

Junos Space 11.4 Release Notes

Release Notes

Contents

Network Application Platform	3
Supported Junos Space Applications	3
Supported Devices	3
New Features	3
Operational Notes	4
Known Issues	5
Resolved Issues	6
Security Design	8
Supported Devices	8
Supported OS Versions	8
Supported Browsers	9
Management Scalability	9
New Features	9
Known Issues	10
Network Activate Release Notes, Release 11.4	10
New Features for Network Activate in Release 11.4	10
Supported Platforms for Network Activate in Release 11.4	11
Supported Standards, RFCs, and MIBs	11
Upgrade and Installation Instructions for Network Activate, Release 11.4	11
Known Issues and Caveats for Network Activate in Release 11.4	12
Transport Activate Release Notes, Release 11.4	12
New Features for Transport Activate in Release 11.4	12
Supported Platforms for Transport Activate in Release 11.4	12
Supported Standards, RFCs, and MIBs	12
Upgrade and Installation Instructions for Transport Activate in Release 11.4	12
Known Issues and Caveats	13
Sync Manager Release Notes, Release 11.4	13
New Features in Sync Manager, Release 11.4	13
Supported Platforms for Sync Manager, Release 11.4	14
Supported Standards, RFCs, and MIBs	14
Installation Instructions	14
Known Issues and Caveats	15

QoS Design Release Notes, Release 11.4	15
QoS Design New Features	15
Supported Platforms in QoS, Release 11.4	15
Upgrade and Installation Instructions for QoS, Release 11.4	15
Known Issues and Caveats	16
Service Now	17
New Features	17
Operational Recommendation	17
Known Issues	17
Resolved Issues	18
Service Insight	18
New Features	18
Ethernet Design	18
New Features	18
Known Issues	18
Junos Space Virtual Control	19
Operational Notes	19
Resolved Issues	19
Known Issues	20
Hardware Support	20
Junos OS Compatibility	20
Troubleshooting Junos Space	23
Junos Space Technical Publications	23

Network Application Platform

The Junos Space Network Application Platform provides the essential tools the network administrator needs for automating network operations, including device discovery and management, deploying device images and scripts, network monitoring, job operation management, user account management, audit logging, and network administration. Network administration tasks include managing the Junos Space fabric (comprising one or more IP-connected nodes), databases, licenses, applications, authorization servers, tags, permission labels, DMI schemas, and troubleshooting.

Supported Junos Space Applications

Service Now 11.4
Service Insight 11.4
Ethernet Design 11.4
Security Design 11.4
Virtual Control 11.3 and 11.4
Network Activate 11.4
Quality of Service 11.4
Transport Activate 11.4

Supported Devices

New with 11.4, Junos Space supports the following platforms running Junos software:

- EX8200 VC
- MX10

New Features

The Junos Space Network Application Platform includes the following new features:

- Image management: an operations workflow that ties images and scripts into bundles for efficient use and reuse.
- Licensing: an embedded LMS system
- Changes in network configuration are reflected in Junos Space applications, i.e. visible through Ethernet Design, for example
- Service level fault management
- Users can upload device network name and credentials via CSV file
- Lightweight logging: Release Candidate Test, with support for single node 11.4 only. Disabled by default

- Hierarchical tagging: multiple tags available for assignment, multiple levels of hierarchy within tags
- Tree view on inventory landing pages: elements organized hierarchically; tree view on left is independent of view on right
- Ability to 'cut through' to Web UIs on devices
- Access Control: increased granularity of user access control through specification of the parts (objects) in Junos Space users can access
- RCT to FRS upgrade now possible
- MIBs included: traps for all devices can now be received

Operational Notes



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

- When Junos Space Platform is upgraded to 11.4 with fault and performance features, devices under management will be configured to send SNMP traps to Junos Space. This will trigger a commit on devices.
- The Script Manager supports only Junos version 10.x and later.
- Navigating through Junos Space Platform is slow when using IE7, due to browser limitations. We recommend using IE 8 instead.
- The supported Network Activate version with Network Application Platform 11.4 is 11.4. Even though NA 11.3 is not supported with Platform 11.4, the NA 11.3 application is not disabled when Platform is upgraded to 11.4. Those running NA 11.3 and Platform 11.3 are advised to upgrade only when NA 11.4 is available, later in January 2012. At that time both Platform and NA can be upgraded together to 11.4 versions.
- Before you upgrade your current Space installation to version 11.4, it is recommended that you ensure that all your devices that are Up are In Sync before proceeding with the upgrade. If any device comes up as Sync Failed after upgrade then a manual Resync operation should bring the device back In Sync.
- Unified ISSU support for both device-initiated and Space-initiated Dual RE connections — It is strongly recommended that you configure the Virtual IP on the Dual RE device. Dual RE device without VIP configuration is not yet fully supported on Junos Space.
- Fault Manager does not support High Availability.
- On an 11.2R1.4->11.4R1 upgraded setup, Network Monitor failed to update the SNMP settings for the devices discovered before upgrade. It updated for the newly discovered devices. The workaround for this is to configure the SNMP string through the Network Monitor UI.

- After doing a Schema Overwrite, newly added schema knobs (configuration options) might not be searchable in Configuration Editor and while creating Template Definitions.
- To enable the logging feature in Space, go to the Space CLI and run this command:

```
bash /usr/local/slogs/bin/configure-env.sh true < IP Address> 1 0
```

where <IP Address> should be replaced with the Node IP address of your Space server (eth0 IP address).

To start devices pushing syslog events to the Space server, there are two options. Use either of the following:

- Use the predefined template that comes with Space (Space_Syslog_J_M MX T TX) and push it to the devices.
- Manually login to each device and configure syslog host to be the IP address of the Space server.



NOTE: The logging feature is RCT-quality, and for Single Node 11.4 Setup only.

Known Issues

The Network Application Platform 11.4 release includes the following known issues:

- Topology visualization has been removed.
- On the Schema Update page, the correct URL for the SVN repository is <https://xml.juniper.net/dmi/repository/trunk>. When entering this URL, do not include any leading or trailing spaces, as they are not correctly parsed. [PR-773679]
- In the Device Images and Scripts workspace, even if you select the option “Remove the package after successful installation,” the system does not remove the package file after installation [PR-718647]
- Stage device script/image fails for JUNOS 9.x devices [PR-717812]
- Modify button is not disabled under device credentials for CSV upload [PR-722042]
- When a 2-node Space fabric was upgraded from 11.2 to 11.4, it was intermittently observed that Device Discovery could not be launched. The error message displayed was: “Service Not Available, please try later”. The issue is attributed to collision of persisting schemas from two nodes. The work-around is to restart Jboss on both fabric nodes [PR 721366]
- Junos Space Platform Script Import fails on op-script when single-quotes are used. The workaround is to use double quotes in the script [PR-719988]
- Image and Script Management – Stage device image/script option works only for Junos 10.x and above [PR-717812]
- The EX 6200 icon may intermittently appear as an EX-VC icon [PR-719232]

- Image management: Selecting the checkbox "Remove the package after successful installation" does not delete the package after installation [PR-718647]
- Sometime Screen OS device fails to re-sync when discover via hostname [PR-712002]
- There is a remote chance of Configuration Template definitions / templates not loading after Space upgrade from 11.2 to 11.4. It is advisable to export the definitions prior to upgrade and import after upgrade. [PR-690376]
- For a Junos Space initiated connection, the Platform > Manage Devices inventory page fails to switch to the new master Routing Engine on the dual Routing Engine on a JUNOS OS device. [PR 563648]
- Image Management: sometimes upload of large device images fails. The work-around is to retry the upload. [PR 579915]
- The scope of Object Level Access Control is to filter the object visibility in the corresponding Object's Inventory Landing Page (ILP) only. [PR 688907]
- Junos Space server goes to start mode when uninstalling the Fault Management application on a single node setup [PR 613189]
- Fault Manager: Fault Manager's Add Application job takes approximately one hour per node to complete. [PR 658912]
- Old SNMP trap targets are not removed from the device when the network settings on the Junos Space appliance are modified. [PR 689042]
- The Disable Users' action does not take effect immediately (multiple node fabric issue). [PR 675694]
- In a multi (three) node fabric, on modifying the network settings, only the IP address of node-1 is removed from the devices. [PR 680435]
- In a multi-node Space fabric, modifying user information from the Manage Users page will not trigger re-authentication of users connected to other nodes. [PR-658923]
- Enable/Disable User will cause re-authorization for all users. [PR 687228]
- Device reboot may trigger additional resyncs in Junos Space initiated connection scenarios, because Junos Space receives syslogs similar to FPC/PIC insertion, thus triggering resyncs. [PR 595664]

Resolved Issues

- SRX 5k devices cannot be discovered and managed by Space [PR-705485]
- Incorrect template config generated for device specific value with choice node [PR-695102]
- Due to openNMS continuous re-sync for devices where seen [PR-694198]
- No support for dot1x config through Space templates [PR-688691]
- Right click on Service Now Incident work space is extremely slow [PR-694801]
- Copying and deploying JUNOS images on a single device through Space image management takes more than 20 minutes [PR-685786]

- Device status poller dies and marks device status as down, but device status shows in sync [PR-701717]
- Not configuring many parameters while Nat/Policy publish with platform patch 11.3p2.1 [PR-706787]
- Jobs for application CEMS is getting disabled after reboot of fabric nodes [PR-693662]
- CEMS Edit config generation issue [PR-698746]
- Update failed on a SRX cluster with Statement not found error [PR-700532]
- Deleting a device from Space does not delete the SNMP target CLI from the device [PR-698688]
- Deleting a device from Space does not always delete the device from the Network Monitoring workspace [PR-698696]
- Configuration Templates for EX devices that contain dot1x parameters do not get pushed to the devices. [PR-688691]
- Object Level Access Control is not applicable for SLP pages, it will display all the objects in the charts. [PR 687203]
- Wildcard characters are not saved with configuration templates. [PR 686313]
- When the Fault Management application is installed on the Junos Space appliance configured with device management interface, eth3 interface ip should be used as the SNMP target on the device but it is currently sending incorrect eth0 IP. [PR 689016]
- When you launch resync jobs on a large number of devices simultaneously, paging in the Manage Devices inventory page may not function properly. [PR 586001]
- When you delete a load balancer node from the fabric, a busy indicator appears. As a work-around, manually refresh your Web browser. [PR 579347]
- Modifying user information from the Manage Users page will trigger re-authentication for all users even though password information is not being modified. This may cause 'Authentication Failure' for the current session and re-login is required if there is password match failure with respect to current authorization mode settings. [PR 613237]
- AI Scripts installation fails on SRX 5K devices [PR-718982]
- Impossible to restore backed up router configuration using Space [PR-717518]
- Under Image Management, the wrong device series is displayed for the LN product family [PR-717434]
- Member Name in Service Now does not accept space, hyphen or underscore character [PR-717253]
- Device Discovery fails when trying to probe using SNMPv3 [PR-704618]
- Documentation contains references to carousel [PR-700684]
- Space UI shows license as 'demo' once a valid organization has been added under Service Now. [PR-697432]

- Not to enforce 'commit synchronise' on device during device discovery through [PR-697425]
- EX3200/4200 JLoader bootstrap image gets classified incorrectly as "M or MX or T" Series under image management [PR-692967]
- Unclear documentation about device specific CSV files and deploy error on particular fields [PR-681221]

Related Documentation

- Junos Space Frequently Asked Questions

Security Design

Junos Space Security Design application is a powerful but easy-to-use solution that allows you to create and publish firewall policies, IPSec VPNs, NAT policies, IPS policies and AppFirewall to provide appropriate security on the network. You would need to procure an IPS license to be able to push IPS signatures and App Firewall signatures to a device.

Supported Devices

Junos Space Security Design 11.4 is supported on the following SRX hardware devices:

- SRX 100
- SRX110
- SRX210
- SRX220
- SRX240
- SRX650
- SRX1400
- SRX 3400
- SRX 3600
- SRX 5600
- SRX 5800

Supported OS Versions

Junos Space Security Design 11.4 is supported on SRX OS version 10.3 and above.

SRX OS version 11.4 is needed to turn on full AppFW feature support. Also on the Junos Space side you would need to upgrade to 11.4 schema file manually and set 11.4 schema to default for junos-es device family to avail AppFW and template based custom object support.

Supported Browsers

Junos Space Security Design 11.4 is best viewed on Mozilla Firefox 4.0 and Internet Explorer 8.0.

Management Scalability

Junos Space Security Design 11.4 is designed to support management of large scale security deployments. Security Design 11.4 was tested to manage 4,000 devices, 20,000 address objects, and 10,000 rules with rule groups of 500 rules.

New Features

Junos Space Security Design 11.4 application presents the following new features:

- **Firewall Policies**— Allows you to create and update firewall policies on SRX devices and SRX device clusters. You can create two types of policies - Group policy and Device policy and add different type of rules for these policies. You can also group the rules based on your preference.
- **IPsec VPNs**— Allows you to create Site to Site, Hub And Spoke, and Full Mesh IPsec VPNs and update the VPN configurations on SRX devices and SRX device clusters. You can configure the tunnel settings, endpoint settings, and routing settings using an intuitive VPN creation workflow. You can also preview and validate these settings before saving the VPN configuration.
- **NAT Policies**— Allows you to create and update NAT policies on SRX devices and device clusters. You can create two types of NAT policies - Group policy and Device policy and add different type of rules for these NAT policies. You can also group the rules based on your preference.
- **Object Builder**— An exclusive workspace that allows you to create sub-configuration objects which can be used across multiple firewall policy, NAT policy, and VPN configurations. You can create and manage address objects, service objects, application signatures, NAT pools, VPN profiles, Policy profiles, Template definitions, Templates and Polymorphic variables using this workspace.
- **Templates**— Allows you to create custom objects that support SRX device features such as Scheduler and UTM. You can apply templates to a policy either at the policy level or at the rule level. If a rule in a policy used a template, then it takes precedence than the templates used for the policy.
- **VPN Profiles**— Allows you to export define the VPN proposals, IKE settings, and IPsec settings. VPN profiles are stored in the Junos Space database and can be re-used to create multiple IPsec settings.
- **Export Policies**— Allows you to export firewall policies and NAT policies to HTML format.
- **Signature Management**— Allows you to download, install, view, and filter App signatures and IPS signatures. You can create application signatures/groups, IPS signatures/groups, and IPS signature-sets from the downloaded and installed

signatures. You can also create static Application signature groups (Static) and both static and dynamic IPS signature groups.

- **App Firewall and IPS Integration with Firewall Policy**— Allows you to enable App Firewall and IPS for every rule in a firewall policy. You can view all the IPS policies and rules in the IPS Management workspace.

Known Issues

- Security Design 11.4 does not support concurrent firewall policy, VPN, NAT policy, and IPS changes by multiple administrators. Since locking is not performed, overlapping updates can result in the loss of changes.
- Current version of Security Design does not import existing policies, objects, VPNs from the devices.
- Clicking on the buttons on the top platform ribbon in the GUI during any changes (Policy, VPN, objects etc) will cause changes to be not saved and no warning will be displayed.
- Device to address mapping cannot be modified in a polymorphic address object.

Workaround: Delete the device to address mapping in variables; and add them again. [PR 717808]

- Wildcard address type or DNS address type objects cannot be modified once created. [PR 710403]
- “External Interface” column cannot be edited in VPN if the “Protected Networks/Zone” cell of the same row is expanded and more than one page. [PR 706402]

Recommended usage: Collapse the “Protected Networks/Zone” cell by clicking “Less” and then edit “External Interface”.

- Sometimes, switching IPS mode to none may cause device configuration update fail.

Workaround: Republish and update the configuration to device. [PR 722213]

Network Activate Release Notes, Release 11.4

Junos Space Network Activate software enables you to provision point-to-point and multipoint services across networks. You provision point-to-point services across networks that use LDP for signaling in the network core. These services use directed pseudowire virtual circuits across the network to establish point-to-point virtual private networks (VPNs). You provision multipoint services across networks that use BGP signaling in the network core. These VPLS services use route targets and route distinguishers to establish service connectivity. Network Activate software also enables you to provision Layer 3 VPN full mesh services.

New Features for Network Activate in Release 11.4

The functional audit feature for Network Activate now includes a troubleshooting function in addition to CLI verification. A functional audit determines whether a deployed service instance is functioning. It checks the control plane to ensure connectivity among endpoints

and that the UNIs are functioning correctly. It also checks the data plane to verify packet transmission between each valid pair of endpoints in the service.

The functional audit provides both a CLI verification and a troubleshooting feature that allows you to check the status of interfaces, LDP sessions, neighbor links, and endpoints of point-to-point services. The **Functional Audit** tab on the **Monitoring** window displays information about the control plane, data plane, and service statistics for the link you are monitoring. The **Troubleshooting** tab displays status of the interfaces, LDP sessions, neighbor links, and endpoints.

Supported Platforms for Network Activate in Release 11.4

- J Series, point-to-point and Layer 3 interfaces only
- M Series
- MX Series

Supported Standards, RFCs, and MIBs

None to report for this release.

Upgrade and Installation Instructions for Network Activate, Release 11.4

Prerequisites for Installation

- You must upgrade the Network Application Platform to Release 11.4 and then install the 11.4P1.3 patch before you install Network Activate 11.4.
- Network Activate, Release 11.4 must be installed before you can install other applications.

JTAC has created a KB for the patch: <http://kb.juniper.net/KB22866> Patch 11.4p1.3

In some situations a prescribed order is required for installation of Transport Activate. Use the following table to determine the order required for your installation or upgrade:

Type of Upgrade or Installation	Order of Installation Required
New Installation	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Install Network Activate, Release 11.4. 4. Install other applications from Release 11.4.
Upgrade from earlier release	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Upgrade Network Activate to Release 11.4. 4. Upgrade other applications as needed.
Uninstalling	<ol style="list-style-type: none"> 1. Uninstall other applications as needed before you uninstall Network Activate. 2. Uninstall Network Activate.

Knows Issues and Caveats for Network Activate in Release 11.4

None to report for this release.

Related Documentation

- Performing a Functional Audit

Transport Activate Release Notes, Release 11.4

Transport Activate allows you to design, provision, and deploy MPLS-dynamic, RSVP-signaled, static single-hop, and static multihop label-switched path (LSP) services that run from a specific ingress router to a specific egress router. You can configure end-to-end point-to-point and point-to-multiple-point LSPs.

Transport Activate is integrated with and codependent upon Network Activate, that provides Layer 2 and Layer 3 VPN service provisioning. Therefore, to use Transport Activate, you must install Network Activate first.

New Features for Transport Activate in Release 11.4

Static Multihop LSPs - Static multihop LSPs are now supported in Transport Activate, Release 11.4. When creating multihop LSPs you also have the option of configuring redundancy for link or node-link protection.

Supported Platforms for Transport Activate in Release 11.4

- BX7000 Multi-Access Gateway (exception: no support for static multihop LSP)
- J Series Services Routers (Exceptions: LSP is supported in Junos OS Release 9.3 only; Static LSP is not supported.)
- M Series Multiservice Edge Routers
- MX Series 3D Universal Edge Routers

Supported Standards, RFCs, and MIBs

None to report for this release.

Upgrade and Installation Instructions for Transport Activate in Release 11.4

Prerequisites for Installation

- You must upgrade the Network Application Platform to Release 11.4 and then install the 11.4P1.3 patch before you install Network Activate 11.4.
- Network Activate, Release 11.4 must be installed before you can install QoS Design.

JTAC has created a KB for the patch: <http://kb.juniper.net/KB22866> Patch 11.4p1.3

In some situations a prescribed order is required for installation of Transport Activate. Use the following table to determine the order required for your installation or upgrade:

Type of Upgrade or Installation	Order of Installation Required
New Installation	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Install Network Activate, Release 11.4. 4. Install Transport Activate.
Upgrade from earlier release	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Upgrade Network Activate to Release 11.4. 4. Upgrade Transport Activate.
Uninstalling	<ol style="list-style-type: none"> 1. Uninstall Transport Activate. 2. Uninstall Network Activate.
If you are uninstalling only Transport activate, perform only Step 1.	
If you are uninstalling both Transport Activate and Network Activate, perform both steps.	

Known Issues and Caveats

PR 732782 - Modification of multihop link-protected service order shows field name as Node-protection . This will be fixed in 12.1

Related Documentation

- [Creating a Multi-Hop Static LSP Definition](#)

Sync Manager Release Notes, Release 11.4

The Sync Manager application manages synchronization devices or subsystems which support the IEEE 1588-2008 standard, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*, commonly known as Precision Time Protocol, or PTP. The application manages Juniper devices such as Juniper's TCA Series Timing Appliances as well as synchronization subsystems within other Juniper devices.

New Features in Sync Manager, Release 11.4

This first release of the Sync Manager application provides capabilities for managing PTP devices. Users can create timing domains, add synchronization devices or subsystems to a domain, and then apply a specific service template to each domain. Sync Manager performs configuration operations on each device in the timing domain based on the service template, thus automating and greatly simplifying the configuration process.

Supported Platforms for Sync Manager, Release 11.4

- TCA Series Timing Appliances
 - TCA6000 line
 - TCA8000 line

Supported Standards, RFCs, and MIBs

Sync Manager supports the following standards:

- IEEE 1588-2008 standard, *Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*.

Installation Instructions

Prerequisites for Installation of Sync Manager

- The TCA adapter should be installed and running.
- TCA schemas must be uploaded before TCA devices can be discovered.
- You must upgrade the Network Application Platform to Release 11.4 and then install the 11.4P1.3 patch before you install Network Activate 11.4.
- Network Activate, Release 11.4 must be installed before you can install Sync Manager.

JTAC has created a KB article for the patch: <http://kb.juniper.net/KB22866> Patch 11.4p1.3

In some situations a prescribed order is required for installation of Sync Manager. Use the following table to determine the order required for your installation or upgrade:

Type of Upgrade or Installation	Order of Installation Required
New Installation	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Install Network Activate, Release 11.4. 4. Install Sync Manager.
Upgrade from earlier release	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Upgrade Network Activate to Release 11.4. 4. Upgrade Sync Manager.
Uninstalling	<ol style="list-style-type: none"> 1. Uninstall Sync Manager.
If you are uninstalling only Sync Manager, perform only Step 1.	<ol style="list-style-type: none"> 2. Network Activate.
If you are uninstalling both Sync Manager and Network Activate, perform both steps.	

Known Issues and Caveats

The following known behaviors might occur in Sync Manager. Both behaviors are rare and have not been reproducible for resolution.,

- Timing Devices might not appear in the list of managed devices even though they were of successfully discovered. This might happen if the TCA Adapter service is not running properly

Workaround: Restart Junos Space and Jboss.

- When a device is down, its IP address can be reset by Junos Space to the internal IP address of 127.0.0.1, making the device unreachable.

This behavior occurs when devices are down. There is no workaround except to delete the device and re-add the same.

Related • [Sync Manager](#)
Documentation

QoS Design Release Notes, Release 11.4

The QoS Design application allows you to configure Quality of Service (QoS) features to provide improved service to certain network traffic on Ethernet services. Enabling QoS on an Ethernet service can improve network service by providing dedicated bandwidth, setting traffic priorities across the network, improving loss characteristics, shaping network traffic, and managing network congestion.

Create a QoS profile to configure classification and policing for UNI ingress traffic and policing, scheduling and shaping for UNI egress traffic on Ethernet services. The QoS Design application lets you to define levels of service that you can then apply to Ethernet services in the Network Activate application:

QoS Design New Features

QoS Design now supports the MX80 3D Universal Edge Router.

Supported Platforms in QoS, Release 11.4

- M Series Multiservice Edge Routers
- MX Series 3D Universal Edge Routers

Upgrade and Installation Instructions for QoS, Release 11.4

Prerequisites for Installation -

- You must upgrade the Network Application Platform to Release 11.4 and then install the 11.4P1.3 patch before you install Network Activate 11.4.
- Network Activate, Release 11.4 must be installed before you can install QoS Design.

JTAC has created a KB for the patch: <http://kb.juniper.net/KB22866> Patch 11.4p1.3

In some situations a prescribed order is required for installation of QoS Design. Use the following table to determine the order required for your installation or upgrade:

Type of Upgrade or Installation	Order of Installation Required
New Installation	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Install Network Activate, Release 11.4. 4. Install QoS Design 11.4.
Upgrade from earlier release	<ol style="list-style-type: none"> 1. Install Network Application Platform, Release 11.4. 2. Install the 11.4P1.3 patch to The Network Application Platform. 3. Upgrade Network Activate to Release 11.4. 4. Upgrade QoS Design.
Uninstalling	<ol style="list-style-type: none"> 1. Uninstall QoS. 2. Network Activate. The order of uninstalling these to applications is flexible. If QoS is uninstalled, you must also uninstall Network Activate.
<p>NOTE: If you are uninstalling only QoS, perform Step 1.</p> <p>If you are also uninstalling Network Activate, perform Step 2.</p>	

Known Issues and Caveats

The following PRs have been fixed for QoS Design in Release 11.4:

- PR 712245: Unable to deploy point-to-point or VPLS services
- PR 698665: Domain discovery is not working on QoS version 11.2
- PR 707581: Unable to view QoS domain details

Known Issues

PR 565752 - Create scheduler issue

There is a Create scheduler issue when you deselect a class of service. If you clear the check box for some CoS rows and then edit one or more selected CoS rows, then click OK; the edited CoS rows that you configured are preserved. However, the CoS rows that were cleared before you clicked OK are automatically selected again. As a workaround, clear the check box for each CoS row that was automatically selected and then click Create. Only the CoS rows you intentionally selected are saved for the QoS scheduler.

Related Documentation

- [QoS Design](#)

Service Now

The Junos Space Service Now application streamlines fault management for JUNOS devices by automating the detection, isolation and resolution of network faults and incidents.

New Features

The Junos Space Service Now application presents the following new features:

- **Create on-demand incidents**—You can now create Juniper Message Bundles (JMBs) for specific devices without having to wait for an event to trigger an incident. These JMBs are called on-demand incidents. When you submit an on-demand incident, Service Now calls a pre-defined on-demand incident profile which triggers an event and generates the incident.
- **Offline activation and registration**—You can now accept a license file and activate the Junos Space Platform and Service Now application without having to connect to the Juniper Support Service (JSS). In the offline mode, you can perform all Service Now tasks except submit cases, create auto submit policies, view exposure, or view cases in case manager.
- **Support for QFX3000 Switches**—You can now use Service Now to install and manage AI-Scripts on a Juniper Networks QFX3000 switch.
- **RESTful API to install event profiles**—Service Now provides you with a Software Development Kit (SDK) that enables you to automatically install event profiles.

Operational Recommendation

- When you upgrade Service Now operating in end-customer or partner proxy mode, ensure that the Service Now partner proxy is of the same version as its end-customer Service Now applications or up to 2 versions higher than the versions of the end-customer Service Now applications that it connects to.
- Read the KB article, <http://kb.juniper.net/KB19155>, before installing AI scripts on devices.

Known Issues

- Service Now does not support JMB processing for dual Routing Engine virtual chassis devices. [PR 614683]
- The status of a technical support case is not updated when the case is associated to a site ID that is not present in Service Now. [PR 575240]
- Service Now does not receive device configuration information (JMBs) from devices running Junos OS 11.2, which have AI-Scripts Install-Package Release 2.1R1 to 2.6R2 installed.

Workaround: Use AI-Scripts Install-Package Release 2.6R2.1 or later. [PR 584236]

- Junos OS devices may not provide specific time zones for incidents, and hence Service Now may display an incorrect time of occurrence for incidents. For example, when the

time zone is EST, Service Now uses US EST by default, while the time zone can also be AEST (Australian EST). [PR 544087]

Workaround: See [Setting a Custom Time Zone on Routers Running JUNOS Software](#) for information on how to configure a custom time zone.

- The connection between the Service Now partner proxy and its end customers fails when a user changes the IP address of a Service Now partner proxy.

Workaround: Manually update the IP address of the Service Now partner proxy in your Service Now application. [PR 564827]

- Service Now cannot uninstall AI-Scripts from the back up RE of a device with dual REs. [PR 555657]

Resolved Issues

- You cannot use Service Now to install AI-Script bundles in a mixed EX4200 and EX4500 Virtual Chassis because, unlike other Junos OS devices, this device does not support the remote procedure call (RPC). [PR 719005]

Service Insight

The Junos Space Service Insight application accelerates operational analysis and manages exposure to known issues.

New Features

This release of the Junos Space Service Insight application has no new features:

Ethernet Design

The Junos Space Ethernet Design application provides you with a workflow enabling you to simultaneously configure and manage multiple Junos devices within a network.

New Features

The Junos Space Ethernet Design application presents the following new feature:

- **Support for EX Series Switches**—Ethernet Design additionally provides support for the following EX Series switches: EX2200-C, EX3300 (standalone and Virtual Chassis), EX4200 (standalone and Virtual Chassis), EX4500 (standalone and Virtual Chassis), Mixed Mode Virtual Chassis (EX4200 and EX4500), EX6200, and EX8200 (standalone and Virtual Chassis).

Known Issues

- Provisioned Native and VoIP VLANs are not listed in the **Port Configurations Parameters** dialog box when you try to reconfigure a port. These provisioned VLANs are also not displayed on the **View Port Associations** page. This issue occurs in VLAN-port associations created in Junos Space prior to the 11.1 Release. [PR 576159]

- When a user modifies and reapplies a customized port profile that is already provisioned to a port, Ethernet Design application might throw an exception. [PR 719537]

Junos Space Virtual Control

Operational Notes

- P+V orchestration support requires Junos OS Release 10.1R1 or a later release.
- Private VLAN orchestration support requires Junos OS Release 10.4R1 or a later release.
- Junos Space Virtual Control has been qualified with EX4200, EX4500, EX8200, QFX3500 series of switches, and the QFX3000 QFabric switch.
- Junos Space Virtual Control has been qualified with VMWare vSphere 4.0 and 4.1.
- Before starting P+V Orchestration, ensure that no other session (CLI or Web) is in Edit mode on the physical switches. Another session in Edit mode holds up the orchestration operation until the session is completed.
- When you upgrade to Junos Space Virtual Control Release 11.3 from Release 2.0 or Release 11.1, all information about switch-port association is lost during the upgrade. The workaround is to note down all of the associations in the earlier version before the upgrade, and re-associate them either manually or using a CSV file import, after upgrading to Junos Space Virtual Control Release 11.4. This issue does not arise when you upgrade from Junos Space Virtual Control Release 11.2 or 11.3 to Release 11.4.

Resolved Issues

The following issues have been resolved in Junos Space Virtual Control Release 11.4

- Discovery of a vNetwork fails if the password for the vNetwork contains any of the following characters: &, <, >, ' , or " , which are reserved characters in XML. We recommend avoiding the use of these characters in vNetwork passwords [PR/ 691424: This issue is resolved.]
- The online help for **Managing Uplink Port Groups** is not available from the application. This information is, however, available in the user documentation. [PR/ 692785: This issue is resolved.]
- When a distributed virtual switch (DVS) is removed immediately after a Host – vSwitch association is removed, the re-sync operation may fail. This is due to the order in which VMWare sends out event notification to Junos space Virtual Control. [PR/ 701428: This issue is resolved.]
- When a vSwitch is created, modified or deleted, a pop-up message should display the respective Job ID that links to Job Manager. This is a usability enhancement. [PR/ 672712: This issue is resolved.]
- In the **Teaming and Failover** screen for a port group that belongs to a DVS, when a dvUplink is selected and moved, the active item is not shown beyond the current scrolling area of the list box. This is a minor usability issue that occurs only if many dvUplinks are listed under the DVS. [PR/ 672714: This issue is resolved.]

Known Issues

- The MAC address of a virtual machine associated with a VSS port group may not be properly reflected in Junos Space Virtual Control. This is due to a limitation with VMWare APIs. Alternatively, you can look up the required MAC address details in the VMWare vCenter. [PR/ 661777]
- When you rename a standalone vSwitch port group in the VMWare vSphere client, it automatically creates a new port group profile and associates it with the port group in Junos Space Virtual Control. This is a limitation of the VMWare APIs. We recommend modifying standalone vSwitch port groups from Junos Space Virtual Control instead of doing that from the VMWare vSphere client [PR/ 661787]
- When the DHCP server in the VMWare vCenter assigns an IP address to a virtual machine, the IP address may not be dynamically updated in Junos Space Virtual Control. This is due to a limitation with VMWare event notifications. The IP address information is reflected in Junos Space Virtual Control after a manual (or scheduled) re-synchronization is completed. [PR/ 661790]
- When you power off a virtual machine comprising five or more network adapters that are associated with a port group of ephemeral binding type and a rename event is triggered off from the VMWare vCenter, Junos Space Virtual Control does not receive notification of the deleted ports. This is due to a limitation with VMWare event notifications [PR/ 672702].

Hardware Support

The Junos Space software supports all platforms in the following product series. For the latest platform support, see the Junos Space Platform and application data sheets.

- MX Series devices
- M Series devices
- T Series devices
- J Series devices
- EX Series devices
- SRX devices
- QFX devices
- BX devices

Junos OS Compatibility

- Specific Junos releases and versions that fully support Junos Space 11.4 Ethernet Design are limited to the following:
 - Junos OS Release 9.6
 - Junos OS Release 10.0

- Junos OS Release 10.1
- Junos OS Release 10.2
- Junos OS Release 10.3
- Junos OS Release 10.4
- Junos OS Release 11.1
- Junos OS Release 11.2
- Junos OS Release 11.3
- Junos OS Release 11.4
- Specific Junos OS releases and versions that fully support Junos Space Network Application Platform 11.4 are limited to the following:
 - Junos OS Release 9.3
 - Junos OS Release 9.4
 - Junos OS Release 9.5
 - Junos OS Release 9.6
 - Junos OS Release 10.0
 - Junos OS Release 10.1
 - Junos OS Release 10.2
 - Junos OS Release 10.3
 - Junos OS Release 10.4
 - Junos OS Release 11.1
 - Junos OS Release 11.2
 - Junos OS Release 11.3
 - Junos OS Release 11.4
- Specific Junos OS releases and versions that fully support Junos Space 11.4 Network Activate are limited to the following:
 - Junos OS Release 9.3
 - Junos OS Release 9.4
 - Junos OS Release 9.5
 - Junos OS Release 9.6
 - Junos OS Release 10.0

- Junos OS Release 10.1
- Junos OS Release 10.2
- Junos OS Release 10.2
- Junos OS Release 10.3
- Junos OS Release 10.4
- Junos OS Release 11.1
- Junos OS Release 11.2
- Junos OS Release 11.3
- Junos OS Release 11.4
- Specific Junos OS releases and versions that fully support Junos Space 11.4 QoS Design are limited to the following:
 - Junos OS Release 9.3
 - Junos OS Release 9.4
 - Junos OS Release 9.5
 - Junos OS Release 9.6
 - Junos OS Release 10.0
 - Junos OS Release 10.1
 - Junos OS Release 10.2
 - Junos OS Release 10.2
 - Junos OS Release 10.3
 - Junos OS Release 10.4
 - Junos OS Release 11.1
 - Junos OS Release 11.2
 - Junos OS Release 11.3
 - Junos OS Release 11.4
- Specific Junos OS releases and versions that fully support Junos Space 11.4 Security Design are limited to the following:
 - Junos OS Release 10.2
 - Junos OS Release 10.3
 - Junos OS Release 10.4

- Junos OS Release 11.1
- Junos OS Release 11.2
- Junos OS Release 11.3
- Junos OS Release 11.4
- Specific Junos releases and versions that fully support Junos Space 11.4 Service Now are limited to the following:
 - Junos Release 9.0 and later
- Specific Junos OS releases and versions that fully support Junos Space 11.4 Transport Activate are limited to the following:
 - Junos OS Release 9.3
 - Junos OS Release 9.4
 - Junos OS Release 9.5
 - Junos OS Release 9.6
 - Junos OS Release 10.0
 - Junos OS Release 10.1
 - Junos OS Release 10.2
 - Junos OS Release 10.2
 - Junos OS Release 10.3
 - Junos OS Release 10.4
 - Junos OS Release 11.1
 - Junos OS Release 11.2
 - Junos OS Release 11.3
 - Junos OS Release 11.4

Troubleshooting Junos Space

For information about troubleshooting Junos Space, see:

http://www.juniper.net/techpubs/en_US/junos-space11.1/topics/concept/junos-space-troubleshoot-overview.html

Junos Space Technical Publications

Junos Space technical documentation is available as online help in the graphical user interface and on the Web in HTML and PDF file formats. The Web-based documentation is maintained after the final build of the online help, therefore use it wherever discrepancies exist between the help and the Web-based documentation.