

Junos Space Network Management Platform Release 19.4R1 Release Notes

19.4R1
10 January 2022
Revision 5

| | |
|-----------------|---|
| Contents | Introduction 3 |
| | Junos Space Network Management Platform Release Notes 3 |
| | New and Changed Features 4 |
| | Installation Instructions 4 |
| | Upgrade Instructions 5 |
| | Supported Upgrade Path 5 |
| | Upgrade Notes 7 |
| | Instructions for Validating the Junos Space Network Management Platform OVA Image 8 |
| | Application Compatibility 11 |
| | Supported Hardware 11 |
| | Supported Devices 12 |
| | Changes in Default Behavior 13 |
| | Known Behavior 15 |
| | Known Issues 21 |
| | Resolved Issues 22 |
| | Hot Patch Releases 23 |
| | Installation Instructions 23 |
| | Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches 24 |
| | Documentation Updates 27 |
| | Finding More Information 28 |

Documentation Feedback | 28

Requesting Technical Support | 29

Self-Help Online Tools and Resources | 29

Creating a Service Request with JTAC | 30

Revision History | 30

Introduction

Junos Space is a comprehensive network management solution that simplifies and automates management of Juniper Networks switching, routing, and security devices.

Junos Space Management Applications optimize network management by extending the breadth of the Junos Space solution for various domains in service provider and enterprise environments.

Junos Space Network Management Platform Release Notes

IN THIS SECTION

- [New and Changed Features | 4](#)
- [Installation Instructions | 4](#)
- [Upgrade Instructions | 5](#)
- [Application Compatibility | 11](#)
- [Supported Hardware | 11](#)
- [Supported Devices | 12](#)
- [Changes in Default Behavior | 13](#)
- [Known Behavior | 15](#)
- [Known Issues | 21](#)
- [Resolved Issues | 22](#)
- [Hot Patch Releases | 23](#)
- [Documentation Updates | 27](#)

These release notes accompany Junos Space Network Management Platform Release 19.4R1.

NOTE: The terms Junos Space Network Management Platform and Junos Space Platform are used interchangeably in this document.

New and Changed Features

Junos Space Network Management Platform Release 19.4R1 includes the following enhancements:

- **CLI configlets information in audit logs description**—Junos Space Network Management Platform Release 19.4R1 provides additional information such as configlet name and device name in the audit logs description, if the following tasks are performed through REST APIs:
 - Apply CLI configlet
 - Validate CLI configlet
- **Purge older device configuration backups from the database**—Starting in Junos Space Network Management Platform Release 19.4R1, you can purge device configuration files that are older than the latest two versions of the configuration files that are backed up.

To purge older device configuration files, use the `/var/www/cgi-bin/cleanUpDevConfigBackup.sh` script.

Installation Instructions

Junos Space Network Management Platform Release 19.4R1 can be installed on a Junos Space Appliance or a Junos Space Virtual Appliance.



CAUTION: During the Junos Space Network Management Platform installation 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 fails.

- For installation instructions for a JA2500 Junos Space Appliance, see the [Installation and Configuration](#) section of the [JA2500 Junos Space Appliance Hardware Guide](#).
- For installation instructions for a Junos Space Virtual Appliance, see the [Deploying the Junos Space Virtual Appliance](#) section of the [Junos Space Virtual Appliance Installation and Configuration Guide](#).

See “[Supported Hardware](#)” on [page 11](#) for more information about the hardware supported.

Upgrade Instructions

IN THIS SECTION

- Supported Upgrade Path | 5
- Upgrade Notes | 7
- Instructions for Validating the Junos Space Network Management Platform OVA Image | 8

This section provides information about upgrading the Junos Space Network Management Platform installations running versions earlier than Release 19.4R1.

Supported Upgrade Path

Table 1 on page 5 provides information about the supported upgrade path across Junos Space Network Management Platform releases.

Table 1: Supported Upgrade Path

| Upgrade from Junos Space Release | Upgrade to Junos Space Release | | | | | | | | | | | |
|----------------------------------|--------------------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| Junos Space Release | Release 16.1 | Release 16.2 | Release 17.1 | Release 17.2 | Release 18.1 | Release 18.2 | Release 18.3 | Release 18.4 | Release 19.1 | Release 19.2 | Release 19.3 | Release 19.4 |
| Release 16.1 | | Yes | Yes | | | | | | | | | |
| Release 16.2 | | | Yes | Yes | | | | | | | | |
| Release 17.1 | | | | Yes | Yes | | | | | | | |
| Release 17.2 | | | | | Yes | Yes | | | | | | |

Table 1: Supported Upgrade Path (continued)

| Upgrade from Junos Space Release | Upgrade to Junos Space Release | | | | | | | | | | | |
|----------------------------------|--------------------------------|--|--|--|--|-----|-----|-----|-----|-----|-----|-----|
| Release 18.1 | | | | | | Yes | Yes | | | | | |
| Release 18.2 | | | | | | | Yes | Yes | | | | |
| Release 18.3 | | | | | | | | Yes | Yes | | | |
| Release 18.4 | | | | | | | | | Yes | Yes | | |
| Release 19.1 | | | | | | | | | | Yes | Yes | |
| Release 19.2 | | | | | | | | | | | Yes | Yes |
| Release 19.3 | | | | | | | | | | | | Yes |

Related Information

- [Junos Space Network Management Platform Overview](#)
- [Juniper Networks Devices Supported by Junos Space Network Management Platform](#)
- [Upgrading Junos Space Network Management Platform](#)

NOTE: Before you upgrade Junos Space Platform to Release 19.4, ensure that the time on all Junos Space nodes is synchronized. For information about synchronizing time on Junos Space nodes, see [Synchronizing Time Across Junos Space Nodes](#).

You can upgrade the existing Junos Space Platform running on your appliance to the immediate next release. You can also choose to skip a release and upgrade to the next release. For example, you can

upgrade to Junos Space Network Management Platform 19.4R1 from Junos Space Network Management Platform 19.3R1 or 19.2R1.



CAUTION: During the Junos Space Network Management Platform 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 upgrade fails.

Upgrade Notes

- Before the upgrade, ensure that the latest backups are available in a location other than the Junos Space server. For more information about backups, see [Backing Up the Junos Space Network Management Platform Database](#).
- Before upgrading Junos Space Platform Release 19.3 to Junos Space Platform Release 19.4, you must install the **Junos Space Platform 19.3 hot patch v2** version.

If you have proceeded with the upgrade to Junos Space Platform Release 19.4 from Junos Space Platform Release 19.3 without installing the Junos Space Platform 19.3 hot patch v2 version, perform the following steps as a workaround:

- Edit the `/etc/httpd/conf/httpd.conf` file by adding the following PATCH entry:

```
<Location />
  <LimitExcept GET POST PUT PATCH DELETE>
    order deny,allow
    deny from all
  </LimitExcept>
</Location>
```

- Restart the HTTPD service using the **service httpd restart** command.
- To upgrade Junos Space Platform to Release 19.4, follow the instructions provided [here](#).
- 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.
- After you upgrade Junos Space Platform to Release 19.4R1, all previously installed applications are disabled until the applications are upgraded to a version compatible with Junos Space Platform 19.4R1. You must upgrade the applications to releases that are compatible with Junos Space Platform Release 19.4R1, by using the Junos Space Platform UI. For information about application versions compatible with Junos Space Platform 19.4R1, see [“Application Compatibility” on page 11](#).

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:

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

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

2. (Optional) If you downloaded the OVA image and the Root CA certificate chain 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 chain 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 chain 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.

3. Navigate to the directory containing the OVA image.

4. 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 chain 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 chain 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-16.1R1.3.ova
-bash-4.1$ mkdir tmp
-bash-4.1$ cd tmp
-bash-4.1$ tar xf ../space-16.1R1.3.ova
-bash-4.1$ ls
junos-space-certchain.pem space-16.1R1.3.cert
space-16.1R1.3-disk1.vmdk.gz space-16.1R1.3.mf
space-16.1R1.3.ovf
-bash-4.1$ ovftool space-16.1R1.3.ovf
OVF version: 1.0
VirtualApp: false
Name: viso-space-16.1R1.3

Download Size: 1.76 GB

Deployment Sizes:
  Flat disks: 250.00 GB
```

```

Sparse disks: 4.68 GB

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

Virtual Machines:
  Name:          viso-space-16.1R1.3
  Operating System:  rhel5_64guest
  Virtual Hardware:
    Families:      vmx-04
    Number of CPUs: 4
    Cores per socket: 1
    Memory:        8.00 GB

  Disks:
    Index:         0
    Instance ID:    7
    Capacity:       250.00 GB
    Disk Types:     SCSI-lsilogic

  NICs:
    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network

    Adapter Type:   E1000
    Connection:     VM Network

-bash-4.1$ openssl verify -CAfile JuniperRootRSACA.pem -untrusted
junos-space-certchain.pem space-16.1R1.3.cert
space-16.1R1.3.cert: OK
-bash-4.1$

```

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 chain file is corrupted or modified. If it is corrupted or modified, download the Root CA certificate chain 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.

Application Compatibility



WARNING: Before you upgrade to Junos Space Network Management Platform Release 19.4R1, ensure that compatible versions of Junos Space applications are available for upgrade by referring to the [Junos Space Application Compatibility](#) knowledge base article. If you upgrade to Junos Space Platform Release 19.4R1 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.

This release of Junos Space Network Management Platform supports Worldwide (ww) Junos OS Adapter adapter and the following application:.

- Network Director 3.9R1
- Connectivity Services Director 5.1R1
- Cross Provisioning Platform 19.4R1
- Security Director 19.4R1
- Intelligent Customer Extendable authentication, authorization, and accounting (ICE-AAA) Framework 19.4R1

Supported Hardware

Junos Space Network Management Platform Release 19.4R1 can be installed on the following hardware:

- JA2500 Junos Space Appliance
- VMware ESXi server 5.5, 6.0, 6.5, 6.7
- Kernel-based virtual machine (KVM) (Release 1.5.3-141.el7_4.4 or later)

For detailed information about hardware requirements, see the *Hardware Documentation* section of the [Junos Space and Applications](#) page.

NOTE: For information about whether a Junos Space application can be installed on a particular Junos Space Appliance (JA2500) or Junos Space Virtual Appliance, see the release notes of the specific Junos Space application release.

NOTE: For detailed information about hardware requirements, see [Junos Space Virtual Appliance Deployment Overview](#) .

Supported Devices

Junos Space Network Management Platform Release 19.4R1 supports the following additional Juniper Networks device and components running Junos OS:

- QFX5120-32C

For a list of supported devices up to and including Junos Space Platform Release 19.4R1, see [Juniper Networks Devices Supported by Junos Space Network Management Platform](#).

[Table 2 on page 12](#) shows the supported Juniper Networks line cards and PEM (Power Entry Module) / PSM (Power Supply Module) / PDM (Power Distribution Module) in Junos Space Network Management Platform Release 19.4R1.

Table 2: Supported Line Cards and PEM/PSM/PDM

| Device | Line Cards | PEM/PSM/PDM |
|--------|----------------|------------------|
| SRX320 | SRX-MP-WLAN-WW | - |
| MX2020 | - | HV PDM HV PSM |

NOTE: When Junos Space Platform discovers EX Series switches running Layer 2 next generation 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.

NOTE: Previous versions of Junos OS releases are also supported. If you are using previous versions of Junos OS releases, you can continue to use the same versions. For a complete list of Junos OS compatibility and support information, see [Junos OS Releases Supported in Junos Space Network Management Platform](#)

Changes in Default Behavior

- From Release 17.2R1 onward, Junos Space Platform does not sort configurations while comparing templates. In releases earlier than 17.2R1, Junos Space Platform sorts configurations while comparing templates, and this causes Junos Space Platform to trigger incorrect deviation reports because of a change in the order of configuration statements caused by the sorting.
- From Release 17.2R1 onward, Junos Space Platform does not support the click action in the Top 10 Active Users in 24 Hours chart. In releases earlier than 17.2R1, you can click within the chart to view details of the selected item on the corresponding page.
- From Junos Space Platform Release 17.1R1 onward, the VLAN field in reports supports both integer and string values. In releases earlier than 17.1R1, the VLAN field in reports supports only integer values, whereas the **VLAN** field for logical interfaces accepts both integer and string values. This mismatch causes issues in displaying VLAN information for logical interfaces in reports.

From Release 17.1R1 onward, the VLAN option in the Add Filter Criteria section of the Create Report Definition page and the filter support for the VLAN column on the View Logical Interface page are removed.

- From Junos Space Platform Release 16.1R2 onward, the upgrade-related logs at `/var/jmp_upgrade` are added to the troubleshooting logs.
- From Release 17.1R1 onward, Junos Space Platform boot menu accepts text inputs, such as reinstall, when you install the Junos Space Platform software from USB drives. In versions earlier than Release 17.1R1, the boot menu supports only numerical values. From Release 17.1R1 onward, when you do a

reinstall, the software restarts and a local reboot occurs by default. Previously, you had to connect to the console and manually trigger a reboot.

- From Junos Space Platform Release 16.1R2 onward, validation messages are provided for tasks where CSV files are used for device selection, and all devices that are listed in the CSV file are not selected when the task is performed. Validation messages are provided when devices are selected using CSV files from the following pages and dialog boxes:
 - Deploy Device Image dialog box
 - Deploy Satellite Device Image dialog box
 - Stage Image on Device page
 - Stage Image on Satellite Device page
 - Remove Image from Staged Device dialog box
 - Undeploy JAM Package from Device dialog box
 - Verifying checksum of image on device(s) dialog box
 - Stage Scripts on Device(s) page
 - Enable Scripts on Device(s) page
 - Disable Scripts on Device(s) page
 - Execute Script on Device(s) page
 - Remove Scripts from Device(s) dialog box
 - Verify Checksum of Scripts on Device(s) dialog box

From Release 17.1R1 onward, validation messages are provided for the following pages and dialog boxes, too:

- Run Operation page
- Stage Script Bundle on Devices dialog box
- Enable Script Bundle on Devices page
- Disable Script Bundle on Devices page
- Execute Script Bundle on Devices dialog box

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.

- Starting from Junos Space Network Management Platform Release 18.1R1 onwards, to view and edit firewall policies, users must have permissions or roles corresponding to all the attributes present under the Firewall Policies and Shared Objects predefined roles. Go to **Network Management Platform>Role Based Access Control>Roles** to view and assign the relevant roles.
- Tag names can be alphanumeric strings. The tag name can also contain underscores, hyphens, and spaces. However, a tag name must not:
 - Exceed 255 characters
 - Start with a space
 - Contain special characters such as commas, double quotation marks, or parentheses.

NOTE: “Untagged” is a reserved term and, therefore, you cannot create a tag with this name.

- The right-click menu is not available on the Import Licenses (Administration > Licenses > Import License) page. You can use either the browser menu options or the keyboard shortcuts to copy and paste onto the page.
- Device-initiated connections to Junos Space can have different IP addresses from those listed in Junos Space. For example, if you use a loopback address to discover a device, you can 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 Platform, the user details are not updated in the `/opt/opennms/users.xml` file.
- You might observe the following limitations on 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 in-service software upgrade (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.

- 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
- For SNMPv3 traps, if more than one trap setting is configured in the `/opt/opennms/etc/trapd-configuration.xml` file, then the **security-name** attribute for the **snmpv3-user** element must be unique for each configuration entry. If a unique **security-name** attribute is not provided, then SNMP traps are not received by Network Monitoring.

The following is a sample snippet of the `/opt/opennms/etc/trapd-configuration.xml` file with two configuration entries:

```
<?xml version="1.0"?>
<trapd-configuration snmp-trap-port="162" new-suspect-on-trap="false">
  <snmpv3-user security-name="Space-SNMP-1" auth-passphrase="abcD123!"
auth-protocol="MD5" />
  <snmpv3-user security-name="Space-SNMP-2" auth-passphrase="abcD123!"
auth-protocol="MD5"
```



```
privacy-passphrase="zyxW321!" privacy-protocol="DES" />
</trapd-configuration>
```

- On the Network Monitoring > Node List > *Node* page, the `ifIndex` parameter is not displayed for IPv6 interfaces if the version of Junos OS running on the device is Release 13.1 or earlier. This is because IPv6 MIBs are supported only on Junos OS Release 13.2 and later.
- When you modify the IP address of a Fault Monitoring and Performance Monitoring (FMPM) node using the Junos Space CLI, the FMPM node is displayed on the Fabric page but cannot be monitored by Junos Space Platform because of a mismatch in the certificate.

Workaround: After modifying the IP address of the FMPM node using the Junos Space CLI, generate a new certificate on the Junos Space VIP node and copy the certificate to the FMPM node by executing the following scripts on the Junos Space VIP node:

- `curl -k https://127.0.0.1:8002/cgi-bin/createCertSignReq.pl?ip='fmpm-node-ip'&user='admin'&password='password'`
- `curl -k https://127.0.0.1:8002/cgi-bin/authenticateCertification.pl?ip='fmpm-node-ip'&user='admin'&password='password'&mvCertToDestn='Y'`

where `fmpm-node-ip` is the IP address of the FMPM node and `password` is the administrator's password.

- When you execute a script and click the View Results link on the Script Management Job Status page, the details of the script execution results are displayed up to a maximum of 16,777,215 characters; the rest of the results are truncated.

This might affect users who execute the **show configuration** command on devices with large configurations or if the output of a Junos OS operational command (executed on a device) is large.

- When you configure a Junos Space fabric with dedicated database nodes, the Junos Space Platform database is moved from the Junos Space nodes to the database nodes. You cannot move the database back to the Junos Space nodes.
- For a purging policy triggered by a **cron** job:
 - If the Junos Space fabric is configured with MySQL on one or two dedicated database nodes, the database backup files and log files (mainly in the `/var/log/` directory with the filenames `*.log.*`, `messages.*`, or `SystemStatusLog.*`) are not purged from the dedicated database nodes.
 - If the Junos Space fabric is configured with one or two FMPM nodes, the log files (mainly in the `/var/log/` directory with the filenames `*.log.*`, `messages.*`, or `SystemStatusLog.*`) are not purged from the FMPM nodes.
- If Network Monitoring receives two traps within the same second—that is, one for a trigger alarm and another for a clear alarm—then the triggered alarm is not cleared because the clear alarm is not processed by Network Monitoring.

- If you use Internet Explorer versions 8.0 or 9.0 to access the Junos Space Platform GUI, you cannot import multiple scripts or CLI Configlets at the same time.

Workaround: Use Internet Explorer Version 10.0 or later, or use a different supported browser (Mozilla Firefox or Google Chrome) to import multiple scripts or CLI Configlets at the same time.

- If you access the Junos Space Platform UI in two tabs of the same browser with two different domains selected and access the same page in both tabs, the information displayed on the page is based on the latest domain selected. To view pages that are accessible only in the Global domain, ensure that you are in the Global domain in the most recent tab in which you are accessing the UI.
- If you select the Add SNMP configuration to device 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 to device 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 want to perform a global search by using partial keywords, append "*" to the search keywords.
- To perform a partial keyword search on tags on the Tags page (Administration > Tags) or the Apply Tags dialog box (right-click a device on the Device Management page and select Tag It), append * to the search keyword.
- Internet Explorer slows down because some scripts can take an excessive amount of time to run. The browser prompts you to decide whether to continue running the slow script. see <http://support.microsoft.com/kb/175500> for instructions on how 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 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).
- 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, see [Compiling SNMP MIBs](#).

- When a physical hard drive is removed from a Junos Space hardware appliance (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.

- If you clear the **Add SNMP configuration to device** check box (on the Modify Network Management Platform Settings page under Administration > Applications > Network Management Platform > Modify Application Settings) and discover devices, and subsequently select the Add SNMP configuration to device check box and resynchronize nodes (Network Monitoring > Node List > Resync Nodes), the SNMPv2 trap target is updated on the devices.
- If you discover devices with the SNMP probing enabled, the correct version of the SNMP trap target is updated on the devices for the following cases:
 - When you modify the virtual IP (VIP) address or the device management interface IP address
 - When a separate interface for device management is configured and there is a failover of the VIP node
 - When you add or delete a Fault Monitoring and Performance Monitoring (FMPM) node
 - When you discover devices when the Network Monitoring service is stopped and subsequently start the Network Monitoring service and resynchronize nodes (Network Monitoring > Node List > Resync Nodes)

In all other cases, the default SNMP trap target (SNMPv2) is updated on the devices. If needed, you can use the predefined SNMPv3 Configlets (CLI Configlets > CLI Configlets) to update the trap settings on the device.

- In Junos Space Platform Release 16.1R1, Network Monitoring supports only a single set of SNMPv3 trap parameters.
- In Junos Space Platform Release 16.1R1, you cannot modify the trap settings for the SNMPv3 manager on the Network Monitoring GUI. You can modify the trap settings manually in the

`/opt/opennms/etc/trapd-configuration.xml` file. After modifying the trap settings manually, restart the Network Monitoring service.

- With default SNMPv3 trap settings, the discovery of devices running worldwide Junos OS (wwJunos OS devices) fails as the default SNMPv3 trap settings cannot be updated to wwJunos OS devices because wwJunos OS devices do not support privacy settings.
- The setting to manage objects from all assigned domains can be enabled globally for all users by selecting the **Enable users to manage objects from all allowed domains in aggregated view** check box in the Domains section of the Modify Application Settings page (Administration > Applications > Network Management Platform > Modify Application Settings). Alternatively, you can enable the setting to manage objects from all assigned domains at the user level by selecting the **Manage objects from all assigned domains** check box on the Object Visibility tab of the Change User Settings dialog box, which appears when you click the User Settings (gear) icon on the Junos Space banner.
- The Juniper Networks Device Management Interface (DMI) schema repository (<https://xml.juniper.net/>) does not currently support IPv6. If you are running Junos Space on an IPv6 network, you can do one of the following:
 - Configure Junos Space to use both IPv4 and IPv6 addresses and download the DMI schema by using the Junos Space Platform Web GUI.
 - Download the DMI schema by using an IPv4 client and update or install the DMI schema by using the Junos Space Web GUI.
- If you are planning on expanding the disk space for nodes in a Junos Space fabric (cluster) comprising of virtual appliances, you must first expand the disk space on the VIP node and ensure that the VIP node has come up (the status of the JBoss and MySQL services must be “Up”) before initiating the disk expansion on the other nodes in the fabric. If you fail to do this, it might cause fabric instability and you might be unable to access to the Junos Space GUI.
- In a Junos Space fabric with two or more nodes configured with both IPv4 and IPv6 addresses (dual stack), the communications between all nodes in the fabric must be enabled for both IPv4 and IPv6 addresses.
- The Network Monitoring Topology feature is not supported on Internet Explorer.
- If the network connectivity at the active disaster recovery site is down and the active site cannot connect to sufficient arbiter devices after resuming network connectivity, both sites become standby disaster recovery sites. Execute the **jmp-dr manualFailover -a** command at the VIP node of the active disaster recovery site to convert the original site to the active site and start the disaster recovery process.
- When you are discovering devices running the worldwide Junos OS (ww Junos OS devices), ensure that you wait at least 10 minutes after the Add Adapter job for the device worldwide Junos adapter has completed successfully *before* triggering the device discovery.
- A new pattern (**requested 'commit synchronize' operation**) is added to the syslog pattern in Junos Space Release 16.1R2. During the syslog registration after a device is discovered or connects back to Junos Space following a Junos Space upgrade from Release 16.1R1 to 16.1R2, the (**requested 'commit**

synchronize' operation) pattern is added to the syslog patterns on the device. When you issue the **commit synchronize** command, Junos Space automatically resynchronizes only those devices that have the **(requested 'commit synchronize' operation)** pattern added to the syslog patterns.

- If you are using Internet Explorer to access the Junos Space Network Platform UI and need to copy the job ID value from the Job ID field of the Job Management page, you must click outside the job ID text to start the selection.
- After you upgrade Junos Space Platform from Release 16.1R1 to 17.1R1, the Last Reboot Reason field on the Administration > Fabric > View Node Detail > Reboot Detail page shows the value as **Reboot from Shell/Other** instead of Space reboot after Software Upgrade.
- If the device IP could not be verified, the Add Unmanaged Devices action fails.

Known Issues

The following issues are still outstanding in Junos Space Network Management Platform Release 19.4R1.

For the most complete and latest information about known defects, use the Juniper Networks online Junos Problem Report Search application.

- Device interfaces are not displayed in Network Monitoring or OpenNMS. [\[PR1437453\]](#)
- The third-party SNMPv3 configuration of Junos Space Platform is not synchronized with the Disaster Recovery nodes. [\[PR1467634\]](#)
- PostgreSQL replication between nodes of an active site fails. [\[PR1467730\]](#)
- Junos Space constantly fails over and the corresponding custom script stops because of high memory usage. All the swap memories are used up. [\[PR1468247\]](#)
- In the CSV file, if you want to select all devices in the Platform column, device selection does not happen as expected. [\[PR1469198\]](#)
- Though the resynchronization of devices job is triggered, many devices are not listed and the inventory data shows incorrect information. [\[PR1469209\]](#)
- Dedicated database nodes do not properly disable PostgreSQL on the database nodes. [\[PR1469218\]](#)
- The standby disaster recovery site does not become an active site in case of automatic failover. [\[PR1471325\]](#)
- During manual failover for disaster recovery, the configured MySQL replication and start replication fail. [\[PR1471940\]](#)
- Graphs show data in the petabytes because the SNMP counter is reset. [\[PR1472868\]](#)

- If you add an SNMP community string on a device that includes @,\$ or & characters, and if Junos Space discovers a device using SNMP, during polling, Junos Space discards anything in the community string that comes after these characters. Therefore, the polling of information or events fail. [\[PR1474017\]](#)
- Images and scripts fail when you downgrade an MX204 platform version through Junos Space. [\[PR1474632\]](#)

Resolved Issues

This section lists the resolved issues in Junos Space Network Management Platform Release 19.4R1.

For the most complete and latest information about resolved defects, use the Juniper Networks online Junos Problem Report Search application.

- Junos Space cluster requires multicast communication even when changed to unicast mode. [\[PR1469177\]](#)
- Detailed description is required in audit logs for the apply CLI and validate CLI configlets triggered by REST APIs [\[PR1427290\]](#)
- Application settings for Junos Space Platform are locked, causing issues in the authentication mode. [\[PR1453883\]](#)
- Disk usage threshold is not applied correctly in the SNMP configuration. [\[PR1459085\]](#)
- A new certificate generate script is created to generate a valid certificate for OpenNMS. [\[PR1459168\]](#)
- If any remote database backup restoration job fails, the user interface displays only the *Remote IP is not reachable* error message. [\[PR1466858\]](#)
- The configuration file backups are large. The older versions must be either removed or cleaned up. [\[PR1469221\]](#)
- The device deletion job fails. [\[PR1469222\]](#)
- The **outbound-ssh** CLI statement was incorrectly added to all the managed devices for the dedicated database nodes. [\[PR1469233\]](#)
- Junos Space database does not synchronize correctly after Junos Space node restart or failover. [\[PR1470431\]](#), [\[PR1468108\]](#).
- Unable to select templates while deploying a Model Device. [\[PR1472754\]](#)
- Due to the security vulnerabilities reported, JDK is upgraded from 1.7 to 1.8. [\[PR1382171\]](#)
- URL is being validated in the backend to prevent any malicious attacks like trying to retrieve sensitive file information. [\[PR1449224\]](#)
- Due to the security vulnerabilities reported, JBOSS is upgraded from 6.4.17 to 6.4.22. [\[PR1449248\]](#)

Hot Patch Releases

This section describes the installation procedure and resolved issues in Junos Space Network Management Platform Release 19.4R1 hot patches.

During hot patch installation, the script performs the following operations:

- Blocks the device communication
- Stops JBoss, JBoss-dc, and watchdog services.
- Backs up existing configuration files and Enterprise Application Archive (EAR) files.
- Updates the Red Hat Package Manager (RPM) files.
- Restarts the watchdog process, which restarts JBoss and JBoss-dc services.
- Unblocks the device communication after the watchdog process is restarted for device load balancing.

NOTE: You must install the hot patch on Junos Space Network Management Platform Release 19.4R1.1 or on any previously installed hot patch. The hot patch installer backs up all the files that are modified or replaced during hot patch installation.

Installation Instructions

Perform the following steps on the CLI of the JBoss-VIP node only:

1. Download the Junos Space Platform 19.4R1 Patch vX from the [Downloads](#) site.
X is the hot patch version. For example, v1, v2, and so on.
2. Copy the Space-19.4R1-Hotpatch-vX.tgz file to the /home/admin folder of the VIP node.
3. Verify the checksum of the hot patch:
md5sum Space-19.4R1-Hotpatch-vX.tgz
4. Extract the Space-19.4R1-Hotpatch-vX tar file:
tar -zxvf Space-19.4R1-Hotpatch-vX.tgz
5. Change the directory to Space-19.4R1-Hotpatch-vX.
cd Space-19.4R1-Hotpatch-vX
6. Execute the patchme.sh script from the Space-19.4R1-Hotpatch-vX folder:

sh patchme.sh

The script detects whether the deployment is standalone deployment or a cluster deployment and installs the patch accordingly.

A marker file `/etc/.19.4R1-hotpatch-Space-vX` is created with the list of RPMs and PRs that are fixed in the hot patch release.

NOTE: We recommend that you install the latest available hot patch version, which is the cumulative patch.

Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches

Table 3 on page 24 lists the resolved issues in Junos Space Network Management Platform Release 19.4R1 hot patches.

Table 3: Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches

| PR | Description | Hot Patch Version |
|-------------------------|---|-------------------|
| 1458969 | Unable to change the policy override option (infected host) on the Juniper Sky ATP Monitoring page of Security Director. | v1 |
| 1481645 | When you try to deploy a device image from Junos Space Platform Release 19.1R1.1 to an SRX320 cluster, the deployment fails, with the Fails to execute RPC commands error message. | v1 |
| 1488363 | When you try to deploy or upgrade an EX Series or SRX Series device from Junos Space Network Management Platform, the image for the device does not appear in the drop-down list. | v1 |
| 1492286 | Deadlock error messages are found in the Junos Space message logs because of multiple automatic resynchronization operations. | v2 |

Table 3: Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches (*continued*)

| PR | Description | Hot Patch Version |
|-------------------------|---|-------------------|
| 1382491 | The Resolve Key Conflict and Modify Device Authentication jobs do not work for devices running Junos OS Release 17.3. The jobs end successfully but there is no change in the key. | v2 |
| 1408363 | If the device goes offline or comes back online, Junos Space does not update the device inventory. | v2 |
| 1477793 | You cannot deploy the MX240 device through the modeled device template from Junos Space, because of the root authentication failure error. | v2 |
| 1478923 | After successfully deleting a database backup, unable to delete other database backups from the Junos Space UI. The page keeps loading and the only option left is to navigate to another page to refresh the UI. | v2 |
| 1485443 | Jobs are failing with the Pessimistic Lock Exception error message. | v2 |
| 1496043 | When you create a security policy template using CSV files, unusable configurations are generated. | v2 |
| 1503472 | When you activate a modeled device using the manual update option, the Activate Modeled Device job gets stuck at 80%. | v2 |
| 1508269 | From the Junos Space Platform UI, if you try to connect to a modeled device using SSH, an Invalid request error message is displayed. | v2 |

Table 3: Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches (*continued*)

| PR | Description | Hot Patch Version |
|-------------------------|---|-------------------|
| 1482133 | Multiple vulnerabilities have been resolved in the Junos Space and Junos Space Security Director 20.1R1 release by updating third party software included with Junos Space and Junos Space Security Director or by fixing vulnerabilities found during internal testing. Refer to https://kb.juniper.net/JSA11023 for more information. | v3 |
| 1482255 | Multiple vulnerabilities have been resolved in the Junos Space and Junos Space Security Director 20.1R1 release by updating third party software included with Junos Space and Junos Space Security Director or by fixing vulnerabilities found during internal testing. Refer to https://kb.juniper.net/JSA11023 for more information. | v3 |
| 1482261 | Multiple vulnerabilities have been resolved in the Junos Space and Junos Space Security Director 20.1R1 release by updating third party software included with Junos Space and Junos Space Security Director or by fixing vulnerabilities found during internal testing. Refer to https://kb.juniper.net/JSA11023 for more information. | v3 |

Table 3: Resolved Issues in Junos Space Network Management Platform Release 19.4R1 Hot Patches (*continued*)

| PR | Description | Hot Patch Version |
|-------------------------|---|-------------------|
| 1482263 | Multiple vulnerabilities have been resolved in the Junos Space and Junos Space Security Director 20.1R1 release by updating third party software included with Junos Space and Junos Space Security Director or by fixing vulnerabilities found during internal testing. Refer to https://kb.juniper.net/JSA11023 for more information. | v3 |
| 1638525 | Image upload fails with Software validation failure, check certificate keys message in Network Director. | v4 |

NOTE: If the hot patch contains a user interface fix, you must clear the Web browser's cache for the latest changes to take effect.

Documentation Updates

This section lists the errata and changes in Junos Space Network Management Platform Release 19.4R1 documentation:

- From Junos Space Platform Release 16.1, the *Frequently Asked Questions* are migrated to [FAQ: Junos Space Network Management Platform](#) on the [Juniper Networks TechWiki](#) and are not available on the [TechLibrary](#).

The *Complete Software Guide* no longer contains the *Frequently Asked Questions*.

Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: <http://prsearch.juniper.net>.

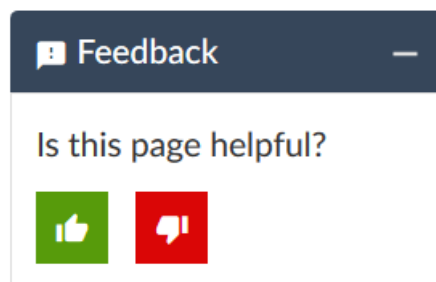
Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <http://pathfinder.juniper.net/feature-explorer/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://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: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
<https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- 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
<https://support.juniper.net/support/requesting-support/>.

Revision History

18 December, 2019—Revision 1—Junos Space Network Management Platform Release 19.4R1.

17 January 2020—Revision 2—Junos Space Network Management Platform Release 19.4R1.

22 January 2020—Revision 3—Junos Space Network Management Platform Release 19.4R1.

27 January 2020—Revision 4—Junos Space Network Management Platform Release 19.4R1.

Copyright © 2022 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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.