort Descending** options in the **State** column do not work. [PR/976589]
- The **Starting jmp-firewall: Error 2003 (HY080) Can't connect to MySQL server** message is displayed during the Junos Space Network Management Platform boot sequence. [PR/982691]
- During the creation of a service template, the **set interfaces ge-x/y/z per-unit-scheduler** configuration is not available. [PR/986185]
- If you modify the timezone from the CLI menu of the Junos Space hardware appliance or virtual appliance and reboot, the timezone is not updated. [PR/987118]
- When you access Junos Space Network Management Platform in Internet Explorer, SNMPv3-specific parameters (in **Network Monitoring > Admin > Configure SNMP Community Names by IP**) are not displayed. [PR/999300]
- The **Use Same Roles Assigned to** field is not available on the Domain Assignment page in the User Creation workflow. [PR/999320]
- Junos Space sends **mcelog: warning: record length longer than expected. Consider update** messages. [PR/999413]
- When a configuration is applied to a device by using templates, Junos Space Network Management Platform adds extra quotation marks to the login banner. [PR/1007131]

- A configuration pushed using a quick template fails because of the extra quotation marks in the configuration generated by Junos Space Network Management Platform. [PR/1007142]
- If you click the **Definition Name** of a report, the **Index: 0, Size: 0** error message is displayed. [PR/1007339]
- Modify the labels for the **Read-only access to parent domain** and **Allow users of this domain to have read-only access to parent domain** fields. [PR/1007444]
- The Global Search function is supported on all columns in the following workspaces: Configlets, Configuration View, Scripts, Templates, Xpath and Regex, Images, Report Definitions, Generated Reports, Config Files, and User. [PR/1009103]
- If you connect to a device by using SSH and then delete the device from Junos Space, the SSH connections to the device are not removed. [PR/1009489]
- In-band cluster upgrade (ICU) upgrade across branch SRX Series clusters fails from Junos Space Network Management Platform. [PR/1015575]

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 14.1R1 documentation:

- The *Fabric Management Overview* topic in the Junos Space Network Management Platform online Help includes an incorrect link to the Junos Space Appliance and Junos Space Virtual Appliance documentation. The correct link is http://www.juniper.net/techpubs/en_US/release-independent/junos-space/index.html.
- The **Upgrading Junos Space Network Management Platform** topic in the Junos Space Network Management Platform online Help includes incorrect information about upgrade paths. Refer to the [Upgrading from Prior Releases of Junos Space Network Management Platform on page 5](#) section for the correct information.
- The **Upgrading Junos Space Software Overview** topic in the Junos Space Network Management Platform online Help contains information about Junos Space Network Management Platform Release 13.3R1. Refer to the [Upgrading Junos Space Software Overview](#) topic for information about Junos Space Network Management Platform Release 14.1R1.

Junos OS Compatibility

For Junos OS compatibility information, see the FAQ topic [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

21 Aug 2014—Revision 1, Junos Space Network Management Platform Release 14.1R1

19 Sep 2014—Revision 2

16 Feb 2015—Revision 3

15 Jan 2016—Revision 4

13 June 2016—Revision 5

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.