Release Notes

Published
2025-12-23

Junos OS Release 24.4R2®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall. This release notes accompany Junos OS Release 24.4R2. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can find release notes for all Junos OS releases at https://www.juniper.net/documentation/product/us/en/junos-os#cat=release_notes.

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewall, and vSRX Virtual Firewall. This release notes accompany Junos OS Release 24.4R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for ACX Series routers.

What's Changed

IN THIS SECTION

Learn about what changed in this release for ACX Series routers.

General Routing

- A new counter **Sessions hit due to high rate** is added to `show services service-sets screen-session-limit-counters` command for all subscriber traffic. This counter tracks the sessions that come up on the screen irrespective of the `alarm-without-drop` configuration. When `alarm-without-drop` option is disabled, all the counters display updated statistics. When `alarm-without-drop` is enabled, then, the screen-drop counters on `show services service-sets statistic screen-drop` command do not increase. The **sessions hit due to high rate** value is displayed.

  [See alarm-without-drop (IDS Screen Next Gen Services), show services service-sets statistic screen-drops (Next Gen Services), and show services service-sets statistic screen-session-limit-counters (Next Gen Services).

- When you run the `request vmhost zeroize` command to zeroize a single Routing Engine on a dual Routing Engine device, the CLI incorrectly displays a message indicating that it will zeroize both Routing Engines.PR1869854

- On the MPC7E-10G line card, when you configure the 10-Gigabit Ethernet ports to operate as 1-Gigabit Ethernet ports, use the speed statement at both the `[edit interfaces` *`interface name`* `gigether-options]` and `[edit interfaces` *`interface name`*`]` hierarchy levels.PR1879198

Serviceablility

- **New option for debug collector data storage path** —We've included the option outdir to specify an output directory for storing debug collector data in a customised path. This allows you to organise and access diagnostic information more efficiently, adapting storage to your specific requirements.

  [See request system debug-info]. PR1889710

User Interface and Configuration

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

[See show system storage.]

Open Issues

IN THIS SECTION

Learn about open issues in this release for ACX Series routers.

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

General Routing

- When restart chassis-control trigged on M/MX router has config with ccc instance, syslog is error out " Err] ACX_ASIC_PROGRAMMING_ERROR: pfe_dnx_translation_set: Error, bcm_vlan_port_translation_set rv:Entry not found ". PR1764966
- On ACX2200 series, ge (gigabit ethernet) interfaces configured for PTP (Precision Time Protocol), after PTP is deactivated and activated or activated for the first time, traffic can experience packet drops. PR1811850

Network Management and Monitoring

- Multiple traps are generated for single event, when more target-addresses are configed in case of INFORM async notifications Cause: INFORM type of async notification handling requires SNMP agent running on router to send a Inform-Request to the NMS and when NMS sends back a get-response PDU, this need to be handled. In this issue state, when more than one target-address(NMS IP) is configured for a SNMP v3 INFORM set of configuration, when Get-Response comes out of order in which the Inform-Request is sent, the PDU is not handled correctly causing snmp agent to

retry the Inform-request. This was shows as multiple traps at the NMS side. Work-around: For this issue would be to use 'trap' instead of 'inform' in the "set snmp v3 notify NOTIFY_NAME type inform" CLI configuration. PR1773863

Virtual Chassis

- The ACX5000 reports false parity error messages such as soc_mem_array_sbusdma_read. The ACX5000 SDK can raise false alarms for parity error messages such as soc_mem_array_sbusdma_read. This is a false positive error message. PR1276970

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for ACX Series routers.

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

General Routing

- On ACX7000 series, the DHCPv4/v6 packets might be dropped because DHCP packets are not routed to kernel after initial jdhcpd starts. PR1816246
- On ACX710 Platforms the clksyncd error is seen affecting IPC. PR1829340
- Packets are forwarded with native VLAN tagged on ACX5448 and ACX710 platforms. PR1849241
- Inner VLAN tag DEI bit in VLAN header set incorrectly. PR1850907

- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- EVPN/VPLS protocol configuration through CLI is not allowed on device. PR1852905
- Packet loss observed across multiple traffic items using SR profiles within the Layer 3 VPN. PR1853294
- Esi link state change causing bum traffic block. PR1853321
- IPv6 neighbor discovery with DHCP packet getting dropped when no-snoop option is enabled for DHCP Relay. PR1855624
- The Layer 2 and layer 3 packet loss and bulk of syslog messages reported in MPLS scenarios. PR1859990
- The rpd process crashes and asserts are seen due to memory leak. PR1868085
- Transient traffic loss for CE in an EVPN MPLS setup with Multi-Homing. PR1874476
- On ACX5448 and ACX710 series, 50 percent of packet gets lost with Explicit Null disabled for BGP-LU Labeled Routes in ECMP scenarios. PR1881742

Routing Protocols

- Disabling the PIM interface underneath the `[edit protocols pim interfaces <intf-name>]` hierarchy may still show PIM as still being UP instead of DOWN. PR1857699

Subscriber Access Management

- Error message is observed after device is restarted. PR1813456

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for ACX Series routers. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, EOL and EEOL:

- End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for thirty six months after the first general availability date and customer support for an additional six more months.

For both EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 1: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

For more information about EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for cSRX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for cSRX.

What's Changed

There are no changes in behavior and syntax in this release for cSRX.

Known Limitations

There are no known limitations in hardware or software in this release for cSRX.

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

Open Issues

There are no known issues in hardware or software in this release for cSRX.

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

Resolved Issues

There are no resolved issues in this release for cSRX.

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

Junos OS Release Notes for EX Series

IN THIS SECTION

What's New in 24.4R2-S1

IN THIS SECTION

Learn about new features introduced in this release for EX.

To view features supported on the EX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- EX4100-H-12MP
- EX4100-H Chassis
- EX4400-48MXP
- EX4400-48XP
- EX4400-24T
- EX4400-24P
- EX4400-24MP
- EX4400-24X
- EX4400-48P,
- EX4400-48F

- EX4400-48T
- EX4100-24P
- EX4100-24MP
- EX4100-24T
- EX4100-48MP
- EX4100-48P
- EX4100-48T
- EX4100-F-12P
- EX4100-F-12T
- EX4100-F-24P
- EX4100-F-24T
- EX4100-F-48P
- EX4100-F-48T
- EX4100-H-24F
- EX4100-H-24F-DC
- EX2300
- EX4650
- EX3400
- EX4300-MP
- EX4000-12MP
- EX4000-24MP
- EX4000-48MP
- EX2300
- EX2300-VC
- EX2300 Multigigabit
- EX3400

- EX3400-VC
- EX4000
- EX4100
- EX4100-F
- EX4300 Multigigabit
- EX4400
- EX4400 Multigigabit
- EX4400-24X
- EX4650-48Y
- EX9200
- EX9204
- EX9208
- EX9214

EVPN

- **VXLAN-GBP profiles with enhanced OISM in EVPN-VXLAN fabrics (EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y)**—We now support running enhanced optimized intersubnet multicast (OISM) in an EVPN-VXLAN network when you configure the `vxlan-gbp-mc-profile` VXLAN group-based policy (GBP) unified forwarding table (UFT) profile at the `[edit chassis forwarding-options]` hierarchy level.

  We don't assign GBP tags to the multicast traffic. Only unicast traffic carries GBP tags in the VXLAN headers.

  You can use enhanced OISM and VXLAN-GBP with:

  - IPv4 underlay connectivity for the EVPN-VXLAN fabric
  - Intra-VLAN (Layer 2 multicast) and inter-VLAN (Layer 3 multicast) traffic
  - IPv4 multicast traffic with IGMP and IGMP snooping

- IPv6 multicast traffic with MLD and MLD snooping

Besides configuring this profile, there are no other configuration differences for either feature when you configure them together.

[See vxlan-gbp-mc-profile, Micro and Macro Segmentation using Group Based Policy in a VXLAN, and Optimized Intersubnet Multicast in EVPN Networks.]

Services Applications

- **Flow based telemetry support for bridged traffic (EX4100, EX4100F, and EX4400)**—You now can use Flow Based Telemetry (FBT) on EX4100, EX4100F, and EX4400 switches to conduct per-flow level analytics on Layer 2 interfaces. This feature allows you to configure an inline monitoring services instance that collects and exports detailed flow information, including Layer 3 and Layer 4 attributes, to an external collector using an IPFIX template. FBT supports a range of attributes such as source and destination IP addresses, ports, and protocols, enhancing your network visibility and performance monitoring capabilities.

  [See Flow-Based Telemetry (EX4100, EX4100-F, and EX4400 Series).]

What's New

IN THIS SECTION

Learn about new features introduced in this release for EX.

To view features supported on the EX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- EX4100-H-12MP

- EX4100-H Chassis
- EX4400-48MXP
- EX4400-48XP
- EX4400-24T
- EX4400-24P
- EX4400-24MP
- EX4400-24X
- EX4400-48P,
- EX4400-48F
- EX4400-48T
- EX4100-24P
- EX4100-24MP
- EX4100-24T
- EX4100-48MP
- EX4100-48P
- EX4100-48T
- EX4100-F-12P
- EX4100-F-12T
- EX4100-F-24P
- EX4100-F-24T
- EX4100-F-48P
- EX4100-F-48T
- EX4100-H-24F
- EX4100-H-24F-DC
- EX2300
- EX4650

- EX3400
- EX4300-MP
- EX4000-12MP
- EX4000-24MP
- EX4000-48MP
- EX2300
- EX2300-VC
- EX2300 Multigigabit
- EX3400
- EX3400-VC
- EX4000
- EX4100
- EX4100-F
- EX4300 Multigigabit
- EX4400
- EX4400 Multigigabit
- EX4400-24X
- EX4650-48Y
- EX9200
- EX9204
- EX9208
- EX9214

Authentication and Access Control

- **GRES support for 802.1X protocol**—You can ensure uninterrupted traffic flow during a Routing Engine failure using Graceful Routing Engine Switchover (GRES) support for the 802.1X protocol. The feature maintains client authentication states, preventing traffic loss and MAC learning disruptions. Use the CLI command `show dot1x sync-pending-sessions` to view unsynced authenticated sessions post-

switchover and ensure proper session synchronization. This enhancement allows seamless transitions without client disconnections, ensuring continuous network access and stability. [See **Understanding Graceful Routing Engine Switchover Support for 802.1X**.]

Network Management and Monitoring

- **On-box packet sniffing support (EX4100-48MP, EX4400-48MP, EX4650, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—We've introduced on-box packet sniffing capability to monitor and analyze network traffic on ports without using an external device, such as collector or an agent.

  On-box packet sniffer allows you to monitor IPv4 packets on ingress or egress ports, matching them based on header attributes like source IP, destination IP, source MAC, destination MAC, VLAN, and VNID. You can store the sniffed packets in pcap format.

  This feature reduces costs and simplifies debugging.

  We've introduced the following configuration statements to support this feature:

  - To enable the tracing operations, configure the `set services pfe traffic traceoptions file` *`filename`* statement.
  - To increase the default timer that is set for uninstalling the filter and deleting the entries, configure the `set services pfe traffic monitor-timer` *`time`* statement.
  - To enable egress packet monitoring, configure the `set interface` *`interface-name`* `ether-options loopback` statement. You must configure an additional unused interface for a virtual loopback interface to achieve egress packet monitoring.

  Use the following commands to monitor data packets and verify the functionality of on-box packet sniffing:

  [See On-Box Packet Sniffer Overview and monitor pfe traffic interface.]

Routing Policy and Firewall Filters

- **Support for counting the number of BGP large communities (ACX Series, cRPD, EX Series, QFX series, MX Series, PTX Series, SRX Series, VRR)**—You can use `large-community-count` to count the number of BGP large communities.

  [See large-community-count.]

- **Support to configure DDoS protocol using CLI (EX3400 and EX4300-MP)**—You can configure the DDOS protocol using CLI on EX3400 and EX4300-MP devices. You can also use the following operational commands to view the DDOS protocol details:

  - `show ddos-protection protocols`

- `show ddos-protection statistics`
- `show ddos-protection protocols violations`
- `show ddos-protection protocols parameters`
- `show ddos-protection protocols statistics`
- `clear ddos-protection protocols`

[See ddos-protection (DDoS), show ddos-protection protocols, clear ddos-protection protocols, show ddos-protection statistics, show ddos-protection protocols violations, show ddos-protection protocols parameters, and show ddos-protection protocols statistics.]

- **Support added for matching ARP request packet, ARP reply packet, ARP header sender IPv4 address, or ARP header target IPv4 address (EX2300, EX3400, EX4100-48P, EX4300-MP, EX4400-24P, and EX4650)**—New ARP match conditions added - `arp-type`, `arp-sender-address`, and `arp-target-address`.

  [See Firewall Filter Match Conditions and Actions (QFX and EX Series Switches).]

- **Filter-based forwarding for GBP-tagged traffic (EX4100-48P, EX4400-48F, EX4650, and QFX5120-48T)**—This is the ability to forward traffic to a specified next hop if the GBP tags assigned to that traffic match the GBP tags specified in the filter. Use this feature to apply different routing treatment for the specified tagged traffic versus regular traffic.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

Routing Protocols

- **Supports a set of BGP self-diagnostics CLI commands (EX Series, MX Series, and SRX Series)**–A set of BGP self-diagnostics CLI commands are now available that help users to streamline the root cause of common BGP issues automatically. This includes troubleshooting commands for BGP global state overview, BGP running state warnings, BGP neighbor down and flap diagnostics, BGP CPU hogging diagnostics, BGP missing route diagnostics, and BGP dropped route diagnostics. These set of commands are available for `show bgp diagnostics` command.

  [See show-bgp-diagnostics.]

Services Applications

Software Installation and Upgrade

- **Support for SZTP (EX4100-H-12MP)**—Use RFC-8572-based secure zero-touch provisioning (SZTP) to bootstrap your remotely located network devices that are in a factory-default state. SZTP enables mutual authentication between the bootstrap server and the network device before initiating ZTP.

To enable mutual authentication, the system generates a unique digital voucher based on the Digital Device ID or Cryptographic Digital Identity (DevID) of the network device. The DevID is embedded inside Trusted Platform Module (TPM) 2.0 chip on the network device. We issue a digital voucher to customers for each eligible network device.

[See Secure Zero Touch Provisioning and Generate Secure ZTP Vouchers.]

- **Hardware root of trust, secure boot, and network boot support (EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-24P, EX4000-24T, EX4000-48P, and EX4000-48T)**—You can enhance the security of your system with the hardware root of trust (HRoT). HRoT is a hardware-based security feature that verifies the integrity of the firmware, ensuring it has not been compromised or modified without authorization. With HRoT, you establish a trusted foundation starting from the hardware, making it highly resistant to tampering and enabling a secure boot process where only verified firmware is loaded.

  Network booting (netboot), refers to the process of initiating a device's startup directly from a network source, rather than relying on local storage devices such as hard disks or USB drives. This method enables the device to load the Junos OS from a centralized server over the network.

  The platforms provide the newly introduced hardware root of trust (HRoT) support along with secure boot support to authenticate and securely verify the software and boot firmware immediately after powering on. The platforms also provide the newly introduced network boot support.

  [See Junos OS Overview and Boot EX4000 using Network Boot.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for EX Series switches.

General Routing

- **Changes to request system recover command syntax (EX Series)**--Options (all-members | local | member member-id) have been added to the request system recover command to specify the members for which the system needs to recover data.

  [See request system recover.]

User Interface and Configuration

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for EX Series switches.

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

General Routing

- Error logs are expected when routes point to the target next hop, which in turn point to hold next hops. These error logs are present for a short time. Later, when the next hop changes from a hold

next hop to valid next hop, unilist next hops will be walked again and updated with the appropriate weight and reroute counters, and no more error logs will be seen. PR1387559

- On EX2300, EX3400,EX4300-48MP and EX4300, pause frames counters does not get incremented when pause frames are sent.PR1580560
- Carrier tranistions is not setting properly for channelized ports on non-DUT EX4400-48F for QSFP28-100G-AOC-30M 740-064980 of FINISAR.PR1723924
- input-vlan-tagged-frames are not in the expected range while verifying VLAN Tagged FramesPR1749391
- Ex-Hardening:Local/Remote fault insertion from TG is failingPR1789999
- EVPN VXLAN BGP with BFD timer as 1sec (1000ms) flap when 'ethernet-switching table' is holding 10K MACs with ARP table is holding 5K MAC-IP bindings and attempted a clearing all the MAC table.PR1846781
- We cannot configure same output interface for multiple port-mirroring/analyzer instance.PR1873269

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. https://kb.juniper.net/TSB18251PR1568757

Open Issues

IN THIS SECTION

Learn about open issues in this release for EX Series switches.

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

General Routing

- On EX2300, EX3400,:EX4300-48MP and EX4300 , Pause frames counters does not get incremented when pause frames are sent.PR1580560
- EX4400-48F :: RLI-53126: Carrier tranistions is not setting properly for channelized ports on non-DUT Lagavulin for QSFP28-100G-AOC-30M 740-064980 of FINISARPR1723924
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission.PR1742565
- The interface of ge-x/0/1 port might go down after virtual-chassis split and merge on EX4300-VCPR1745855
- On all Junos and Junos evolved platforms with telemetry enabled, if the streaming server and export profile for reporting-rate are not properly configured in the analytics settings, rebooting the FPC would prevent any of the interfaces from coming up.PR1779722
- After rebooting a mixed Virtual Chassis (VC) of EX4300-xxP and EX4300-MP switches or rebooting a EX4300-xxP member, interfaces with Power over Ethernet (PoE) configured will not come up on EX4300-xxP members.PR1782445
- Ex-Hardening:Local/Remote fault insertion from TG is failingPR1789999
- If standalone device has vccpd running with configurations as per virtual chassis, then it is considered a virtual chassis and not a standalone device. All messages seen will be as per virtual chassis as well.PR1805266
- Autoneg error log observed in case of jack-out followed by jack in(JiJO) of SOURCE PHOTONICS & ACCELINK vendor 10G SFP-T industrial grade transceiver PR1815035
- Traffic loss will be seen on 1G-SFP-T if speed is configured to 100m. 1G SFP-T has the AN feature enabled but the PHY we have b/w SFP-T and switch ie., PHY82756 doesn't support AN and this mismatch is causing the traffic loss. This needs feature enhancement PR1817992
- Time Domain Reflectometry (TDR) support for detecting cable breaks and shorts aborts intermittently on some random ports.PR1820086
- On all Junos and Junos Evolved platforms, 72-byte size memory leak is seen when interface configuration is added. But there is no traffic impact due to this issue.PR1842546

- When a poe bounce command is issued in quick succession for multiple ports, the 'poe enabled' logs may not be printed for some of the poe ports. This is a cosmetic issue and functionality works as expected.PR1845161
- A memory corruption issue can result random dcpfe (dense concentrator packet forwarding engine) process crashes on specific Junos QFX and EX platforms configured with VXLAN (Virtual Extensible Local Area Network) configuration.PR1856424
- After multiple iterations of dc-pfe process restart, we may see interface with 10g-base-t transceiver (part# 740-123734) will not come up. PR1864715
- dhcp-snoop routes are not installed when IPSG group is full when IPv4/v6 source guard is enabled along with DAI/NDI. When dhcp snooping binding entries exceed 512, even new bindings show up in the binding table, the dhcp-snoop route is not installed in HW. New bindings will be dropped due to DAI/NDI. This behavior is expected. As we are running out of space of FP entries in HW, routes are NOT installed beyond the scale. IPv4 and IPv6 uses the same VFP in HW. switch> request pfe execute command "show filter hw groups" target fpc0 Unit:0 Group Information: > VFP groups: Dynamic group id: 1. Pipe: 0 Entries: 1 Total_available: 512 Pri: 0 Def Entries: 0 VFP group for COS id: 143. Pipe: 0 Entries: 7 Total_available: 512 Pri: 2 Def Entries: 0 VFP group for DYN IPSG group id: 391. Pipe: 0 Entries: 512 Total_available: 512 Pri: 3 Def Entries: 0 full group with 512 entries PR1878355
- EX4000: "ERROR: Unknown uboot version in pkg, not saved in EFI partition during Junos OS 24.4R2.25 upgrade" will be reported if any prior firmware image is not added in the device.PR1910075
- Telemetry streaming pertaining to poe functionality performed under stressed system conditions involving specific daemon start/restart scenarios may sometimes lead to chassis daemon crash.PR1909197

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. Please see KB https://kb.juniper.net/InfoCenter/index?page=content&id=KB26616 resolution rib policy is required to apply as a work-aroundPR1754351

Platform and Infrastructure

- It is noticed that EX4300 switches after an upgrade of Junos from 21.2R3-SX to 21.4R3-SX may exhibit a higher Cpu. Issue is resulting from fast path thread profiling code. It takes on an average 1 ms more for one fast path thread cycle, cumulatively overall fast path thread usage had increased. Thread profiling code has been optimised and the issue is fixed in the future JUNOS.PR1794342
- On EX4300 switches, Address Resolution Protocol (ARP) requests used for Media Access Control (MAC) learning are not handled correctly when MAC limiting features, such as the 'mac-move-limit' knob, are configured. These features change MAC learning from hardware-based to software-based.PR1873052

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for EX Series switches.

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

General Routing

- JDI_REG::QFX5200:: After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device PR1703229

- EX3400: "Error:tvp_optics_eeprom_read: Failed to read eeprom for link" syslog error message PR1757034
- Establishing virtual-chassis connection between EX4300-MP platforms, the traffic sent via the VCP port is lost minimally PR1805100
- [interfaces] EX4100-H-12MP : :: Rampur: "dc-pfe[22751]: BCM Error: API bcm_plp_mode_config_get(phy_name, plp_info, &speed, &intf_type, &r_clk, &if_mode, &aux) at tvp_bcm_mgig_phy_basic_init:433 -> -25 " Error message is seen during image upgrade PR1812228
- Packet drops when jumbo frames forwarded through ge interfaces configured for 10/100Mbps speed PR1812891
- Complete packet loss will be observed for the inter-VLAN traffic in EVPN-VXLAN CRB scenario PR1820830
- Protocol traffic drops were seen in the network for any configuration change in the protocol PR1823601
- Interface goes down after a dc-pfe (Data Centre Packet Forwarding Engine) process restart in a Virtual Chassis environment on EX4400 platform PR1823688
- The SFP 10GBASE-T part No. 740-083295 on platforms running Junos/Junos EVO is unable to detect a linkdown PR1823771
- Random ports of EX4400 will not be created on upgrade or reboot PR1825281
- On an EX4400 device with 4x25G Uplink module configured in 1GE or 25G speed, peer side of an interface with 10GBASE-T transceiver may remain up even when the IFD(xe-x/2/y) is not created PR1831409
- EX2300/EX3400 : The status LED of uplink port is not working properly PR1833177
- Continuous increment of tcpAttemptFails counter on Junos EX2300 and 3400 PR1839618
- Delay in GBP installation in an EVPN-VXLAN scenario PR1839916
- PFE process crash is observed when web-management is not configured in a CWA setup PR1840988
- TDR test can cause a CPU hog and result in BFD flaps PR1841117
- Junos OS and Junos OS Evolved: Receipt of a specifically malformed DHCP packet causes jdhcpd process to crash (CVE-2025-30648) PR1842682
- Media Access Control Security (MACsec) does not work properly after a transceiver is removed and re-inserted PR1844354

- EX4100 looses connectivity with the directly connected management port of QFX5120-48Y series platform PR1844709
- Lane laser temperature value is incorrectly displayed in the snmp query PR1844751
- The push pop function on the QFX5120 and EX4650 is not correctly pushing the VLAN PR1844853
- PEM mismatch alarms vanished after performing system reboot on member PR1845365
- Interface not added back to AE bundle with multiple changes in single commit PR1845370
- The error message will be seen on EX4100 platforms when deactivating/activating IRB interfaces PR1846286
- Memory Leak: Memory leak is detected with rpd task blocks "rpd-trace" PR1846294
- Reachability issues are seen on interfaces that are aggregated without address-family PR1847159
- Junos EX platform will display multiple intermittent Fan overspeed alarms PR1848292
- EX4400: Storm-control is created for the GE interfaces for 4x10G uplink modules. PR1848338
- IGMP snooping stops working after reboot PR1848764
- Handling AE Child Members, VT port properties reset when Access Port is destroyed PR1849952
- EX4400 uplink ports (PIC 2) with the 4x25G uplink module may go down when SFPs (SFP+-10G-BX10-D/U or SFP+-10G-BX40-D/U) are inserted. PR1849992
- EX3400 Dot1x Radius accounting send incorrect value to the server for Acct-Input-Gigawords/ Acct-Output-Gigawords PR1851299
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC PR1852019
- VoIP Phones are unable to receive an IP address with or without dot1x configuration PR1852215
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled PR1854253
- In Junos EX and QFX platforms, when ERPS protocol is enabled on a ISL trunk, the commit command fails PR1855088
- PoE ports go down when only PSU in slot 1 is connected PR1855409
- Traffic drop observed due to ECMP next-hop programming issue PR1855990
- Error logs : "PFE_BRCM_COS_HALP_ERR: BRCM_COS_HALP" are observed and CoS not working on EX2300 switches PR1856201
- Port mirroring fails due to mismatched analyzer and outgoing interface configuration PR1856361

- L2ald process crash is observed upon executing hidden command "show ethernet-switching debug-statistics fast-mac-update" in case the command doesn't have any output PR1864295
- STP/MSTP/RSTP/VSTP convergence issue due to BPDU drop by l2cpd PR1864371
- Default Route configured with Discard Next Hop on PFE instead of ECMP Next Hop after reboot PR1867562
- Traffic will be dropped due to IPv4 header checksum mismatch on EX4400 platform PR1870016
- RPD might crash when upgrading using no-validate. PR1870183
- Inserting any unsupported optics in 4x25G ULM will cause any port on the ULM to go down PR1877524

Infrastructure

- Junos OS: A local attacker with shell access can execute arbitrary code (CVE-2025-21590) PR1872010

Layer 2 Ethernet Services

- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle PR1854827
- DNS resolution will fail for DNS entries written to "resolv.conf" PR1872292
- AE member not able to discover lost LACP peer connection leading to traffic black-holing PR1874126

Platform and Infrastructure

- Traffic drops after link flap on active-active ESI setup with MAC pinning enabled PR1846365
- User root is shown as incorrect after power cycle of the device PR1855393
- STP/RSTP/MSTP/VSTP enters a disputed and blocked state when the anchor FPC of an AE link, with members distributed across multiple FPCs, goes offline PR1870522

Routing Protocols

- Memory leak is seen when BGP is activated and deactivated PR1849027
- BGP queue deadlock on Junos/Junos OS Evolved/cRPD platforms leading to route advertisement failure and traffic loss PR1860786
- Disabling the PIM interface underneath the `[edit protocols pim interfaces <intf-name>]` hierarchy may still show PIM as still being UP instead of DOWN. PR1857699

User Interface and Configuration

- Unexpected issues such as login failures or disabled interfaces observed following abrupt reboot during commit operation PR1861063
- The `show system storage` command output should show only true and distinct storages. PR1873253

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for EX Series switches. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for JRR Series

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for JRR Series Route Reflectors.

What's Changed

There are no changes in behavior and syntax in this release for JRR Series Route Reflectors.

Known Limitations

There are no known limitations in hardware or software in this release for JRR Series Route Reflectors.

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

Open Issues

There are no known issues in hardware or software in this release for JRR Series Route Reflectors.

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

Resolved Issues

There are no resolved issues in this release for JRR Series Route Reflectors.

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for the JRR Series Route Reflector. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the JRR200 Route Reflector Quick Start and Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 3: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for Juniper Secure Connect.

What's Changed

There are no changes in behavior and syntax in this release for Juniper Secure Connect.

Known Limitations

There are no known limitations in hardware or software in this release for Juniper Secure Connect.

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

Open Issues

There are no known issues in hardware or software in this release for Juniper Secure Connect.

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

Resolved Issues

There are no resolved issues in this release for Juniper Secure Connect.

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

Junos OS Release Notes for MX Series

IN THIS SECTION

What's New in 24.4R2-S1

IN THIS SECTION

Learn about new features introduced in this release for the MX Series routers.

To view features supported on the MX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- MX204
- MX240
- MX304
- MX304-LMIC
- MX480

- MX960
- MX2008
- MX2010
- MX2020
- MX10003
- MX10004
- MX10008
- MX10016

MACsec

- **Support for a custom EAPoL EtherType to improve network tunneling of MACsec packets (MX240, MX304, MX480, MX960, MX10004, and MX10008)**—MACsec uses Extensible Authentication Protocol over LAN (EAPoL) as a transport protocol to establish sessions. Some networks filter packets based on their EtherType value. By default, the EtherType for all EAPoL packets is 0x888e. To ensure the network tunnels the MACsec packets properly, you can set a custom EtherType for EAPoL packets. On interfaces where a custom EAPoL EtherType is enabled, 802.1X authentication is not supported. Features dependent on it such as dynamic connectivity association key (CAK) are also not supported.

  To configure the EAPoL EtherType, use the `ether-type` *`ether-type-value`* statement at the `[edit forwarding-options custom-eapol-ether-type-profiles` *`eapol-profile-name`*`]` hierarchy level. You must use an EtherType that isn't already reserved for another use. To apply the EtherType to MACsec packets, configure the `eapol-ethertype-profile` *`eapol-profile-name`* statement at the `[edit security macsec connectivity-association` *`ca-name`* `mka]` hierarchy level.

  To view the new EtherType profile, use the `show security mka sessions detail` command.

  [See Media Access Control Security (MACsec) over WAN.]

Routing Protocols

SUMMARY

- **Replace BGP AS path to maintain network interoperability (MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**– Define a routing policy to match and replace a list of autonomous systems (AS) numbers or private AS numbers with the local AS number of the BGP peering session to maintain network interoperability. This configuration works only on AS sequences and not on AS sets. In addition to using external BGP (EBGP), enable internal BGP (IBGP) to leverage this capability in route-reflector scenarios. Include the policy action `as-path-replace` *`as-list`* / *`private`* statement at the `[edit policy-options policy-statement` *`statement-name`* `then]` hierarchy level to activate the feature.

  [See Autonomous Systems for BGP Sessions.]

What's New

IN THIS SECTION

Learn about new features introduced in this release for the MX Series routers.

To view features supported on the MX Series platforms, view the Feature Explorer using the following links. To see which features are supported in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- MX204

- MX240
- MX304
- MX304-LMIC
- MX480
- MX960
- MX2008
- MX2010
- MX2020
- MX10003
- MX10004
- MX10008
- MX10016

Network Management and Monitoring

- **OAM on S-VLAN bidirectional state propagation (MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—We've enhanced the OAM on S-VLAN feature for bidirectional state propagation. The OAM on S-VLAN feature allows monitoring of CFM at the S-VLAN level and propagates the state to associated C-VLANs within the S-VLAN for point-to-point services. This reduces the scale of CFM monitoring by propagating the state from the customer edge (CE) to the provider edge (PE) for a specific S-VLAN.

  To enable PE to CE state propagation for an OAM on SVLAN session, configure the `interface-status-tlv` for the CFM session on the S-VLAN logical interface. This configuration ensures that the PE state is propagated as part of the interface status TLV.

  The feature supports propagating SVLAN status on down MEP CFM session using `interface-status-tlv` for CCC family in PPMAN and CFMMAN modes (inline and non-inline).:

  [See Ethernet OAM Support for Service VLANs Overview]

- **Mirror outgoing control-plane traffic with family `any` filters (MX Series with MPC-9 or MPC-10 line cards)**—Port mirroring copies IPv4 or IPv6 packets entering or leaving an interface and sends copies of these packets to an external host or packet analyzer for analysis. One port-mirroring method that you can use allows you to mirror selected transit network traffic to remote network analyzers by sending the mirrored packets through overlay tunnels. The enhanced method allows you to use `family`

any filters with the same match conditions that you would use with family inet or family inet6 to selectively mirror the host-outbound traffic.

For IPv4 traffic—You can use the family any filter with these match conditions:

- address, destination-port, destination-port-except, destination-prefix-list, dscp, dscp-except, first-fragment, fragment-flags, fragment-offset, fragment-offset-except, gre-key, gre-key-except, icmp-code, icmp-code-except, icmp-type, icmp-type-except, ip-address, ip-destination-address, ip-precedence, ip-precedence-except, ip-protocol, ip-protocol-except, ip-source-address, is-fragment, port, port-except, prefix-list, source-port, source-port-except, source-prefix-list, tcp-established, tcp-flags, tcp-initial, ttl, ttl-except

For IPv6 traffic—You can use the family any filter with these match conditions:

- address, destination-port, destination-port-except, destination-prefix-list, extension-header, extension-header-except, first-fragment, gre-key, gre-key-except, hop-limit, hop-limit-except, icmp-code, icmp-code-except, icmp-type, icmp-type-except, ip6-address, ip6-destination-address, ip6-source-address, is-fragment, last-fragment, next-header, next-header-except, payload-protocol, payload-protocol-except, port, port-except, prefix-list, source-port, source-port-except, source-prefix-list, tcp-established, tcp-flags, tcp-initial, traffic-class, traffic-class-except

- **Chunked framing support in NETCONF sessions (MX304, MX960, MX2020, MX10008, and MX10016)**—Junos devices support the chunked framing mechanism for messages in a NETCONF session. Chunked framing is a standardized framing mechanism that ensures that character sequences within XML elements are not misinterpreted as message boundaries. If you enable RFC 6242 compliance, and both peers advertise the :base:1.1 capability, the NETCONF session uses chunked framing for the remainder of the session. Otherwise, the NETCONF session uses the character sequence]]>]]> as the message separator.

  [See Configure RFC-Compliant NETCONF Sessions.]

- **64-bit nanosecond EPOCH timestamp over port-mirrored packets (MX10008, MX10016)**—You can specify that the software provide a 64-bit nanosecond EPOCH timestamp over a port-mirrored packet for family any packets mirrored in ingress and egress directions.

  The port-mirroring destination can be a next-hop group. In this case, every mirrored packet, for each member of the group, carries the same timestamp.

  The timestamp on the mirrored packet is extracted during port-mirror post processing, which executes after the mainline packet is processed. Thus, there is a microsecond-worth delay since the mainline packet entered or exited on the corresponding interface. Also, an L2 or L3 feature that depends on the MAC address for forwarding of the mirrored packet might not function as expected, because the MAC header fields are overwritten with the timestamp.

  [See Timestamping of Port-Mirrored Packets.]

Routing Policy and Firewall Filters

- **Support for counting the number of BGP large communities (ACX Series, cRPD, EX Series, QFX series, MX Series, PTX Series, SRX Series, VRR)**—You can use `large-community-count` to count the number of BGP large communities.

  [See large-community-count.]

Routing Protocols

- **Enhancements to RFC 7775 performance** (MX Series) - RFC 7775 compliance can be achieved with a single CLI command: `set protocols isis rfc7775-compliance`. This command can be used for both single instance and multi-instance configurations. When this command is enabled, the following configurations are started automatically:

  - IS-IS protocol begins originating the "IPv4/IPv6 Extended Reachability Attribute Flags" sub-TLV for applicable TLVs 135, 235, 236, and 237.
  - LSP size is increased by 3 bytes for each of the prefixes containing the attribute sub-TLV.
  - Any Layer 2 LSP with the Down bit set is ignored and treated as if it is not set while route preference calculations are made.
  - Route preference is determined by the rules defined in RFC 7775 for best prefix selection.
  - Up/Down bit and Prefix Attribute flag values are in compliance with the definitions in RFC 7775.

  [See Supported Standards for IS-IS and rfc7775-compliance.]

- **Supports a set of BGP self-diagnostics CLI commands (EX Series, MX Series, and SRX Series)**–A set of BGP self-diagnostics CLI commands are now available that help users to streamline the root cause of common BGP issues automatically. This includes troubleshooting commands for BGP global state overview, BGP running state warnings, BGP neighbor down and flap diagnostics, BGP CPU hogging diagnostics, BGP missing route diagnostics, and BGP dropped route diagnostics. These set of commands are available for `show bgp diagnostics` command.

  [See show-bgp-diagnostics.]

- **Minimum ECMP (MX960)**—We support conditional advertising and withdrawal of BGP routes based on certain constraints such as bandwidth and minimum available next-hop ECMP. When a BGP receiver learns the same route from multiple BGP peers, BGP updates the active BGP path and the routing information base (RIB), also known as the routing table. The BGP export policy determines whether to advertise the BGP route to these next hops based on the number of ECMP BGP peers it receives the prefix from. A BGP route that has multiple ECMP BGP peers creates better resiliency in case of link failures. You can configure a BGP export policy to withdraw a BGP route unless it receives the BGP route prefix from a minimum number of ECMP BGP peers.

- **Enhanced Routing Policies and Multi-Instance IS-IS Support (MX204, MX240, MX304, MX480, MX960, MX10004, MX10008,and MX10016)**—We've introduced enhancements to simplify routing policies and improve IS-IS multi-instance support. You can now tag local and direct routes with tag and tag2 values, match multiple tag2s in a single policy term, and set IS-IS Down bits during inter-instance route redistribution for precise control. Policy configurations support regex for dynamic matching of multiple IS-IS instances, while wildcard patterns streamline operational commands. Additionally, administrators can reuse the same Micro SID Locator and Node-SID across IS-IS instances, enhancing SRv6 scalability. These updates reduce complexity, improve flexibility, and provide greater control for efficient network management.

- **AS loop check in BGP Networks (MX304, MX10004, and MX10008)**--We have enabled AS path loop check for EBGP and IBGP sessions by default and the loop check is made in the BGP peer's AS path domain.

  To disable AS path loop check for IBGP sessions including all routing instances, include the statement `no-loop-check` statement at the `[edit protocols bgp defaults ibgp]` hierarchy level.

- **Generate static RT-Constrain route based on community/wildcard (MX304, MX10004, and MX10008)** –When the RT-Constrain feature is partially deployed in a network, the resource saving benefit is lost. We have extended the static RT-Constrain feature to generate host static RT-Constrain entries from fully qualified route targets configured in the routing policy. You can assign BGP communities or a wildcard route target on the static RT-Constrain route. You can also configure the static RT-Constrain route's origin AS in the NLRI while retaining the global AS number.

- **Selectively disable NH validation based on Community/RT/RD (MX304, MX10004, and MX10008)**—Define a BGP import policy to selectively disable next hop resolution. The policy action sets the next hop to fictitious instead of indirect next hop and avoids resolving the next hop for routes that match the community specified in the policy.

- **Support for VPN BGP Prefix Limit (MX304, MX10004, and MX10008)**–Typically L3VPN deployments limit routes at the customer edge peer level with the `prefix-limit` configuration for a BGP peer family. We have shifted this control to a central location such as the route reflector or a ASBR so that routes originating at all sites in a VPN are taken into account. BGP maintains and enforces the prefix limit as specified by the route target communities originating at various VPN sites to limit the number of prefixes a BGP peer can advertise or receive to conserve resources.

Securing GTP and SCTP Traffic

- **SCTP Firewall Support (MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)—**We support firewall filters for Stream Control Transmission Protocol (SCTP) traffic, allowing network administrators to inspect and manage SCTP packets with custom filters at both ingress and egress points. This update enhances network security by enabling granular control over SCTP traffic, supporting a full range of firewall actions such as accepting, discarding, logging, or tracking packets based on specific criteria. The integration of SCTP filtering into the

firewall infrastructure strengthens protection against unauthorized access and potential threats, ensuring only legitimate SCTP traffic passes through the network.

[See firewall]

Serviceability

- **PacketIO process restart mechanism (MX304)**—We've changed what happens after the PacketIO process crashes. When the PacketIO process crashes, instead of immediately rebooting the line card, the system attempts to restart the PacketIO process three times before rebooting the line card. During these restart attempts, traffic is disrupted and any host-bound traffic is expected to be dropped.

Services Applications

- **Full reassembly of IPv4 and IPv6 packets for MAP-T (MX Series routers)**—The line cards on MX Series routers support full reassembly of IPv4 and IPv6 packets for Mapping of Address and Port with Translation (MAP-T). We are introducing the following enhancements:

  - Maximum supported IP fragment size is increased to 9000 bytes.
  - Maximum IP packet size that can be fully reassembled is increased to 9000 bytes.

  [See Understanding Mapping of Address and Port with Translation (MAP-T).]

- **SecIntel support (MX204, MX304, MX10003, MX10004, MX10008, and MX10016)**—We have integrated Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) with MX204, MX304, and MX10K routers to protect all hosts in your network against security threats.

  The Security Intelligence (SecIntel) process (IPFD) downloads the SecIntel feeds and parses them from the feed connector or ATP Cloud cloud feed server. The web filtering process (URL-filterd) reads the file contents that are fetched from the IPFD and configures the filters on the Packet Forwarding Engine accordingly.

  For the threats configured with `log` action, the `threat-level` and the tenant or the VRF information are embedded in the outgoing syslogs. The CoS policy maps are enhanced with a new `user-attribute` *`integer`* keyword to store and indicate the threat level.

  [See Integration of Juniper ATP Cloud and Web Filtering on MX Series Routers.]

- **Support for inline services (MX304)**—You can use the following inline services on the Packet Forwarding Engine when it is offline or online due to line-card MICs (LMIC) online insertion and removal (OIR):

  - Inline 6rd
  - Network Address Translation (NAT)

- Mapping of Address and Port with Encapsulation (MAP-E) with IPv4/IPv6 reassembly
- Mapping of Address and Port with Translation (MAP-T) with IPv4/IPv6 reassembly.

[See Configuring Inline 6rd, Mapping of Address and Port with Encapsulation (MAP-E), and Mapping of Address and Port with Translation (MAP-T).]

- **Inline IPsec multipath forwarding with UDP encapsulation (MX304, MX10004, and MX10008))**—You can enable the UDP encapsulation of the IPsec traffic which appends a UDP header after the ESP header. The encapsulation provides entropy to the intermediate routers, which helps ECMP. The IPsec packets to be forwarded over multiple paths, thus increasing the throughput.

  [See Inline IPsec Multipath Forwarding with UDP Encapsulation.]

- **Port based `si-` interface support (MX304, MX10004, and MX10008)**—Create four `si-` interfaces per PIC in the format `si-fpc/pic/port` for inline IPsec configuration. If both FPC and PIC are 0, you can have four `si` interfaces: `si-0/0/0`, `si-0/0/1`, `si-0/0/2`, and `si-0/0/3`.

  [See Inline IPsec -Overview.]

Software Installation and Upgrade

- **Static configuration of MAC-IP bindings (MX204, MX240, MX480, MX960, MX10004, MX10008, MX2008, MX2010, and MX2020)**—You can configure MAC-IP bindings on interfaces to improve network management and host communication. This setup is similar to configuring static MAC addresses on an interface. Use this feature to streamline operations in static environments, such as Internet Exchange Points (IXPs), where Customer Edge (CE) routers remain fixed.

  [See Static Configuration of MAC-IP Bindings.]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Multi-instance OSPF with SR (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—Configure and run multiple independent interior gateway protocol (IGP) instances of OSPFv2 with segment routing (SR) on a router. You can create two or more OSPF instances and apply SR-MPLS on each instance. Multiple instances of OSPF can advertise different prefix-segment identifiers (prefix-SIDs). Other instances can use these SIDs for making routing decisions.

  Multi-instance OSPF combined with SR enhances network flexibility, scalability, and control over traffic engineering, especially in large and complex networks.

  NOTE: Junos OS does not support the configuration of the same logical interface in multiple IGP instances of OSPFv2.

[See Multiple Independent IGP Instances of OSPFv2 Overview and Example: Configure Multiple Independent Instances of OSPFv2 with Segment Routing.]

- **NSR support for SRv6 IS-IS and SRv6 BGP (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—We support IS-IS nonstop active routing (NSR) for dynamic micro adjacency segment identifiers (SIDs) and dynamic classic adjacency End-x SIDs. Junos OS allocates the same dynamic SID on both the active and backup Routing Engines after switch-over to ensure dynamically allocated SIDs on the primary RE are not repurposed. You can also use BGP NSR for dynamic DT SIDs. Note that Junos OS currently does not support NSR for classic dynamic End SIDs.

  [See How to Enable SRv6 Network Programming in IS-IS Networks.]

Subscriber Management and Services

- **Resiliency support for PPPoE/DHCP/L2TP subscribers on Packet Forwarding Engine-disable (MX960 and MX10004)—**Ensure resiliency of subscriber services when a Packet Forwarding Engine is disabled. Currently this feature is supported until MPC7(EA) based line cards. Packet Forwarding Engines may become non-functional due to various errors including Error Correcting Code (ECC) errors, parity errors, or timeout issues, resulting its memory being invalidated.

  When a PFE in a line card is disabled and if at least one aggregated Ethernet link is present on the active PFE:

  - There is no impact to the existing subscriber functionality.
  - New subscriber login is seamless.

  The feature support includes:

  - **Subscriber operations** for DHCP, PPPoE, and L2TP, remain operational if there is at least one member link of the Aggregated Ethernet present on the active PFE.
  - Traffic redistribution .
  - Session continuity.
  - Subscriber stability.
  - Mode support
  - VLAN compatibility.
  - Redundancy and fault tolerance.

- **Chassis-based DHCP redundancy (MX480)**—We support 1:1 redundancy for active lease queries below the limit of quantification (BLQ). This feature enhances reliability by providing redundancy for non-participating underlying subscriber interfaces, regardless of topology discovery. You can exclude

interfaces without topology discovery. Use this feature on subscriber stacks and DHCP configurations and BBE and non-BBE DHCP configurations in the following scenarios:

- Subscriber management "Enabled" and "Disabled" modes.
- IP Demux and IP Demux Lite.
- Dual-stack and dual-stack single-session modes.
- Pseudowire access model PS Interfaces (L2 Circuit, EVPN VPWS, and L2VPN).
- VRRP access model for gigabit Ethernet, 10Gb Ethernet, and aggregated Ethernet interfaces.
- Non-default routing instances.
- DHCP relay and DHCP servers.

[See M:N Subscriber Service Redundancy on DHCP Server, active-leasequery (DHCP Server), active-leasequery (DHCP Relay agent), and exclude-interface.]

- **Support for ANCP on AFT line cards (MX304)—**

  This feature supports 15 non-Juniper and 14 Juniper-specific vendor-specific attributes (VSAs). Use the new RADIUS VSA for Layer-2 VLAN dynamic profile management. You can use the new Junos OS variable, `$junos-inner-vlan-tag-protocol-id`, to set VLAN map identifiers through RADIUS server or default configuration values.
  [See VSAs Supported by the AAA Service Framework, Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs, access-line (Access-Line Rate Adjustment), and show-ancp-subscriber.]

  We provide support for border network gateway (BNG) for cascading DSLAM deployments including four QoS scheduler levels for residential subscribers. Passive Optical Network (PON) access technologies with broadband internet service models, Copper to the Business (CuTTB), and Fiber to the Business (FTTB).
  [See DSLAM Deployments Over Bonded Channels.]

  MX Series routers configured as L2TP network servers (LNSs) can process detailed subscriber access line information from L2TP access concentrators (LACs), with more accurate CoS shaping. You can detect and autogenerate logical interface sets with expanded traffic rate adjustments for DSL access lines. Use ANCP traffic control and new DSL types for access. [See Layer 2 forwarding when running unified ISSU on AFT-based line cards.]

- **Packet triggered recovery for static VLAN subscribers (MX240, MX304, MX480, MX960, MX2010, MX2020, MX10004, and MX10008)**—We support packet triggered functionality based on the line card on the MX304 and other MX Series devices with MPC10 (ZT ASIC) and MX10K-LC9600 (YT ASIC) line cards.

The packet triggered feature supports static IP assigned subscribers with IPv4 and IPv6 addresses regardless of the VLAN availability. This feature also supports:

- One IP Demux connection per IPv4 or IPv6 address.
- Packet triggered subscribers using authentication and service selection by using RADIUS server and Session and Resource Control (SRC) network.
- CoS at subscriber level.
- Throttling mechanism to mitigate DOS-like attack.
- Removal of IP demux interface when no activity is seen for certain configurable duration. Enable subscriber management service for packet triggered configuration on an underlying interface by using the `enable force` command under `[edit system services hierarchy]` or the `set system services subscriber-management enable force` command.

  [See BNG Redundancy for DHCP Subscribers Using Packet Triggered Based Recovery and enable (Enhanced Subscriber Management).]

- **IPoE DHCP packet triggered recovery for BNG (MX480, MX960, and MX2020)**—Use IPoE DHCP packet-triggered recovery to automatically update IP configurations in DHCP networks. When a data packet from a client with a pre-assigned IP is received, the system creates an IP demultiplexing interface (IP demux IFL).The routing engine authenticates the subscriber with an authentication server, applying requested services such as volume accounting, firewall filters, or CoS. The feature supports failover detection, subscriber creation after failover, static VLAN support for IP demux interfaces (IFL), IPv4 and IPv6 addresses, auto-clear timeout for dynamic IP subscribers, and DHCP recovery after failover. It ensures reliable service for dynamic IP and DHCP subscribers.

  This feature supports stateless border network gateway (BNG) redundancy for LAG (an active backup model) and pseudowire for L2VPN scenario, L2 Circuit based on IP/MPLS PWHT scenario, and EVPN-VPWS access network topologies.

  Use the command `auto-configure session-timeout<seconds>` under `family [inet | inet6]` hierarchy to configure the auto clear timeout functionality on the Active Dynamic IP subscriber.

  Remove Dynamic IP subscriber when DHCP renew or re-connect happens from the same subscriber or customer premises equipment (CPE).

  [See BNG Redundancy for DHCP Subscribers Using Packet Triggered Based Recovery and session-timeout.]

- **Load-based throttling for AFT-based line cards (MX10004 and MX10008)—** Use this feature enabled by default for the advanced forwarding toolkit (AFT)-based line card MX10K-LC9600 on the MX10004 and the MX10008, to prevent saturation of line card processing capacity, reduce programming delays, and improve efficiency. The Packet Forwarding Engine supports multithreading and guides the Routing Engine to control packet management and load balancing. This feature is

supported for integrated and disaggregated border network gateway (BNG) modes, on the following interface types:

- Gigabit Ethernet/Line Termination interface for a single and multiple AFT cards.
- Aggregated Ethernet/Remote Link Termination interface on
- Aggregated Ethernet/Remote Link Termination interface with non-AFT cards.

Use the `no-load-throttle` command under `[edit] system services resource-monitor` hierarchy to disable load-based throttling on AFT-based line cards. [See Load based throttling for AFT based linecards on MX10004 and MX10008 and no-load-throttle.]

- **Subscriber management redundancy for Packet Forwarding Engine during graceful OIR (MX304-LMIC)**—Use subscriber management redundancy on the Packet Forwarding Engine for seamless online insertion and removal (OIR). The system retains the subscribers and flows when an alternate Packet Forwarding Engine provides redundancy. DHCP subscribers remain active even if the Packet Forwarding Engine goes offline, and their functionalities resume when the LMIC is back online. You can cache subscriber accounting statistics during offline periods to ensure accurate values across offline-online transitions. You can clear interface statistics when the Packet Forwarding Engine goes offline.

  [See Subscriber management redundancy for Packet Forwarding Engine during graceful OIR.]

System Logging

- **Trace infrastructure improvements for Junos OS-Junos OS Evolved hybrid systems (MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—We have improved the trace infrastructure for hybrid systems, where the Routing Engine runs Junos OS and the Flexible PIC Concentrators (FPC) run Junos OS Evolved. The trace-writer on the Junos OS Routing Engine can now receive traces from the Junos OS Evolved FPCs and then store the traces in the **/var/log/traces** directory on the Routing Engine. The trace logs are stored in the **/var/log/trace-logs** directory. The FPCs no longer store any traces. We have disabled the existing `show trace` command on the Routing Engine for hybrid devices because these traces are not in human-readable format.

VPNs

- **Signature authentication in IKEv2 (cSRX, MX240, MX304, MX480, MX960, MX10004, MX10008, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Secure your IPsec VPN service that runs using the iked process with IKEv2 signature authentication based on RFC 7427. Enable this feature by using the following options:

- digital-signature—Configure this option at the [edit security ike proposal *proposal-name* authentication-method] hierarchy level to enable the signature authentication method. You can use this method only if your device exchanges a signature hash algorithm with the peer.
- signature-hash-algorithm—Configure this option at the [edit security ike proposal *proposal-name*] hierarchy level to enable the peer device to use one or more specific signature hash algorithms (SHA1, SHA256, SHA384, and SHA512). Note that the IKE peers can use different hash algorithms in different directions.

See [Signature Authentication in IKEv2, proposal (Security IKE), and Signature Hash Algorithm (Security IKE).]

Additional Features

We've extended support for the following features to these platforms.

What's Changed

IN THIS SECTION

Learn about what changed in this release for MX Series routers.

General Routing

- A new counter "Sessions hit due to high rate" is added to show services service-sets screen-session-limit-counters command for all subscriber traffic. This counter tracks the sessions that come up on the screen irrespective of the alarm-without-drop configuration. When alarm-without-drop option is disabled, all the counters display updated statistics. When "alarm-without-drop" is enabled, then, the screen-drop counters on show services service-sets statistic screen-drop command do not increase. As a result, the "sessions hit due to high rate" value is displayed.

[See https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/statement/alarm-without-drop-edit-services-screen-ids-options-usf.html, https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-services-service-sets-statistic-screen-drop.html, and https://www.juniper.net/documentation/us/en/software/junos/cli-reference/topics/ref/command/show-services-service-sets-statistic-screen-session-limit-counters.html.]PR1849594

- When you run the `request vmhost zeroize` command to zeroize a single Routing Engine on a dual Routing Engine device, the CLI incorrectly displays a message indicating that it will zeroize both Routing Engines.

- **G.8275.1 profile configuration with PTP, SyncE, and hybrid mode (Junos)**— On all Junos platforms, when configuring the G.8275.1 profile, it is mandatory to configure Precision Time Protocol (PTP), Synchronous Ethernet (SyncE), and hybrid mode. Earlier, the system would not raise a commit error even if the required hybrid and SyncE configurations were missing while configuring G.8275.1 profile. However, going forward you will not be able to configure the G.8275.1 profile without configuring PTP, SyncE and hybrid mode to be compliant with the ITU-T standards.

  [See G.8275.1 Telecom Profile].

- You can monitor chassis temperature on MX Series devices at Flexible PIC Concentrator (FPC) level as well using the `show chassis alarms` command, which displays a minor, major or critical alarm, "Temperature Warm" when the FPC exceeds the configured warm threshold temperature. PR1877621

- On the MPC7E-10G line card, when you configure the 10-Gigabit Ethernet ports to operate as 1-Gigabit Ethernet ports, use the speed statement at both the [edit interfaces *interface-name* gigether-options] and [edit interfaces *interface-name*] hierarchy levels.PR1879198

- **log-tag functionality**—The log-tag functionality is introduced in `set services service-set`PR1885614

- **Default route installation for non-default routing instances with iked process (MX480 and MX960)**—You can install default route when the `st0` interface is in a non-default routing instance. This enhancement supports migration from MS-MPC to SPC3 as MX-SPC3 injects these routes through auto route insertion (ARI) for traffic selector routes. The configuration facilitates route installation in specified routing instances.

  [See Traffic Selectors in Route-Based VPNs.]

- **New option for debug collector data storage path**—We've included the option `outdir` to specify an output directory for storing debug collector data in a customised path. This allows you to organise and access diagnostic information more efficiently, adapting storage to your specific requirements.

  [See request system debug-info.]

Subscriber Access Management

- You can configure VLAN termination cause codes to specify RADIUS attribute values for different termination scenarios on JUNOS MX platforms supporting the Layer-2 Bitstream Access (L2BSA) feature. You can diagnose and manage network issues effectively by understanding the specific reasons for VLAN termination. Ensure that the correct termination cause codes are sent by validating configuration and testing scenarios to correctly interpret network events. When a subscriber logs out, the system occasionally sends an incorrect termination cause value to RADIUS. The subscriber VLAN "Account-Terminate-Cause" in "Acct-Stop" message for different L2BSA subscriber logout error scenarios is modified to display correct reasons for termination.

  [See VLAN Termination Causes and Code Values and show network-access aaa terminate-code.

User Interface and Configuration

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- **Stale ui-state.db data in persistent NETCONF sessions post-mgd restart**—Existing NETCONF sessions might fetch stale data from ui-state.db after mgd -N restart. New sessions correctly map the refreshed database. Scripts must establish new sessions post-restart to access updated values. Functional configuration remains unaffected. Script failures monitoring "local-host" NETCONF sessions-Scripts might fail when including "local-host" NETCONF sessions in monitoring operations. Internal sessions are now excluded from tracking. Scripts must filter out "local-host" sessions. No impact to internal application functionality.

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for MX Series routers.

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

General Routing

- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality.PR1678453
- This issue is caused because of the fact that peers-synchronize is configured, and master-password is configured to encrypt the config being sync'ed. However since there is no master-password configured on the peer device, the encrypted configuration cannot be decrypted (this is expected). This has not been supported from day-1, however a workaround can be done in order to get this to work. The workaround is to manually configure the same master password on the peer device manually. At a high level the problem is as follows: Consider there are two devices A and B in a peer-sync config 1. config on dev A contains secrets which need to be encrypted with the master password and synced with the device B 2. The master-password (juniper123+masterpassword) is configured on device A and the configuration is encrypted and written to /tmp/sync-peers.conf 3. The /tmp/sync-peers.conf is then synced to device B but device B does not have the same master-password configured which results in the config failing to decrypt. The master-password itself is not a part of the config-database. Additionally, it cannot be transmitted over an unencrypted HA Link, as this would lead to the master-password getting leaked. This is by design, and would be a security concern if it were to be transmitted across an unencrypted channel. Therefore, this work as designed. In order to work around this issue follow these steps: 1. configure the master-password on device B and commit the config 2. configure the same master-password on device A and commit the config and it should get sync'ed correctly.PR1805835
- 40g interface does not support EM policy feature, but it will still display in the CLI output of `show chassis temp-threshold` as it gets created as "et" interface. PR1807219
- There are no registers in the MX304 PSM to find out feed is connected or not. The only thing that we have in the MX304 PSM is whether the input voltage is zero or not. But that does not confirm whether the feed is connected or not. PR1807254

- We will see an extra flap of link happening whenever the link come up first time or when we do link enable or disable. This is due to limitation of the marvell device.PR1817595

- The commit error "Command remap failed" observed on the dual re controller.

  Workaround steps to follow to recover jnu-controller-schema.db:

  - Remove `/var/db/vSRX/<versionname_of_satellite_connected>` directory from the controller shell.
  - Remove **/var/db/jnu_current_sw_version** file from the satellite shell.
  - Restart jnu-management from CLI of the satellite.

  PR1839015

- When PFE Major/Fatal errors were configured for pfe-reset, MPC7/MPC8/MPC9 FPCs gets into ? HOST LOOPBACK WEDGE? post pfe-reset action triggered by the errors. PR1839071

- During LMIC Offline, occasionally we might get the following error messages and this has no functional /traffic impact. mqss_dstat_stream_wait_to_drain: Final Values: Invalid: False, Timeout: False, Timestamp: False, Queue Depth: 16 bytes) mqss_dstat_stream_wait_to_drain: Timeout while waiting for the PHY stream 130 to drain - Queue 130. PR1843705

- On MX304, during the MIC offline sequence, the following error messages can be intermittently observed for a short period in **/var/log/messages [Log]** `mqss_sched_fab_q_node_is_configured: Queue scheduler node doesn't exist - q_node_num 0 mqss_sched_fab_q_node_is_configured: Queue scheduler node doesn't exist - q_node_num 1 . mqss_sched_fab_q_node_is_configured: Queue scheduler node doesn't exist - q_node_num 255` These error messages are harmless in this context (MIC Offline) and have no functional impact. They can be safely ignored. PR1844325

- The JNU's design was to bring in the committed config from satellite to controller but it doesn't include the platform-specific default configs that come from various other junos default config files. This configuration is kept local to the satellite. Application match configuration under security policy is one such config for which warning message will be seen in MX Series controller while using application match as any or any SRX default application. PR1847209

- MX Series bandwidth alarms are refreshed at the configured log interval (default 06:00AM). Any usage changes within this interval which maintains license non-compliance will not raise new alarms just for the changed in license-needed value. Real time license-needed value is updated in the output of `show system license`. PR1853132

- Due to design limitations, syncE clock status on backup Routing Engine will not be displayed properly. There is no functional issue. Use `show chassis synchronization clock-module` to get the correct status of the syncE clock.PR1856148

- Due to design limitations, syncE clock status on backup Routing Engine will not be displayed properly. There is no functional issue. Ignore the status on backup Routing Engine. Always refer the master Routing Engine status.PR1856152

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Junos OS Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. See TSB18251. PR1568757

Layer 2 Ethernet Services

- The issue was seen when test was done back to back GRES within 5 minutes time. This is expected behavior from the system as per current architecture. Wait for sometime before may be 10 minutes or so for subsequent GRES. PR1801234

Platform and Infrastructure

- With a sensor being subscribed via Junos Telemetry Interface (JTI), after the interface is deleted, deactivated, or disabled, the TCP connection is still established, and the CLI command of `show agent sensors` still shows the subscription. PR1477790
- An authentication bypass by spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Refer to JSA88210 for more information.PR1850776

Open Issues

IN THIS SECTION

Learn about open issues in this release for MX Series routers.

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

EVPN

- After GRES, VPWS Switchover occurs only after NSR Phantom Timer expires. The NSR Phantom timer is configurable. This can result in packet loss for that duration. This needs to be fixed in DCBPR1765052
- On all Junos OS and Junos OS Evolved platforms with Ethernet Virtual Private Network - Multiprotocol Label Switching (EVPN-MPLS) setup , stale MAC entries may remain in the MAC table of the EVPN (Ethernet Virtual Private Network) routing instances during rapid MAC-IP move scenarios. This can cause MAC tables to reach their limits preventing new MAC addresses learning and user registration.PR1833660
- On MX Series platforms, to improve the convergence of node failures in EVPN MH interconnects with Data Plane VXLAN, migrating to an Active-Active setup may cause the data plane to become out of sync for ARP entries. The gateway learns the MAC address and advertises it to the peer gateway. However, on the peer gateway, some MAC-IP entries may remain stuck in the 'Unresolved' (Ur) state. PR1848993

General Routing

- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (Primary and Secondary) and switchover happens from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask PR1557999
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality.PR1678453
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. PR1707944
- fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder.PR1717520
- During heavy network churn (interface flaps, session flaps etc.) PFE crash may be seen when streaming both SR and SRTE stats on PTX JUNOS platforms. Issue is not seen when only SR stats or SRTE stats are enabled. PR1730927
- On MX Series Virtual Chassis, due to some timing issue when RPD is restarted, It will not be spawned again. This issue is rarely reproducible.PR1740083
- On MX480 CommonDiag::JDE3(volt_services_show_clients) failing on MPC7e. PR1747033
- On MX2010 Diagnostics::Jde3Diag(phy_reg_access) test fails. PR1747297
- In Netconf private edit configuration session, commit RPC fails when unprotect operation is performed. PR1751574
- On all Junos OS and Junos OS Evolved platforms with telemetry enabled, if the streaming server and export profile for reporting-rate are not properly configured in the analytics settings, rebooting the FPC would prevent any of the interfaces from coming up.PR1779722
- On MX104, the AFEB could crash and reboot following a change of PTP GM clock source, which affects traffic forwarding.PR1782868
- Additional logging has been added to the primry Routing Engine. This is to help narrow down the issue which chassisd process restarted unexpectedly at snmp_init_oids( ) function on the primary Routing Engine while booting up.PR1787608
- When interfaces with different speed are configured as members of AE, some of the members are not added to AE. And if GRES is enabled, vmcore might be generated on backup REPR1799451

- MPC11 In-Service-Software-Upgrade command fails from Junos OS 24.1R1 release to Junos OS 24.2R1 release and causes MPC11 linux crash. The issue only applies to ULC image.PR1803205
- If standalone device has vccpd running with configurations as per virtual chassis, then it is considered a virtual chassis and not a standalone device. All messages seen will be as per virtual chassis as well.PR1805266
- An improper resource shutdown or release vulnerability in the SIP ALG of Junos OS on MX Series with MS-MPC allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). Refer to JSA100088 for more information.PR1806872
- On all Junos OS QFX5K platforms, traffic loss occurs and the layer 3 interface cannot be deleted when many routes use the same layer 3 interface. QFX5K is encapsulating the packets with the wrong destination MAC (DMAC) and virtual network identifier (VNID) for a few IP addresses after disabling the interface.PR1808550
- IS-IS session over MPC11 cards flapped due to "3-Way handshake failed" during ISSU (FRU upgrade stage - reboot phase). PR1809351
- `set chassis no-reset-on-timeout` is a debug command for SPC3 to prevent rebooting in case of issue. It is not to be set during normal operations since SPC3 may need reboots to come online.PR1809929
- Incorrect configuration of packet trigger IPv6 subscribers may result in misleading output of `show subscribers extensive` command, which may report sessions as ACTIVE, even though they have not been installed in the forwarding engine.PR1817549
- Traffic loss will be seen on 1G-SFP-T if speed is configured to 100m. 1G SFP-T has the AN feature enabled but the PHY we have b/w SFP-T and switch ie., PHY82756 doesn't support AN and this mismatch is causing the traffic loss. This needs feature enhancement PR1817992
- On MX Series platforms with MPC-3D-16x10GE cards, errors "Error to get synce int status" flood continuously when trying to get synce status. synce is an unsupported feature on MPC 3D and has no impact on traffic. So when device is trying to get the synce status which is not supported on MPC 3D card we are landing on that error state and log is flooding with the same error.PR1818617
- Observing that actual total count is not matching with exact count while verifying no of files present under /var/log in r0 device.PR1819456
- Multicast packets duplication happens under the condition ELAN + MVPN network and RP is out side of its core network. In this scenario, egress PE which is non-DF will send back multicast traffic to core side duplicated traffic will happen.PR1820746
- On MX platforms with MS-MPC/MS-MIC with IPsec (Internet Protocol Security) configured, IPsec traffic loss will be observed if an SA (Security Association) deletion request is sent by the peer just before the SA installation is completed. The issue happens in the scale scenario (4000 tunnels are configured, and when the SA count reaches up to 3900).PR1825835

- On MX Series platforms with MS-MPC and Carrier-Grade Network Address Translation (CGNAT) configured, a large number of "out-of-address" errors and stale NAT mappings for SIP (Session Initiation Protocol) traffic can occur. This can lead to a lack of available resources and cause new connections to be dropped.PR1826847

- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. Therefor, to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options or arguments. Note: Incoming SCP connections from outside hosts that are running OpenSSH version >=9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server"PR1827152

- On Junos OS MX Series with MS-MPC/MS-MIC cards, when clear service sessions are executed from multiple windows (approx 5 terminals), the PIC reboots and eventually all the service traffic will be impacted.PR1827806

- "user.notice logrotate: ALERT exited abnormally with [1]" messages can be seen on a system with an MPC10E. PR1833493

- On all Junos and Junos Evolved platforms, 72-byte size memory leak is seen when interface configuration is added. But there is no traffic impact due to this issue.PR1842546

- Memory leak is detected with rpd task blocks "so_in". PR1842558

- Based on SFB2 board has PF chip, SFB3 board has ZF chip. When FPC online/offline performed on MX2K platform, spmb syslog message will be generate zfchip_is_faulty message even if there is only SFB2 board using. == messages == Oct 16 13:17:56 testRouter_RE0 spmb0 fn = zfchip_is_faulty line = 603 name = zfchip->hw_initialized is NULL ========== These are just harmless messages (related to zfchip_is_faulty), should not impact any functionality. Here as ZFchip does not exist, so we see NULL, but this is NOP, does not do anything, just the log.PR1845228

- Memory leak is detected with rpd task blocks "so_in6".PR1846297

- On MX Series platforms with MPC5/MPC7 line cards when there are active pseudo wire subscribers and there is a change in the tunnel-services bandwidth configuration, FPC (Flexible Physical Interface Card Concentrators) crash is observed with the subsequent impact on the traffic.PR1849552

- spmbpfe core can be seen sometimes in these two case: 1. During ISSU when old master RE comes up with the new image, a spmbpfe core is generated when the old master RE goes down after reboot is given post new image installation. The core will be seen post the reboot. 2. When "request system reboot" cli command is executed, a spmbpfe core will occur when the junos goes down and the core

will be seen post the system comes up. These cores generated at these stages will have no impact on a running system. The core are seen only when some kind of reboot is triggered.PR1852648

- On MX Series and SRX Series platforms a rare occurrence issue causes a sudden reboot of the Services Processing Cards (SPC3) in use leading to packet loss during the card offline period in the reboot process.PR1857890
- On MX240, MX480, and MX960 platforms with Services Processing Card 3 (SPC3) , new Network Address Translation (NAT) pools may fail to install, this is due to a mismatch in service-set name length handling. The system stores only 32 characters for service-set information, causing failures when names exceed this limit.PR1881192
- Currently, `request system debug-info mode (custom)` command supports only one mode at a time, not supports multiple modes. PR1886371
- Logs from internal ethernet links monitoring script keep repetitively logged to /var/log/messages file if `set system syslog file messages user any` configuration is used.PR1886633
- When using static address pools BNG Controller allows for the SGRP using the pool to be deleted while subscribers are still logged in. PR1886696
- On all Junos and Junos Evolved platforms, in an Ethernet Virtual Private Network (EVPN) MultiHoming setup with Ethernet Segment Identifier (ESI) configured under logical Interface (IFL) (CE-facing), when the corresponding IFD (Physical Interface) flaps, the MAC route will point to the ESI interface, while it should point to the Multihoming CE (Customer Edge) interface. This results in traffic loss.PR1889335
- On all Junos MX10004 and MX10008 platforms with FPM/craft interface, the craftd (craft control daemon) is unable to run, it causes the craft-control process does not start properly, leading the jnxAlarmRelayMode unable to retrieve data when an alarm condition is triggered. The issue does not cause traffic impact and only may affects monitoring traffic.PR1898722
- MX304 acting as an LNS saw an FPC restart and core file is generated in aft-trio after offlining a MIC. PR1885754
- An LSI logical interface remains in RPD even after being deleted by the interface manager daemon. It is visible in show interface routing but not in show interfaces, indicating that RPD still holds the logical interface despite its removal elsewhere. rpd-agent does not send a delete message to RPD due to a reference count issue. Another daemon likely l2ald, still holds a reference to the logical interface. The rpd-agent only sends the delete once all references are cleared, which doesn't happen in this case. As a workaround, send a "delete pending" message from rpd-agent to RPD. PR1866522
- On all Junos and Junos Evolved platforms, in an Ethernet Virtual Private Network (EVPN) MultiHoming setup with Ethernet Segment Identifier (ESI) configured under logical Interface (IFL) (CE-facing), when the corresponding physical interface flaps, the MAC route will point to the ESI

interface, while it should point to the multihoming customer edge (CE) interface. This results in partial traffic loss.PR1889335

- On MPC3, delete MACsec provisioning before deleting interface.PR1909013

High Availability (HA) and Resiliency

- GRES do not support the configuration of a private route, such as fxp0, when imported into a non-default instance or logical system.

  See KB26616 resolution rib policy is required to apply as a work-around. PR1754351

Layer 2 Ethernet Services

- In order to allow protocol daemons (such as rpd, dot1xd et. al.) to come up fast when master password w/ TPM is configured, the daemons must be allowed to cache the master-password when they read their config. In order to cache the master-password, the daemons must individually reach out to the TPM to decrypt the master password and cache it in their memory. This scenario leads the TPM to be flooded with decryption requests, and therefore causes the TPM to be busy and start rejecting decryption requests. To prevent the daemons from core dumping in this scenario, and to allow successful decryption of secrets, we retry the decryption request to the TPM. However, to allow the TPM queue to drain, we introduce a sched_yield() call before retrying to sleep for 1 quantum of time. Without this, we will fail on all our retries. Additionally, a decryption request can also take a large amount of time (greater than 5 seconds). This results in SCHED_SLIP messages being seen in the logs, as the requesting process is idle while the decryption request is being processed by the TPM. This can exceed the SCHED_SLIP timeout, and result in libjtask logging the SCHED_SLIP messages into the configured system log file. These SCHED_SLIPs should not cause any route instability, are benign, and can be ignored as these are seen only during configuration consumption by the various daemons.PR1768316

- DHCP-Relay short cycle protection can get stuck in grace period. PR1835753

- On all Junos OS and Junos OS Evolved platforms, when performing the `clear dhcp relay active-leasequery statistics peer x.x.x.x` or same for DHCPv6, the relay the statistics are not cleared.PR1849259

MPLS

- While performing ISSU if you have RSVP session scale, with ukern based MPCs you can experience few of the RSVP session protocols flap due to combined effect of ~12 secs dark window followed high utilization of CPU resource utilization by the local ttp rx thread (for ~13 secs). This problem can be avoided by the workaround provided.PR1799286

Network Address Translation (NAT)

- On Junos OS MX Series platform with MSMPC card, Network Management System (NMS) times out when polling any data from jnxSpSvcSetIfTable OID.PR1788400

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- Multiple traps are generated for single event, when more target-addresses are configed in case of INFORM async notifications Cause: INFORM type of async notification handling requires SNMP agent running on router to send a inform-request to the NMS and when NMS sends back a get-response PDU, this need to be handled. In this issue state, when more than one target-address (NMS IP) is configured for a SNMP v3 INFORM set of configuration, when Get-Response comes out of order in which the Inform-Request is sent, the PDU is not handled correctly causing snmp agent to retry the inform-request. This was shows as multiple traps at the NMS side. As a work-around, for this issue would be to use 'trap' instead of 'inform' in the `set snmp v3 notify NOTIFY_NAME type inform` CLI configuration.PR1773863

Platform and Infrastructure

- On upgrading Junos OS 21.2R3-SX release to Junos OS 21.4R3-SX release, it is noticed that EX4300 switches exhibit a higher CPU. Issue is resulting from fast path thread profiling code. It takes on an average 1 ms more for one fast path thread cycle, cumulatively overall fast path thread usage had increased. Thread profiling code has been optimised and the issue is fixed in the future JUNOS.PR1794342

- An authentication bypass by spoofing vulnerability in the RADIUS protocol of Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use.

  See JSA88210 for more information.PR1850776

Routing Protocols

- LDP OSPF are in synchronization state because the IGP interface is down with ldp-synchronization enabled for OSPF. `user@host> show ospf interface ae100.0 extensive Interface State Area DR ID BDR ID Nbrs ae100.0 PtToPt 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 1 Type: P2P, Address: 10.0.60.93, Mask: 255.255.255.252, MTU: 9100, Cost: 1050 Adj count: 1 Hello: 10, Dead: 40, ReXmit: 2, Not Stub Auth type: MD5, Active key ID: 1, Start time: 1970 Jan 1 00:00:00 UTC Protection type: None Topology default (ID 0) -> Cost: 1050 LDP sync state: in sync, for: 00:04:03, reason: IGP interface down config holdtime: infinity.`

  As per the current analysis, the IGP interface goes down because although LDP notified OSPF that LDP synchronization was achieved, OSPF is not able to take note of the LDP synchronization notification, because the OSPF neighbor is not up yet. PR1256434

- On MX Series platforms, unexpected log message will appear if the CLI command 'show version detail' or 'request support information' is executed: test@test> show version detail *** messages *** Oct 12 12:11:48.406 re0 mcsnoopd: INFO: krt mode is 1 Oct 12 12:11:48.406 re0 mcsnoopd: JUNOS SYNC private vectors set PR1315429

- If the file size is too small and the amount of traceoptions volume is too high it can cause scheduler slips and operational impact.PR1815837

- On Junos and EVO platforms, after a Graceful Routing Engine Switchover (GRES), in New master, Indirect routes gets updated to the PFE and result in traffic loss when the transport is L-ISIS with telemetry traffic sensors enabled. In this scenario, Indirect routes going over L-ISIS route. Reason for Indirect route change is due to Underlying L-ISIS route next-hop getting changed. L-ISIS route next-hop getting changed due to ?Sensor-based-stats? configuration which does not support NSR functionality. Hence After Switchover, New Master Create sensors and Installed in the L-ISIS next-hop result in L-ISIS next-hop changed. Once L-ISIS routes nex-thop gets changed, Indirect routes under going for re-resolution which cause traffic impact. PR1886347

- On platforms supporting where BGP Routing Information Base (RIB) Sharding is configured the rpd process crashes on both Routing Engines due to route churns. This timing issue is caused when a particular internal function is used by multiple threads.PR1903829

- Memory leak is detected with rpd task blocks "tm-alloc-bytes_task_trace_filter".PR1849089

Services Applications

- On all MX Series platforms that support MS-MPC/MS-MIC cards, memory leak is observed on kmd (Key Management Deamon) process when IPSec VPN is configured with DiffieHellman group24. The issue is not seen on platforms that support iked process. Memory leak causes incorrect outputs for CLI ipsec/ike show commands and over time kmd might crash when reach its maximum memory, creating a core-dump and resulting in ipsec/vpn going down.PR1781993
- On all MX Series platforms with Multiservices Modular PIC Concentrator (MS-MPC), when Dead Peer Detection (DPD) is enabled under IPsec/Internet Key Exchange (IKE) VPN settings and for any reason an IPsec Security Association (SA) is deleted, the kmd process crashes. Due to the kmd process restart some disruption in tunnel establishment is seen.PR1869769

User Interface and Configuration

- On all Junos OS and Junos OS Evolved platforms, configuration changes using Python script in ZTP does not work and leads to errors. The following errors are seen: `warning: [edit system scripts op allow-url-for-python] not enabled >>> error: The remote op script execution not allowed.` PR1718692
- After switchover in MX2010 platform, test configuration is removed with load update and then rollbacked. During rollback commit, configuration commit failed with error. `Error: commit-check-daemon: Invalid XML from dfwd error: configuration check-out failed.` PR1829614

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for MX Series routers.

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

Authentication and Access Control

- RADIUS authentication is failing when Challenge Token is entered. PR1862203

Class of Service (CoS)

- CoS configured on logical interface does not work on Junos platform when CoS wildcard configurations applied using groups. PR1872595

EVPN

- RPD core file generates on Junos OS 22.2R3-S4. PR1841965

- Few seconds traffic loss during previous DF coming back with EVPN-VPWS non-revertive DF preference feature enabled. PR1851659
- Using SRv6 or MPLS IPv6 encapsulation over EVPN instances causes IPv4 packets to be dropped. PR1857154
- Traffic drops observed in EVPN-VXLAN using ARP NDP entries. PR1859778
- Junos OS and Junos OS Evolved: Specific BGP EVPN update message causes rpd crash (CVE-2025-60004). PR1860302
- EVPN/ETREE not learning MAC's on root. PR1862755
- Junos OS and Junos OS Evolved: In an EVPN environment, receipt of a specifically malformed BGP update causes RPD crash (CVE-2025-52949). PR1863170
- 'TLV type 00000052 not supported on IFL gr' seen repeatedly in syslog for EVPN routing-instance configured with gr- ifls. PR1870365

Forwarding and Sampling

- Incorrect color-aware srTCM marking with yellow packet loss priority. PR1837840
- Junos OS: IPv6 firewall filter fails to match payload-protocol (CVE-2025-52951). PR1844796
- MIB2D will see 100 percent CPU utilization due to MIB2D walk fail. PR1856854
- MIB2D stucked at 100 percent on MX10003. PR1859894
- System becomes unresponsive or crash due to frequent filter changes in a scale scenario having mib2d process in use. PR1872347

General Routing

- Multiple J-UKERN core files might be generated during the sanity test. PR1641517
- Extremely fast interface flaps in MPC10E line-card causes cpu to hog which leads to fpc reboot. PR1727066
- Error message may occur once in a while with full scale when `clear bgp neighbor all` with all the services like EVPN, vrf etc being present. PR1744815
- MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 400G PR1767930

- [./sw-vale-mx-indus] [generic] MX10004 :: LC480 line card crashed with reference to posix_interface_abort () at ../src/pfe/platform/linux/posix_interface.c:2729. PR1784824
- Speed change between 1G and 10G with traffic in high-priority queue on ports causes the link to go down. PR1807277
- FPC crashes due to race condition on MX Series platforms with LC480. PR1809644
- Tunnel source and destination in the same broadcast domain lead to traffic drop. PR1811488
- On MX10K4, MX10K8, MX10K16 systems, in some cases, a SPMB PFE (spmbpfe) core file might be seen when system is going down. PR1817097
- Complete packet loss will be observed for the inter-VLAN traffic in EVPN-VXLAN CRB scenario. PR1820830
- Protocol traffic drops were seen in the network for any configuration change in the protocol. PR1823601
- At the time of Routing Engine switchover the backup Routing Engine serial and part number values are replaced by the CB0 serial and part number values PR1825538
- The rpd crash is observed during upgrade or restart. PR1826194
- TAG and UNTAG bridge interface bandwidth-limit policer are not equal traffic.PR1827843
- Counters not getting cleared at the PFE level when clear ddos-protection protocol statistics is executed. PR1830188
- FPC crash will occur when modifying or deleting a filter instance on Junos OS platforms .PR1830706
- The RPD crashes after executing `show krt error-statistics errorno X`.PR1834859
- Missing telemetry data for FRUs when subscribed to /components/component. PR1837761
- High FPC CPU utilisation and local MAC learning failure in EVPN-MPLS scenario due to rapid MAC moves. PR1838335
- Subscriber's session created using the dynamic profile leads to rpd crash. PR1838354
- The MPC7/MX2K-MPC8E/MX2K-MPC9E line cards of the FPC gets stuck into HOST LOOPBACK WEDGE state post pfe-reset action triggered by any PFE major/fatal errors. PR1839071
- Traffic loss due to tunnel establishment failure in HA setup.PR1839090
- Resource errors observed on PFE slices when egress is logical tunnel. PR1839265
- Line card crashes due to high scale subscribers. PR1839268

- The commit error is seen in backup RE on MX Series platforms. PR1839362
- Tactical Traffic Engineered load sharing utilization displays incorrect percentage on MX Series platforms. PR1840503
- Major alarm "Host 0 bme1 : Ethernet Link to other RE Down" or log "CHASSISD_LINK_RE_ERROR_RECOVER: RE_TO_ORE iface recovery: bme1 is down" is seen when backup RE is removed. PR1840810
- PCP mapping fails for specific internal IPv4 addresses in DS-lite scenario. PR1841231
- ISSU fail for the MPC2E/3E NG FPC result in FPC crash. PR1841400
- The `show chassis synchronization extensive` command output shows syncE is locked to both primary and secondary sources after switching between primary and secondary sources. PR1841695
- MGeo Telemetry - Added cluster name and generation number to subsystem health sensor tree. PR1842439
- Unable to console to VNF using a non-root user from Juniper Device Manager. PR1842451
- Junos OS and Junos OS Evolved: Receipt of a specifically malformed DHCP packet causes jdhcpd process to crash (CVE-2025-30648). PR1842682
- Incorrect MTU value in the ICMP next-hop MTU field, regardless of the actual MTU of the outgoing interfaces. PR1842744
- Inline IPsec tunnel traffic forwarding stops when destination IP prefix is moved from user-defined Virtual routing and forwarding (VRF) to default VRF or from default VRF to user-defined VRF. PR1843098
- The BMP rib-in-post route withdraw feed is not being generated towards the BMP station when an import policy is configured. PR1843374
- Memory leak when deactivating/reactivating routing instances with vrf-table-label. PR1843627
- vlan tagging in Q-in-Q is not handled correctly over EVPN-VxLAN. PR1843817
- Memory leak is seen with rpd task blocks "nhlib_nexthops_004". PR1844160
- Stale MAC-IP entries are not cleared in an EVPN-VXLAN scenario when `encapsulate-inner-vlan` or `decapsulate-accept-inner-vlan` or both configuration statements are present. PR1844623
- High heap memory caused MX-SPC3 PIC to go offline. PR1844731
- Lane laser temperature value is incorrectly displayed in the snmp query. PR1844751
- Subscribers unable to connect in GNF setup. PR1844934

- Unnecessary trace log files related to licenses are generated. PR1845079
- Interface not added back to AE bundle with multiple changes in single commit. PR1845370
- Traffic drop is observed for IPv4 /32 LDP prefixes advertised over BGP-LU when BGP sharding is configured. PR1845425
- Incorrect warning message is seen post hyper-mode configuration change and mismatch of hyper-mode between FPC and Routing Engine impacts performance. PR1845497
- PTP/SyncE config on Junos fusion port causes crashes. PR1846115
- Memory leak is detected with rpd task blocks "rpd-trace". PR1846294
- When `set chassis redundancy failover on-re-to-fpc-stale` is configured unexpected master Routing Engine switchover will be seen if backup Routing Engine reboots resulting in traffic disruption. PR1846557
- ASLA configuration creates ISIS/subTLV 3 with empty value. PR1846610
- Misleading warning when trying to zeroize just one Routing Engine on a dual Routing Engine device. PR1846914
- Some ports take longer than others to come back online when multiple ports experience simultaneous flap. PR1847378
- Core being generated for some processes while using license feature. PR1848160
- Support FW_Continue with HW Segmented Filters on AFT TRIO platform. PR1848740
- Junos OS: A low-privileged user can disable an interface (CVE-2025-52963). PR1848754
- Routing-services enabled on PPPoE dynamic profile causes subscriber login failure for new subscribers. PR1848887
- Configuring BGP rib-sharding and generate route will cause rpd process to crash. PR1848971
- The SNMP mib walk for lldpConfigManAddrPortsTxEnable fails. PR1849307
- The bbe-statsd process crash due to malformed PFE packets. PR1849377
- Handling AE Child Members, VT port properties reset when Access Port is destroyed. PR1849952
- The dot1xd crash on MACsec enabled ports due to key length limit. PR1850387
- Host unreachable from the router with PPPoE when "routing-service" and "RPF-check" are enabled, and the route is learned via EBGP. PR1850562

- Packet duplication and flooding issues are seen when vpls bridge domain is configured on an aggregated Ethernet and label-switched interface across multiple line cards. PR1850604
- When BGP RIB Sharding is enabled, new BGP group/peer added gets stuck at Flags: Sync InboundConvergencePending. PR1850620
- Chassis MX304 going offline due to Power-cycle. PR1850857
- EX3400 Dot1x RADIUS accounting send incorrect value to the server for Acct-Input-Gigawords/ Acct-Output-Gigawords. PR1851299
- Next-hop APIs to support LDP stitching cases over BGP routes pointing to list of indirects. PR1851629
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- With rib-sharding enabled, IPFIX exports wrong SrcAS / DstAS fields. PR1852278
- Memory leaks are seen in bbe-statsd process during the subscriber logout phase. PR1852532
- EVPN/VPLS protocol configuration through CLI is not allowed on device. PR1852905
- On BNG CUPS controller loss of subscriber state is observed when cluster node restarts. PR1853279
- Packet loss observed across multiple traffic items using SR profiles within the L3VPN. PR1853294
- BGP keeps trying to retrieve VPLS table info from the kernel even after the Layer2 instance is deactivated. PR1853521
- Router flag is not getting set in Neighbor Advertisement message. PR1853868
- Devices fail to obtain an IP address when DHCP Security Option 82 is enabled. PR1854253
- The rpd gets struck with 100 percent CPU usage after enabling BGP RIB-Sharding. PR1854481
- The chassisd process crashes when `commit` command is issued multiple times. PR1854658
- Warning message 'Too many VLAN-IDs on untagged interface' is seen when 2049 vlans are configured on trunk LAG interface. PR1855085
- IPv6 neighbor discovery with DHCP packet getting dropped when no-snoop option is enabled for DHCP Relay. PR1855624
- License is missed post system reboot. PR1855728
- IPv4 frameroutes with prefix length of less than /32 do not get applied. PR1855891

- During ISSU the repd experiences a process crash in the master Routing Engine during the image validation phase. PR1855947
- WAN Interfaces fail to receive hostbound traffic when OGE interface FIFO overflow error is detected. PR1855966
- Junos OS and Junos OS Evolved: When RIB sharding is configured each time a show command is executed RPD memory leaks (CVE-2025-52986). PR1856054
- Unable to ping IRB on the Spine when ping from the leaf after upgrade to the 22.2R3-S5 PR1856062
- The "Input errors" shows 0 even when the "Resource errors" in `show interface extensive` CLI command have non-zero number. PR1856231
- Input traffic on physical interface increases in the fabric statistics count despite locality bias feature configured. PR1857225
- The chassisd process crash is seen after the device reboot when chassisd stalls after configuration commit. PR1857833
- The rpd process crashes when generate routes are configured in a rib-sharding scenario.PR1858032
- MX10008: After doing offline fpc, observing major alarms on FPC. PR1858079
- IPv6 link cannot be used for around 10 seconds after DAD finishing due to NS delay. PR1858741
- Route change is not synced after rpd restart due to rib-fib inconsistency. PR1858750
- A momentary drop in traffic is observed when changes are applied on multipath SR-TE LSPs. PR1860334
- When rib-sharding or update-threading are enabled, generated bgp traceoptions files become accessible only to root users. PR1860792
- The rpd crash due to overlapping flow route updates in a single transaction. PR1860888
- The authd process crashes when /etc/resolv.conf file is empty. PR1860913
- IPv6 Inline Distributed BFD sessions for ISIS fail to establish after applying CoS transmit-rate rate-limit configuration. PR1861238
- BGP PIC failover is taking longer than expected when IS-IS as an IGP enabled with LFA. PR1861451
- In BBE scenario the rebalancing event happens later than expected due to periodic rebalance interval miscalculation. PR1861619
- The process rpd is cored while adding or removing dynamic-tunnels. PR1861810
- FPC will crash in MX10003 during the Master switchover to RE1 or Master set to RE1. PR1863091

- MAP-T translation is not working. PR1863280
- Link error reported on one Packet Forwarding Engine will also report error on other PFE. PR1863674
- Observing out-of-order packets when the TCP traffic gets passed over AE bundle and tunnelled via MPLSoUDP tunnel. PR1864237
- Traffic to anycast IPv6 destination addresses dropped when using ECMP routes. PR1865354
- Due to race condition the FPC on MX Series platform crashes. PR1865576
- Traffic drop from subscriber will be observed when `rpf-check` configuration statement is enabled under subscriber dynamic-profile with static underlying VLAN interface. PR1865649
- The vms logical interface(s) remains down when inline-jflow is configured in the system. PR1866570
- PPPoE subscriber login failures observed after interface flapping resulting in AC system errors on Junos MX Series platforms. PR1868007
- The rpd process crashes and asserts are seen due to memory leak. PR1868085
- Debug collector utility should not ask for root password when invoked by super-user class. PR1868326
- CGNAT traffic is dropped when inactive mams interface in AMS due to an empty slot or defective SPC3 card in slot. PR1868509
- After IPv6 tunnel is up and the iked daemon is restarted, post clearing of the IKE SA, ping from one end to the other end is not working as expected. PR1869198
- Subscribers failed to establish DS-Lite softwires due to stale softwire entries. PR1869450
- Image validation fails during the Junos VM validation. PR1870082
- Link instability is seen on 4x10GSR and 40G-SR4 SFP modules from Finisar having high Rx output value. PR1870156
- RPD might crash when upgrading using no-validate. PR1870183
- CUPS-L2-Regression: dbng_single_up_igmp_mld_mts_part1_mts.robot fails in teardown with error no response from radius server. PR1871403
- Fragmented packets dropped in EVPN-MPLS scenario due to the IRB interface MTU limitation. PR1871420
- Filter-Based Forwarding (FBF) failed for over unicast IRB over AE on MX Series and EX Series platforms. PR1871698
- High memory and CPU usage due to unintended phone-home client activation. PR1871802

- The device is in a reboot loop when fips mode is enabled. PR1871858
- The l2ald process crash is observed on non L2NG Junos OS platforms configured with "native-vlan-id" and "bridge-domains" on logical interfaces. PR1872280
- Packet loss or retransmissions observed on MX Series platforms using SFP-T transceivers. PR1872743
- The SPC3 card resets due to kernel memory exhaustion in MX Series platforms with highly scaled routing tables and inline active flow monitoring configured. PR1873938
- Transient traffic loss for CE in an EVPN MPLS setup with multi-homing. PR1874476
- IPSec and IKE SA will remain down and the traffic through IPSec tunnel gets impacted. PR1876271
- Wrong digest algorithm is used for ECDSA key based certificate requests using PKI. PR1876497
- IPsec-inside-IPsec tunnel establishment fails on MX Series platforms with SPC3 cards. PR1876801
- Multicast traffic loss is seen when MVPN with node protection is enabled. PR1877538
- MPC10E: 1PPS measurement failed for class-B over 100GE to 100GE port combinations using SR4 optics. PR1878254
- FPC crash is seen on MX series when disabling AE IFL in mixed-speed configuration without enhanced-ip enabled. PR1880860
- The rpd crash would be observed when two separate next-hops in rpd map to the same next-hop-index in the kernel. PR1881012
- BFD fail to establish over an IPsec tunnel on Juniper MX Series with the SPC3. PR1882490
- EVPN-MPLS BUM Traffic Disruption Due to Incorrect QinQ STag Insertion. PR1882561
- The debug-collection fails due to insufficient space. PR1883317
- MX304 acting as an LNS saw an FPC restart and core dump in aft-trio after offlining a MIC. PR1885754
- snmp mib walk DomCurrentLaneAlarms does not show proper lanes Values in the latest builds. PR1886889
- LC480 - retransmissions seen on NON-JNPR SFP-T when close to IGP recommendations. PR1887864
- Data still seems to be streaming somewhere when the DialOut (Established) connection on the port is already closed. PR1889924
- BNG CUPS Controller will not deploy on a Multi-Geo RHOCP Multicluster. PR1890548

- [MX304] Jack-out and Jack-in standby Routing Engine results in communication loss between the Routing Engines. PR1891577
- Clear security log reports with time interval support. PR1892154
- Intermittent kernel panic results in device reboot or fxpc crash. PR1902609

Infrastructure

- Memory leak is observed when Telemetry is configured. PR1865403
- A local attacker with shell access can execute arbitrary code (CVE-2025-21590). PR1872010

Interfaces and Chassis

- JUNOS MX | iflset stats not getting cleared after issuing `clear interfaces statistics all` and `clear interfaces interface-set statistics all` CLI command. PR1741282
- Incorrect speed assigned to 1G interfaces on MPC2E-3D-NG high-capacity line card modules. PR1824215
- Routing instance configuration statement for ICCP backup liveness detection. PR1850316
- The jpppd process crashes when subscribers frequently login/logout. PR1854387
- FPC process crash observed due to heap memory errors with Inline CFM and VLAN Normalisation. PR1856132
- Observing traffic loss on PS service interface after deactivate and activate VPLS/EVPN instance type. PR1858289
- The "show system storage" command output should show only true and distinct storages. PR1873253

Layer 2 Ethernet Services

- System crash occurs due to duplicate DHCP-assigned IP addresses. PR1810213
- JDHCPD core @ ce_lease_time_compare GenAVLTreeDelete GenAVLTreeEntryDelete. PR1835954

- DHCPv6 BLQ not working as expected. PR1839348
- DHCPv6 Renew from a dual-stack CPE may be ignored if DHCP server is using DUID type 3 (DUID-LL) and DHCPv6 binding doesn't exist. PR1843596
- AE member not able to discover lost LACP peer connection leading to traffic drop. PR1874126

Layer 2 Features

- The snmp mib walk on jnxVplsPwBindTable fails with vpls routing-instances having multiple mesh-groups. PR1806424
- A traffic outage is seen when disabling and enabling the LACP configuration. PR1850803
- On all Junos OS and Junos OS Evolved based platforms, deactivate and active operations are implemented on the master Routing Engine generates rpd core file on backup Routing Engine in rare case. PR1865782

MPLS

- Missing HELLO object in RSVP Hello messages after RE failovers in the NSR mode. PR1792192
- mgd timeout communicating with routing daemon rpd for 30 minutes during RSVP MBB event. PR1837770
- RSVP authentication check fails if the length of the authentication-key is sixteen characters. PR1850130
- The rpd process crashes due to memory exhaustion. PR1854623
- The "in-place-lsp-bandwidth-update" functionality does not work as expected. PR1854987
- Traffic loss will be observed when container-LSP with in-place-lsp-bandwidth-update configured. PR1857867
- RSVP-TE LSP path is not re-optimised to the path with best IGP metric. PR1859219
- The rpd with per-priority subscription configuration. PR1864823
- Traffic drop in LSP is due to link failure before protection signalling is processed. PR1866944
- BFD session failure causes LSP to go down and the inactive route remains in the routing table leads to traffic drop. PR1881906

- Record Route Object displayed in show mpls lsp output is trucated if number of hops is sixteen or more. PR1893822

Network Address Translation (NAT)

- The 'UI_CONFIGURATION_ERROR' error message is seen when a NAT rule-set has multiple rules. PR1873928

Network Management and Monitoring

- REST API doesn't work with passwords that includes the "%" character. PR1840232
- TCP session between syslog server and device remains in closed state. PR1843602
- The eventd memory leak on Syslog over TLS with unconfigured PKI certificate. PR1845058
- Unable to run event scripts for events: system_abnormal_shutdown/system_shutdown/ system_reboot_event. PR1847814
- The eventd process crash occurs due to flooding of out of memory logs. PR1848106
- SNMPV3 Engine-ID does not update to MAC address as configured. PR1866948

Platform and Infrastructure

- An authentication failure occurs when the TACACS+ server detects an error in sending authentication response. PR1829031
- Traffic drops after link flap on active-active ESI setup with MAC pinning enabled. PR1846365
- The standby router goes into the error state when the switchover is performed. PR1847307
- The self-generated traffic on Junos OS platforms use the incorrect source IP with ECMP configuration. PR1849296
- SCFD incorrectly decodes 802.1q tag as the source IP address for suspicious DHCPv4 flows. PR1852259
- User root is shown as incorrect after power cycle of the device. PR1855393

- Junos OS and Junos OS Evolved: Device allows login for user with expired password (CVE-2025-60010). PR1862890
- TCP listening sockets are not displayed correctly. PR1864027
- ARP packet drops seen if proxy-arp restricted is configured on an IRB interface. PR1865605
- NTS for NTP not working even after the Ceritficate is validated with External servers like Chrony and NTPSec. PR1872704
- An IPv6 neighbor solicitation packet is dropped at the ingress PE router when it is received with more than two VLAN tags. PR1874503
- FTP default mode changed from active to passive on Junos OS Release 24.2R2. PR1874525

Routing Policy and Firewall Filters

- Commit delay will be observed when the configuration is changed for the logical system. PR1832853
- Static route validation fails when using an interface-route leaked with rib-groups using "to rib routing-instace-name" as matching condition under rib-groups import-policy PR1849500
- Protocols involved with TCP/IP on a lsi interface have issues as TCP 3-way handshake cannot be completed. PR1871431

Routing Protocols

- Disabling the PIM interface underneath the `[edit protocols pim interfaces <intf-name>]` hierarchy may still show PIM as still being UP instead of DOWN. PR1857699
- The changes from instance-type DEFAULT_INSTANCE to others and vice versa will not be allowed. PR1663776
- "snmp-options backward-traps-only-from-established" for logical-system doesn't work properly. PR1813048
- rt_instance memory leak on bulk configuration changes. PR1832162
- BGP_PREFIX_THRESH_EXCEEDED warning message keeps flooding after accepted max prefix limit is reached. PR1838490
- BGP import policy does not process the next-hop statement. PR1839318

- Configuration check-out fails when applying "inet6.0 static route" with qualified-next-hop and interface settings. PR1839631
- The rpd process will crash when secondary route in VRF is auto-exported. PR1841090
- Route validation fails to synchronize when GRES is configured. PR1842955
- Handling cores when always-compare-med is configured in BGP path selection. PR1854194
- RPD process crash observed with dynamic tunnel configuration with overlap in destination networks under APP based and NHB mode and rollback. PR1842654
- MVPN traffic does not recover after clearing forwarding-cache. PR1845087
- BGP stops advertising VPN routes to EBGP peer if static route-target-filter as local is configured. PR1845169
- Link State of IS-IS IPv6 adjacency is not updated after interface flap (Due to any reason). PR1847557
- The rpd crash on commit when configuring router-advertisement with DNS search label under 3 characters. PR1847811
- Executing a specific CLI command when asregex-optimized is configured causes an rpd crash (CVE-2025-30652). PR1848929
- The CPU for the rpd stuck at 100% on Junos OS platforms PR1848939
- Memory leak is seen when BGP is activated and deactivated. PR1849027
- BGP route still seen in routing table when route not available. PR1849202
- L3VPN routes are not advertised to peer when BGP sessions with route-target filter flaps. PR1849568
- Updating a source-file to load ROAs should be done by changing the name of the source file. PR1853025
- Junos OS and Junos OS Evolved: An unauthenticated adjacent attacker sending a valid BGP UPDATE packet forces a BGP session reset (CVE-2025-52953) PR1855477
- Native_Multicast::: Protocol PIM Interface disable command not working. PR1857699
- Memory leak is observed when "graceful-shutdown" is configured. PR1857801
- Incorrect subcode NOTIFICATION is sent when local interface is disabled for which multihop is configured for directly connected peer. PR1859020
- Memory leak is observed for certain topologies when TI-LFA is configured. PR1859099

- BGP queue deadlock on Junos/Junos OS Evolved/cRPD platforms leading to route advertisement failure and traffic loss. PR1860786
- The rpd crash due to memory corruption in PIM/MSDP network. PR1863470
- The rpd process will crash because of the memory leak. PR1864676
- Valid BGP routes in RIB are displayed with verification state as Invalid. PR1865114
- Too frequent LSP generation is observed on specific SR-LDP stitching scenario. PR1865829
- Longer convergence is seen for a BGP neighbor having validation configured in its import policy. PR1875144
- MX960 mcsnoopd core dump during rt_mcnh_nh_release. PR1876458
- The aggregate-bandwidth feature inconsistency is observed on BGP Route Reflectors with VRF L3VPN multipath. PR1877111
- BGP updates missing graceful-shutdown community after quick sender configuration statement flaps. PR1877261
- rpd crashes when changes are applied to as-path with dynamic-db in use. PR1877288
- EBGP MULTIPATH is not set on ACTIVE route. PR1877332
- Incorrect MPLS label derivation with inactive EBGP route advertisement. PR1881717

Services Applications

- The MX Series devices is unable to properly convert SRC/DST port value for Radius-flow-tap Lawful Intercept DTCP ADD request. PR1839617
- Traffic was lost on MX Series platforms following a Routing Engine failover. PR1853304
- L2TP subscriber is unable to connect when configuration is loaded over default config on all Junos platforms with L2TP subscribers. PR1877876
- On-Box IPv6 packet capture support. PR1880090

Subscriber Access Management

- Error message is observed after device is restarted. PR1813456

- Junos OS and Junos OS Evolved: Vulnerability in the RADIUS protocol for Subscriber Management (Blast-RADIUS) (CVE-2024-3596). PR1822300
- CoA request failure from RADIUS over IPv6. PR1857161

User Interface and Configuration

- BGP IPv6 session control packets are discarded when changing the ipv6 neighbor-address using 'replace pattern' PR1816534
- The `rollback` configuration fails with commit error: Invalid XML from dfwd. PR1829614
- XML namespace string in rpc-reply tag for system-uptime-information was changed to represent the full version name. PR1842868
- TFTP server crashes when configuration to limit connections are not reflected. PR1854461
- Unexpected issues such as login failures or disabled interfaces observed following abrupt reboot during commit operation. PR1861063

VPNs

- Master-encryption-password is not accessible when system is in FIPS mode. PR1665506
- The MVPN traffic forwarding is affected when BGP PIC is enabled. PR1861726
- IFL configured on the LAG interface goes down when the VLAN operation is changed. PR1863228
- On rare circumstances the kmd or iked process crash will be observed on using the third-party library API. PR1864322
- MVPN Source PE might incorrectly send mcast traffic on SPT while actual receiver is still on RPTree. PR1888630

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the MX Series. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

Basic Procedure for Upgrading to Release 24.4R2

NOTE: Before upgrading, back up the file system and the currently active Junos OS configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

```
user@host> request system snapshot
```

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see the Installation and Upgrade Guide.

For more information about the installation process, see Installation and Upgrade Guide and Upgrading Junos OS with Upgraded FreeBSD.

Procedure to Upgrade to Junos OS

To download and install Junos OS:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the routing platform.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

All customers except the customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package:

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-24.4R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-24.4R2.9-signed.tgz
```

Customers in the Eurasian Customs Union (currently composed of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) can use the following package (Limited encryption Junos package):

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-24.4R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-24.4R2.9-limited.tgz
```

Replace source with one of the following values:

- */pathname*—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - **ftp://** *hostname/pathname*
  - **http://** *hostname/pathname*
  - **scp://** *hostname/pathname*

Use the `reboot` command to reboot the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process might take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host

OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

- Starting in Junos OS Release 24.2R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

  [See https://kb.juniper.net/TSB17603.]

NOTE: Most of the existing `request system` commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 4: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform the following Junos OS installation on each Routing Engine separately to avoid disrupting network operation:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine, and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

For the detailed procedure, see the Installation and Upgrade Guide.

Downgrading from Release 24.2R1

To downgrade from Release 24.2R1 to another supported release, follow the procedure for upgrading, but replace the 24.2R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for the NFX Series.

Network Address Translation (NAT)

What's Changed

There are no changes in behavior and syntax in this release for NFX Series devices

Known Limitations

IN THIS SECTION

There are no known limitations in hardware or software in this release for NFX Series devices.

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

General Routing

- On the NFX 250 devices, INSIGHTD messages are logged every 5 seconds.PR1850987.

Open Issues

IN THIS SECTION

Learn about open issues in this release for NFX Series devices.

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

General Routing

- On the NFX350 devices, `srxpfe core` is seen.PR1792616.

VNF

- On the NFX devices, VNF related SNMP traps not generated when a client IP is configured.PR1868397.

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for NFX Series.

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

VNF

- On NFX350 device, in flex mode, traceoptions consume memory which causes IKE (Internet Key Exchange) SAs (Security Associations) tunnel to be down for IPv6 with IKEv1. Enable selective traceoptions to allow other components to work with limited memory.PR1832087.

General Routing

- On the NFX platforms, to map the front panel L2 interfaces to a single L3 interface you can run the `set vmhost virtualization-options interfaces` *`L3-interface-name`* `mapping fail-on-any-peer` command. However, the user can map the interfaces by using the `set vmhost virtualization-options interfaces` *`L3-interface-name`* `mapping peer-interface` command too. Although this latter method is not according to design, it does not affect any traffic. PR1861770.
- When you configure the security policies on the NFX devices using the CLI, [edit security policies from-zone trust to-zone untrust policy <policy-name> match application], the default application, junos-vxlan now appears in the application list. PR1870006.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the NFX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

NOTE: For information about NFX product compatibility, see NFX Product Compatibility.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 5: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Basic Procedure for Upgrading to Release 24.2

When upgrading or downgrading Junos OS, use the `jinstall` package. For information about the contents of the `jinstall` package and details of the installation process, see the Installation and Upgrade Guide. Use other packages, such as the `jbundle` package, only when so instructed by a Juniper Networks support representative.

NOTE: The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the device, such as configuration templates and shell scripts (the only exceptions are the juniper.conf and ssh files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the device. For more information, see the Software Installation and Upgrade Guide.

NOTE: We recommend that you upgrade all software packages out of band using the console because in-band connections are lost during the upgrade process.

To download and install Junos OS Release 24.2R1:

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks webpage:

   https://www.juniper.net/support/downloads/

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

Junos OS Release Notes for QFX Series

IN THIS SECTION

What's New in 24.4R2-S1

IN THIS SECTION

Learn about new features introduced in this release for QFX.

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- QFX10002
- QFX10008
- QFX10016
- QFX10002-60C
- QFX5210-64C

- QFX5200
- QFX5210-48YM
- QFX5210-48T
- QFX5210-32C
- QFX5210-48Y
- QFX5110

EVPN

- **VXLAN-GBP profiles with enhanced OISM in EVPN-VXLAN fabrics (EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4100-H-12MP, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24MP, EX4100-H-24MP-DC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48P, EX4400-48T, EX4400-48XP, EX4650, QFX5120-32C, QFX5120-48T, and QFX5120-48Y)**—We now support running enhanced optimized intersubnet multicast (OISM) in an EVPN-VXLAN network when you configure the `vxlan-gbp-mc-profile` VXLAN group-based policy (GBP) unified forwarding table (UFT) profile at the `[edit chassis forwarding-options]` hierarchy level.

  We don't assign GBP tags to the multicast traffic. Only unicast traffic carries GBP tags in the VXLAN headers.

  You can use enhanced OISM and VXLAN-GBP with:

  - IPv4 underlay connectivity for the EVPN-VXLAN fabric
  - Intra-VLAN (Layer 2 multicast) and inter-VLAN (Layer 3 multicast) traffic
  - IPv4 multicast traffic with IGMP and IGMP snooping
  - IPv6 multicast traffic with MLD and MLD snooping

  Besides configuring this profile, there are no other configuration differences for either feature when you configure them together.

  [See vxlan-gbp-mc-profile, Micro and Macro Segmentation using Group Based Policy in a VXLAN, and Optimized Intersubnet Multicast in EVPN Networks.]

What's New

IN THIS SECTION

Learn about new features introduced in this release for QFX Series switches.

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features are added in Junos OS Release 24.4R2, click the group by release link. You can collapse and expand the list as needed.

- QFX10002
- QFX10008
- QFX10016
- QFX10002-60C
- QFX5210-64C
- QFX5200
- QFX5210-48YM
- QFX5210-48T
- QFX5210-32C
- QFX5210-48Y
- QFX5110

Network Management and Monitoring

- **On-box packet sniffing support (EX4100-48MP, EX4400-48MP, EX4650, QFX5110, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)**—We've introduced on-box packet sniffing capability to monitor and analyze network traffic on ports without using an external device, such as collector or an agent.

On-box packet sniffer allows you to monitor IPv4 packets on ingress or egress ports, matching them based on header attributes like source IP, destination IP, source MAC, destination MAC, VLAN, and VNID. You can store the sniffed packets in pcap format.

This feature reduces costs and simplifies debugging.

We've introduced the following configuration statements to support this feature:

- To enable the tracing operations, configure the `set services pfe traffic traceoptions file` *`filename`* statement.
- To increase the default timer that is set for uninstalling the filter and deleting the entries, configure the `set services pfe traffic monitor-timer` *`time`* statement.
- To enable egress packet monitoring, configure the `set interface` *`interface-name`* `ether-options loopback` statement. You must configure an additional unused interface for a virtual loopback interface to achieve egress packet monitoring.

Use the following commands to monitor data packets and verify the functionality of on-box packet sniffing:

[See On-Box Packet Sniffer Overview and monitor pfe traffic interface.]

Routing Policy and Firewall Filters

- **Support for counting the number of BGP large communities (ACX Series, cRPD, EX Series, QFX series, MX Series, PTX Series, SRX Series, VRR)**—You can use `large-community-count` to count the number of BGP large communities.

  [See large-community-count.]

- **Filter-based forwarding for GBP-tagged traffic (EX4100-48P, EX4400-48F, EX4650, and QFX5120-48T)**—This is the ability to forward traffic to a specified next hop if the GBP tags assigned to that traffic match the GBP tags specified in the filter. Use this feature to apply different routing treatment for the specified tagged traffic versus regular traffic.

  [See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]

Software Installation and Upgrade

- **ZTP with IPv6 support (QFX5200-32C)**—Use a DHCPv6 client and zero-touch provisioning (ZTP) to provision a device. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 and DHCPv4 bindings sequentially. If one of the DHCPv4 bindings fails, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device follows the same process for DHCPv6 until the device is provisioned

successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device.

The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information with the DHCP client.

[See Zero Touch Provisioning.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for QFX Series Switches.

EVPN

- **Duplicate MAC detection timeout (QFX5000 Series switches and EX4650 switches)**—The default setting for `auto-recovery-time` is 5 minutes on these platforms only.

  [See duplicate-mac-detection.]

General Routing

- A new counter **Sessions hit due to high rate** is added to `show services service-sets screen-session-limit-counters` command for all subscriber traffic. This counter tracks the sessions that come up on the screen irrespective of the `alarm-without-drop` configuration. When `alarm-without-drop` option is disabled, all the counters display updated statistics. When `alarm-without-drop` is enabled, then: - The screen-drop counters on `show services service-sets statistic screen-drop` command do not increase. - The **sessions hit due to high rate** value is displayed.

[See alarm-without-drop (IDS Screen Next Gen Services), show services service-sets statistic screen-drops (Next Gen Services), and show services service-sets statistic screen-session-limit-counters (Next Gen Services).

- When you run the request vmhost zeroize command to zeroize a single Routing Engine on a dual Routing Engine device, the CLI incorrectly displays a message indicating that it will zeroize both Routing Engines.PR1869854
- On the MPC7E-10G line card, when you configure the 10-Gigabit Ethernet ports to operate as 1-Gigabit Ethernet ports, use the speed statement at both the edit interfaces <interface name> gigether-options and edit interfaces <interface name> hierarchy levels.PR1879198

User Interface and Configuration

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

- Stale ui-state.db data in persistent NETCONF sessions post-mgd restart-Existing NETCONF sessions might fetch stale data from ui-state.db after mgd -N restart. New sessions correctly map the refreshed database. Scripts must establish new sessions post-restart to access updated values. Functional configuration remains unaffected. **Script failures monitoring "local-host" NETCONF sessions**-Scripts might fail when including "local-host" NETCONF sessions in monitoring operations. Internal sessions are now excluded from tracking. Scripts must filter out "local-host" sessions. No impact to internal application functionality.PR1888557

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for QFX Series switches.

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

General Routing

- Error logs are expected when routes point to the target next hop, which in turn point to hold next hops. These error logs are present for a short time. Later, when the next hop changes from a hold next hop to valid next hop, unilist next hops will be walked again and updated with the appropriate weight and reroute counters, and no more error logs will be seen. PR1387559
- Channelized interfaces leds are not properly represented in `show chassis led`.PR1720502
- Problem: Performing VC split and merge operation causes traffic to be affected for Broadcast, Unknown-unicast and Multicast traffic. RCA: When the Link is Brought down, each FPC will try to re-synchronize the IFDs, in addition resources are busy with updating for the new role. This can cause some synchronization issues with for IFDs/IFLs and other such lists. Test: This can be seen by the VTY command `show ifd brief` and `show ifl brief` for all the FPCs Workaround: It is recommended to wait at least 240 seconds after Splitting the VC ad merging it back again. This ensures that the system can get enough time to synchronize the IFDs/IFLs etc. from the kernel.PR1867979

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. PR1568757

Open Issues

IN THIS SECTION

User Interface and Configuration | 95

Learn about open issues in this release for QFX Series switches.

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

General Routing

- QFX10000 platform drops the Veritas CFS heartbeat , as result the Veritas CFS cannot work. PR1394822
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash.PR1679919
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission.PR1742565
- In a QFX51200-48YM-8C VC setup, after a a primaryship switch over fan tray of linecard might not be displayed in show chassis hardware and show chassis environment. There is no functional impactPR1758400
- On an Ethernet Virtual Private Network (EVPN) / Virtual eXtensible Local-Area Network (VXLAN) scenario, after removing an Aggregated Ethernet (AE) Interface along with its associated physical interface on a QFX5000 series device and then applying any configuration to the physical interface, the fxpc process crashes and the device undergoes an automatic reboot.PR1783397
- On Junos QFX5100 and EX4600 Platforms, high storage Utilization is observed in /var/log due to uncompressed UKERN_GBL.log file. This can lead to low storage warnings and potential write errors for other system logs during that period.PR1804090
- On all Junos QFX5000 platforms, traffic loss happens and the Layer 3 interface cannot be deleted when many routes use the same layer 3 interface. QFX5000 is encapsulating the packets with the wrong DMAC(destination MAC) and VNID(virtual network identifier) for a few IP addresses after disabling the interface.PR1808550

- QFX10002-60C platforms might not send back ICMPv4/v6 reply packets properly due to defects leading to misprogramming of hardware. Ping with v4/v6 from another device to the QFX10002-60C platform will fail. PR1827286
- A memory corruption issue can result random dcpfe (dense concentrator packet forwarding engine) process crashes on specific Junos QFX platforms configured with VXLAN (Virtual Extensible Local Area Network) configuration.PR1856424
- On QFX10008 and QFX10016 , IFL memory is not freed on non-local interface of FPC during configuration changes (eg: IFL delete/deactivate) for L3IFL/L2IFL on AE/Scalar interfaces. Fix is present in common code and risky. It is a day one issue and the per IFL leak is minimal (0.00016% of total Kernel heap size). PR1884163

High Availability (HA) and Resiliency

- Graceful Routing Engine Switchover (GRES) not supporting the configuration of a private route, such as fxp0 , when imported into a non-default instance or logical system. Please see KB https://kb.juniper.net/InfoCenter/index?page=content&id=KB26616 resolution rib policy is required to apply as a work-around. PR1754351

Routing Protocols

- If the file size is too small and the amount of traceoptions volume is too high it can cause scheduler slips and operational impact. PR1815837

User Interface and Configuration

- On all Junos platforms, configuration changes using Python script in ZTP does not work and leads to errors. The following errors are seen: warning: [edit system scripts op allow-url-for-python] not enabled >>> error: The remote op script execution not allowed. PR1718692
- ZTP upgrade in dual RE fails if the image name has special characters. PR1851232

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for QFX Series switches.

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

General Routing

- QFX5000 series platforms become unresponsive after ISSU upgrade. PR1703229
- The remote end of port JNP-SFPP-10GE-T doesn't shut down when the hardware is rebooted using request system reboot. PR1820286
- Protocol traffic drops were seen in the network for any configuration change in the protocol. PR1823601
- The SFP 10GBASE-T part No. 740-083295 on platforms running Junos/Junos EVO is unable to detect a linkdown. PR1823771
- Counters not getting cleared at the PFE level when clear ddos-protection protocol statistics is executed. PR1830188
- FPC crash will occur when modifying or deleting a filter instance on Junos OS platforms. PR1830706
- VRRP fails on 802.1Q VLAN Layer 3 logical interface on QFX10002-60C. PR1834429

- On all Junos QFX5000 and EX4000 platforms the next hop for WECMP (Weighted Equal Cost MultiPath) is not programmed in PFE (Packet Forwarding Engine) properly. PR1838623
- Delay in GBP installation in an EVPN-VXLAN scenario. PR1839916
- The VXLAN ARP packets goes to the ARP queue 34 after disabling ARP suppression. PR1840251
- QFX5210/AS7816 lpm ip route install failed due to table full unit 0. PR1841913
- Incorrect MTU value in the ICMP Next-Hop MTU field, regardless of the actual MTU of the outgoing interfaces. PR1842744
- VLAN tagging in Q-in-Q is not handled correctly over EVPN-VxLAN. PR1843817
- The push pop function on the QFX5120 and EX4650 is not correctly pushing the VLAN. PR1844853
- Unnecessary trace log files related to licenses are generated. PR1845079
- Interface flap between the QFX5120 and QFX5210 with QSFP-100G-LR4-T2 optics PR1845158
- QFX5000 TVP platforms clean-install support with nist compliant secure-erase. PR1847058
- Core being generated for some processes while using license feature. PR1848160
- Handling AE child members, VT port properties reset when access port is destroyed. PR1849952
- Telemetry query on /system xpaths does not work on QFX10002-36Q platform. PR1850033
- Duplication of DHCP request packets when unicast to VRRP gateway. PR1850203
- The l2ald process crash is observed when same Type 5 MAC-IP received with same IP and different MAC. PR1852019
- The dcpfe crash will be seen on Junos QFX5200 platforms due to route churn. PR1854995
- Warning message **Too many VLAN-IDs on untagged interface** is seen when 2049 VLANs are configured on trunk LAG interface. PR1855085
- On some PTX and QFX platform parity error causes packet drop. PR1855459
- Traffic drop observed due to ECMP next-hop programming issue. PR1855990
- Port mirroring fails due to mismatched analyzer and outgoing interface configuration. PR1856361
- Enabling FIPS, committing the configuration, with performing a reboot triggers a boot loop. PR1856855
- QFX10002-60C dropping MPLS to VXLAN traffic. PR1861501

- On particular QFX and EX devices firewall filter counters display double the actual packet count. PR1863813
- L2ald process crash is observed upon executing hidden command `show ethernet-switching debug-statistics fast-mac-update` in case the command doesn't have any output. PR1864295
- Traffic to anycast IPv6 destination addresses dropped when using ECMP routes. PR1865354
- The dcpfe crash is seen in the EVPN-VXLAN scenario. PR1865432
- Traffic loss is seen due to ECMP resource exhaustion on QFX5200, even after ECMP group usage is lower than the threshold. PR1870380
- ON QFX5000 and EX4000 platforms a log is required for route leaking when destination table hits a platform limitation. PR1876359

EVPN

- RPD core-dump on 22.2R3-S4. PR1841965
- Few seconds traffic loss during previous DF coming back with EVPN-VPWS non-revertive DF preference feature enabled. PR1851659

Infrastructure

- Junos OS: A local attacker with shell access can execute arbitrary code (CVE-2025-21590). PR1872010

Interfaces and Chassis

- Routing instance configuration statement for ICCP backup liveness detection. PR1850316
- The jpppd process will crash with frequent subscribers login/logout. PR1854387

Layer 2 Ethernet Services

- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle. PR1854827
- DNS resolution will fail for DNS entries written to "resolv.conf". PR1872292

Platform and Infrastructure

- FTP default mode changed from active to passive on 24.2R2. PR1874525

Routing Protocols

- Disabling the PIM interface underneath the `[edit protocols pim interfaces <intf-name>]` hierarchy may still show PIM as still being UP instead of DOWN. PR1857699
- Configuration check-out fails when applying **inet6.0 static route** with qualified-next-hop and interface settings. PR1839631

User Interface and Configuration

- TFTP server crashes when configuration to limit connections are not reflected. PR1854461

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrading Software on QFX Series Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For information about the contents of the jinstall package and details of the installation process, see the Installation and Upgrade Guide and Junos OS Basics in the QFX Series documentation.

NOTE: For all QFX5110 models, the standard name of the image has been changed from "5e" to "5x." As follows:

Old format: jinstall-host-qfx-5e-

New format: jinstall-host-qfx-5x-

The new format is in effect starting with Junos OS 24.2R1 and will be used for all subsequent mainline Junos OS releases. No maintenance or service releases for release trains prior to 24.2 will implement the change.

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to https://www.juniper.net/support/downloads/junos.html.

   The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.

3. Select **24.2** in the Release pull-down list to the right of the Software tab on the Download Software page.
4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 24.2 release.

   An Alert box appears.
5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.
8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.

   NOTE: We recommend that you upgrade all software packages out of band using the console, because in-band connections are lost during the upgrade process.

   Customers in the United States and Canada use the following command:

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-24.2-R1.n-secure-signed.tgz reboot
```

   Replace *source* with one of the following values:

   - */pathname*—For a software package that is installed from a local directory on the switch.
   - For software packages that are downloaded and installed from a remote location:
     - **ftp://** ***hostname/pathname***
     - **http://** ***hostname/pathname***
     - **scp://** ***hostname/pathname*** (available only for Canada and U.S. version)

   Adding the `reboot` command reboots the switch after the upgrade is installed. When the reboot is complete, the switch displays the login prompt. The loading process can take 5 to 10 minutes.

   Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 24.2 `jinstall` package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-*x*.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add *<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-x86-64-20.4R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the `force-host` option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the `force-host` option.

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* reboot** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add** ***<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **re0** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-
m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the `show version` command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI `delete chassis redundancy` command when prompted. If GRES is enabled, it will be removed with the `redundancy` command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the `[edit routing-options]` hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

```
user@switch# delete chassis redundancy
```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the `request system software add` command:

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-20.4R1.n-secure-signed.tgz
```

For more information about the `request system software add` command, see the CLI Explorer.

9. Reboot the switch to start the new software using the `request system reboot` command:

```
user@switch> request system reboot
```

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the `request system software delete <package-name>` command. This is your last chance to stop the installation.

All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the `show version` command to verify the version of the software installed.

```
user@switch> show version
```

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Master (default)

Routing Engine status:
  Slot 1:
    Current state                  Master
    Election priority              Backup (default)
```

14. Install the new software package using the `request system software add` command:

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-20.4R1.n-secure-signed.tgz
```

For more information about the `request system software add` command, see the CLI Explorer.

15. Reboot the Routing Engine using the `request system reboot` command:

```
user@switch> request system reboot
```

NOTE: You must reboot to load the new installation of Junos OS on the switch. To abort the installation, do not reboot your system. Instead, finish the installation and then issue the `request system software delete jinstall` *<package-name>* command. This is your last chance to stop the installation.

The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the `show version` command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the `request chassis routing-engine master` command, see the CLI Explorer.

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)

outing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- No Link Title
- No Link Title

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

  NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

  ```
  user@switch> show task replication
          Stateful Replication: Enabled
          RE mode: Master
  ```

  If nonstop active routing is not enabled (`Stateful Replication` is `Disabled`), see Configuring Nonstop Active Routing on Switches for information about how to enable it.

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on EX Series Switches for information on how to enable it.

- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Installing Software Packages on QFX Series Devices.

2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.

3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.

4. Start the ISSU:

   - On the switch, enter:

     ```
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     ```

     where *package-name*.tgz is, for example, jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz.

     NOTE: During the upgrade, you cannot access the Junos OS CLI.

     The switch displays status messages similar to the following messages as the upgrade executes:

     ```
     warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
     ISSU: Validating Image
     ISSU: Preparing Backup RE
     Prepare for ISSU
     ISSU: Backup RE Prepare Done
     Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
     Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
     Spawning the backup RE
     Spawn backup RE, index 0 successful
     GRES in progress
     GRES done in 0 seconds
     Waiting for backup RE switchover ready
     GRES operational
     Copying home directories
     Copying home directories successful
     Initiating Chassis In-Service-Upgrade
     Chassis ISSU Started
     ISSU: Preparing Daemons
     ISSU: Daemons Ready for ISSU
     ISSU: Starting Upgrade for FRUs
     ISSU: FPC Warm Booting
     ISSU: FPC Warm Booted
     ISSU: Preparing for Switchover
     ISSU: Ready for Switchover
     Checking In-Service-Upgrade status
       Item           Status                  Reason
       FPC 0          Online (ISSU)
     Send ISSU done to chassisd on backup RE
     ```

```
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

NOTE: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 6: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for SRX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for SRX Series devices.

To view features supported on the SRX Series platforms, view the Feature Explorer using the following links. To see which features are added in Junos OS Release 24.4R1, click the group by release link. You can collapse and expand the list as needed.

- SRX300
- SRX320
- SRX340
- SRX345
- SRX380
- SRX1500
- SRX1600
- SRX2300
- SRX4100
- SRX4200

- SRX4300
- SRX4600
- SRX4700
- SRX5400
- SRX5600
- SRX5800

Hardware

- **New SRX4120 Firewall**—The SRX4120 Firewall provides next-generation firewall capabilities and advanced threat detection and mitigation. This firewall is ideal for small-medium enterprise edge, campus edge, data center edge firewall and secure VPN router deployments for distributed enterprise use-cases.

  Table 7: Features Supported on SRX4120 Firewall

Feature	Description
Chassis	• Support for chassis management and temperature monitoring infrastructure [See Chassis-Level User Guide.]
Chassis Cluster	• Support for ISSU and dual control links with MACsec [See Upgrading a Chassis Cluster Using In-Service Software Upgrade and Media Access Control Security (MACsec) on Chassis Cluster.]
Class of service (CoS)	• Support for CoS [See Understanding Class of Service.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description

Hardware	• The SRX4120 is a 1-U chassis with the following ports. All the ports are MACsec capable ports:
	  • Eight 10Gigabit-Ethernet (GbE) BASE-T ports
	  • Eight 10GbE SFP+ ports
	  • Four 1/10/25GbE SFP28 ports
	  • Two 40/100GbE QSFP28 ports
	  • Two 1GbE SFP HA ports
	  To install the SRX4120 hardware and perform initial software configuration, routine maintenance, and troubleshooting, see SRX4120 Firewall Hardware Guide.
	  [See Feature Explorer for the complete list of features for any platform.]

High availability (HA) and resiliency	• Support for BFD
	  • Support up to 3 x 300 msec failure detection time
	  • Support up to 100 BFD sessions
	  [See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.]
	• Support for Multinode High Availability
	  [See Multinode High Availability.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Interfaces	Supports four PICs (PIC 0, PIC 1, PIC 2, and PIC 3) with the following interfaces: • PIC 0 has eight Base-T interfaces • PIC 1 has eight SFP+ interfaces • PIC 2 has four SFP28 interfaces • PIC 3 has two QSFP28 interfaces The Junos OS creates PIC 0 ports by default. You can channelize the QSFP28 (PIC 3) ports into 4x25 Gbps and 4x10 Gbps. [See Port Speed on SRX Series Firewalls.]
Junos Telemetry Interface	Junos telemetry interface (JTI) streaming support for the following sensors: • System log messages (/junos/events/) • Memory utilization for routing protocol tasks (/junos/task-memory-information/) • Interfaces (/interfaces/) • Hardware operational states for Routing Engine, power supply units (PSUs), switch fabric boards, control boards, switch interface boards, MICs, and PICs (/components/) • Sensor for flow sessions (/junos/security/spu/flow/) [See Junos YANG Data Model Explorer.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Layer 7 security features	• Support for advanced policy-based routing (APBR) [See Advanced Policy-Based Routing.] • Support for application identification (APPID) [See Application Identification.] • Support for application quality of experience (AppQoE) [See Application Quality of Experience.] • Support for application quality of service (AppQoS) [See Application QoS.] • Support for Content Security [See Content Security Overview.] • Support for intrusion detection and prevention (IDP) [See Intrusion Detection and Prevention Overview.] • Support for Juniper Advanced Threat Prevention (ATP) Cloud [See File Scanning Limits.] • Support for Juniper Networks Deep Packet Inspection-Decoder (JDPI) [See Overview.] • Support for Cloud Access Security Broker (CASB) [See Cloud Access Security Broker (CASB).] • Support for SSL proxy

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
	[See SSL Proxy.]
MACsec	• Support for Media Access Control Security (MACsec) [See Understanding Media Access Control Security (MACsec).]
Network management and monitoring	• Support for the filter based packet capture which captures the real-time data packets traveling over the network. Support for data path debugging is not yet available. [See Example: Configure a Firewall Filter for Packet Capture.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
Services applications	• Support for Application Layer Gateway (ALG) [See ALG Overview.] • Support for Domain Name System (DNS) [See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.] • Support for user authentication [See User Authentication Overview.] • Support for security zones [See Security Zones.] • Support for Network Address Translation (NAT) [See NAT Overview.] • Support for screens options for attack detection and prevention [See Screens Options for Attack Detection and Prevention.] • Support for traffic processing [See Traffic Processing on SRX Series Firewalls Overview.] • Support for user identity [See Identity Aware Firewall.] • Support for PowerMode IPsec (PMI) [See PowerMode IPsec.] • Support for DHCP [See DHCP Overview.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
	• Support for GPRS Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP) [See Monitoring GTP Traffic and SCTP Overview.] • Support for on-box reporting [See report (Security Log).] • Support for inline active flow monitoring [See Understand Inline Active Flow Monitoring.] • Support for Two-Way Active Measurement Protocol (TWAMP) [See Understand Two-Way Active Measurement Protocol.] • Support for real-time performance monitoring (RPM) [See Real-Time Performance Monitoring for SRX Devices.] • Support for logical systems [See Logical Systems Overview.]
Software Installation and Upgrade	• Support for BIOS, Secure Boot and boot loader [See Secure Boot.] • Support for Jfirmware [See request system firmware upgrade and show system firmware.] • Support for secure ZTP [See Secure Zero Touch Provisioning.]

Table 7: Features Supported on SRX4120 Firewall *(Continued)*

Feature	Description
User access and authentication administration	• Support for trusted platform module [See SZTP Infrastructure Components.]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Traffic Restriction for New Devices in Juniper ATP Cloud**—Ensure secure communication for all newly enrolled Trusted Platform Module (TPM)-based and non-TPM-based devices by allowing traffic to junipersecurity.net domain only on port 443. Restricting other ports enhances security and reduces the risk of unauthorized data transmission.

  [See Enroll an SRX Series Firewall Using Juniper ATP Cloud Web Portal and Enroll an SRX Series Firewall Using the CLI.]

J-Web

- **J-Web support for SRX4120 Firewall (SRX4120)**—You can use the J-Web UI for initial setup, basic connectivity, and troubleshooting of your SRX Series Firewalls.

Public Key Infrastructure (PKI)

- **HTTPS support for PKI (SRX380, SRX300, SRX320, SRX340, SRX345, SRX1500, SRX1600, SRX2300, SRX4100, SRX4120, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—HTTPS support for PKI enhances the security of certificate management operations. The HTTPS on the PKI establishes secure communication channels for SCEP enrollment and CRL revocation, protecting sensitive information. The PKI process dynamically selects HTTP or HTTPS based on configured URLs, providing flexibility and secure transmissions.

  [See PKI Components in Junos OS.]

What's Changed

IN THIS SECTION

Learn about what changed in this release for SRX Series.

General Routing

- **G.8275.1 profile configuration with PTP, SyncE, and hybrid mode (Junos)**—On all Junos platforms, when configuring the G.8275.1 profile, it is mandatory to configure Precision Time Protocol (PTP), Synchronous Ethernet (SyncE), and hybrid mode. Earlier, the system would not raise a commit error even if the required hybrid and SyncE configurations were missing while configuring G.8275.1 profile. However, going forward you will not be able to configure the G.8275.1 profile without configuring PTP, SyncE and hybrid mode to be compliant with the ITU-T standards.

  [See G.8275.1 Telecom Profile].

Intrusion Detection and Prevention (IDP)

- **Improved Handling of IDP Policy Compilation Status (SRX Series)**—Previously, if an IDP policy compilation failed and a subsequent commit did not involve IDP changes, the compilation status could be lost or appear blank. This has been resolved--the system now retains and displays the last known policy compilation status, even when later commits do not trigger policy recompilation or when the policy is unloaded due to configuration changes. There is no change in the underlying IDP functionality, only in how the status message is preserved.

J-Web

- You can upgrade the zone-based address book to global address books in Global Addresses page. To do this, click Upgrade in the right-side corner of the Global Addresses table. Then, click Yes to continue with the upgrade and click OK to complete. During the upgrade, the system appends the zone name to the zone address name.

Platform Infrastructure

- **ARP restriction for VLAN IDs 3072 to 4094 (SRX4700)**—You cannot configure VLAN IDs ranging from 3072 to 4094. This ensures correct network behavior and prevents potential conflicts within these VLAN ranges, promoting network stability and reliability.

Public Key Infrastructure

- **Certificate enrollment system logs (Junos)**—We've added system logs to notify if there is an SCEP and CMPv2 certificate failure. On SCEP certificate enrollment failure, you can see the PKID_SCEP_EE_CERT_ENROLL_FAIL message. On CMPv2 certificate enrollment failure, you can see the PKID_CMPV2_EE_CERT_ENROLL_FAIL message.

  [See System Log Explorer.]

SSL Proxy

- **Configuration Limits for SSL Proxy Profiles**—We have updated the limits for Trusted CA certificates, Server certificates, and URL categories in both SSL forward proxy and SSL reverse proxy configurations. These changes ensure compliance with the maximum configuration blob size limit of 56,986 bytes.

  Changes in Limit Size:

  - Trusted CA certificate/Server certificates: Maximum limit - 400 (reduced from 1024)
  - URL categories: Maximum limit - 800 (unchanged)

Configuration Statements:

```
user@host# set services ssl proxy profile profile-name trusted-ca (all | [ca-profile] )
user@host# set services ssl proxy profile profile-name server-certificate
user@host# set services ssl proxy profile profile-name whitelist-url-categories [whitelist
url categories]
```

NOTE: In the reverse proxy configuration, ensure combined size of server certificates and URL categories does not exceed 56,986 bytes. If the combined size exceeds the limit, the following error message is displayed during commit:

```
ERROR: Maximum blob size (56986 bytes) exceeded...current blob size is 57014 bytes.
             400 Server certs are taking 54400 bytes, and 27 URL categories are
taking 1728 bytes.
```

This error provides a breakdown of memory usage, helping you adjust the configuration accordingly.

[See Configuring SSL Proxy.]

User Access and Authentication

- **Captive Portal Web Login Page (SRX Series)**—Firewall users must keep the captive portal web login page open after they successfully authenticate. The system automatically logs the user out of the captive portal when the login page is closed.

  [See Captive Portal Authentication and Configure a Custom Logo and Banner Messages.]

User Interface and Configuration

- **Changes to the `show system storage` command output (ACX Series, EX Series, MX Series, QFX Series, and SRX Series)**—We've updated the `show system storage` command output to include only true (physical) storage and exclude any host/hypervisor level storage. In earlier releases, the output also includes a container/jail storage, which does not have a separate storage of its own.

  [See show system storage.]

VPNs

- **Support for hmac-sha-384/512 authentication in PMI (SRX Series Firewalls and vSRX 3.0)**—You can configure hmac-sha-384 and hmac-sha-512 authentication algorithms with PowerMode IPsec (PMI) when running IPsec VPN with the iked process.

  [See PowerMode IPsec.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for SRX Series Firewalls.

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

Flow-Based and Packet-Based Processing

- The rst_sequence knob request SPU flow to keep having sequence number in the record. But, for sessions which has been offloaded, the packet is forwarded directly on NP, due to which SPU did not receive the packet. Also, the sequence number is not synchronize to the SPU session. To use the feature rst_sequence check disable the SOF. PR1830053

General Routing

- The peers-synchronize is configured, and master-password is configured to encrypt the config being synchronize. However, the master-password configured on the peer device, the encrypted configuration cannot be decrypted. PR1805835

Infrastructure

- When upgrading from releases before Junos OS release 21.2 to release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the no-validate option to complete successfully. https://kb.juniper.net/TSB18251. PR1568757

Platform and Infrastructure

- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Refer to https://supportportal.juniper.net/JSA88210 for more information. PR1850776

User Interface and Configuration

- On SRX300 line of devices, when running BFD, performing CLI commands which have a long output and high impact on control plane CPU load, might cause a BFD flap. In such case, use the Dedicated BFD or Real-time BFD feature to avoid the impact. PR1657304

Open Issues

IN THIS SECTION

Learn about open issues in this release for SRX Series Firewall.

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

Chassis Clustering

- With restart-chassis control command on SRX4200/SRX4700/SRX5k, BFD ICL will flap.PR1789245

Content Security

- Avira is not supported for SRX4700 in 24.4R1-S2PR1851627

Flow-Based and Packet-Based Processing

- On all SRX platforms, if IPv6 traffic passes on GREoIPSec tunnel, and IPv4 traffic over same IPSEC tunnel, the path MTU of the sessions gradually decreases and might result in traffic drop and core dump.PR1876536

General Routing

- Additional logging has been added to the primry Routing Engine. This is to help narrow down the issue which chassisd process restarted unexpectedly at snmp_init_oids( ) function on the primary Routing Engine while booting up.PR1787608
- Right after rebooting one of SRX4600 at HA setup, CTL link might keep down.PR1802158
- An Improper Resource Shutdown or Release vulnerability in the SIP ALG of Juniper Networks Junos OS on MX Series with MS-MPC allows an unauthenticated, network-based attacker to cause a Denial-of-Service (DoS). Please refer to https://supportportal.juniper.net/JSA100088 for more information.PR1806872
- On Junos SRX4100/SRX4200 platform, starting and stopping the "monitor traffic interface" or "tcpdump", causes VLAN tagged traffic to be dropped. While the "monitor traffic interface" or "tcpdump" is still running the traffic will function properly, but traffic will stop flowing when it is stopped. This issue only occurs on vlan-tagged interfaces.PR1808353
- On Junos SRX5600 and vSRX3 platforms while upgrading from an older JUNOS version to 22.4R3-S1 or 22.4R3-S2, the upgrade process can fail as the rpd crashes as part of validation process. This is seen if the router config has Multicast/Internet Group Management Protocol (IGMP) or Broadband Edge configuration.PR1810817
- MACSec is supported in routing mode but not in transparent mode.PR1812427
- On all SRX platforms except for SRX5k series platforms , when Secure or Explicit Web Proxy is configured, the flowd process crasches due to a race condition causing traffic outage.PR1813355
- On SRX1500 platform, large IP packets of size 1470 bytes or larger may be dropped when using ethernet-switching and trunk ports.PR1813536
- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version 9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server"PR1827152
- On Junos SRX1600, SRX2300 and SRX4300 platforms, when MVRP (Multiple VLAN registration protocol) is enabled and static vlans are also present, the dynamic vlan learning and assignment doesn't work resulting in traffic loss for the impacted vlans. This issue is observed only when the

interface is converted into routing mode and rolled back to switching mode without reboot.PR1839275

- On SRX3xx series configured with native-vlan-id, after upgrading an SRX3xx series device to Junos version 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-vlan-id was set before the upgrade, the device keeps the setting but it doesnt apply it to the interface. Trying to delete native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) was used then traffic for that VLAN will be affected.PR1847366
- On SRX and MX platforms a rare occurrence issue causes a sudden reboot of the SPC3 (Services Processing Cards) in use leading to packet loss during the card offline period in the reboot process.PR1857890

Network Address Translation (NAT)

- The existing RSI misses out on few important information from NAT plugin, which can now be collected via a new RSI CLI command - "request support information security-components nat". This will provide more data and help in better debugging.PR1825372

Platform and Infrastructure

- On SRX5400/SRX5600/SRX5800 platforms, if vmcore is initiated for XLP PIC (Extreme Low Power Peripheral Interface Controller), vmcore process crashes.PR1811765
- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of Juniper Networks Junos OS and Junos OS Evolved platforms allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. Please refer to https://supportportal.juniper.net/JSA88210 for more information.PR1850776

Services Applications

- On SRX5K HA cluster in FIPS mode, repeated manual failovers of redundancy groups can result in SPC3 or IOC4 or both the cards going offline.PR1797468

VPNs

- On SRX5K platforms with SPC3 installed, IPSec (Internet Protocol Security) tunnels with iked which reuses the same IKE (Internet Key Exchange) gateway peer IP, could be observed not re-establishing.PR1877966

Resolved Issues

IN THIS SECTION

Learn about the issues fixed in this release for SRX Series Firewalls.

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

Application Layer Gateways (ALGs)

- The SRX platform may experience a flowd process crash and generate core dump files when the ALG feature is enabled PR1852968

Authentication and Access Control

- Radius authentication is failing when Challenge Token is entered PR1862203

Chassis Clustering

- Traffic through ipsec vpn tunnel halts/stops after back to back failover until rekey occurs PR1842874
- MNHA with SRG1 IPSEC : MNHA ICL ipsec encryption link went down permanently after rebooting connected router through which ICL was established before. During this state IKE process got stuck at ~70% on MNHA Active node. PR1850967
- Node fails to come back online after chassis-control restart in MNHA architecture PR1873432

Content Security

- The utmd process crashes when EWF or NG web-filtering is configured on SRX with scaled custom URLs PR1841370
- FPC crashing when web filtering type set to "juniper-enhanced" or "NG-juniper" PR1854519

Flow-Based and Packet-Based Processing

- AppQoS rate limit in PMI mode on SRX5K and SRX4600 may drop packets unexpectedly PR1828819

- [False Drop messages for defrag traffic] Packet-drop records with fragmented traffic ",Dropped by FLOW:Defrag return error" seen on " show security packet-drop records " PR1833132
- GRE traffic is getting blocked due to a software programming issue and MTU going below minimum value PR1834338
- Type 5 VXLAN traffic drops are observed when SRX run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer PR1847419
- Junos SRX platforms with chassis cluster configured experience flowd crash due to a race condition in multicast session handling PR1854492
- Data Plane CPU on one device spikes up to 95% during primary node system reboot in SRX cluster PR1856521
- The flowd process crash when service offload and system stats are enabled PR1859062
- Security forwarding process crash may occur when multicast traffic triggers a route resolution request that needs to be processed for a pending session PR1859163
- SRX4700 custom application session inactive timeout is half of the configured value PR1865294
- PFE crash is observed when PFE processes the traffic passing through the dedicated fabric link PR1872613
- The TCP session is not closing properly on the SRX4600 and SRX5K platforms after receiving the FIN-ACK message causing packets to drop for new session if reusing same source port PR1873580
- SRX platforms drops MPLS traffic when "gre-performance-acceleration" knob is enabled PR1876356

General Routing

- Multiple J-UKERN core files might be generated during the sanity test PR1641517
- ifHCOutOctets unexpected spikes in value PR1706125
- Crash dump on DNSF plugin observed on SRX platforms PR1816951
- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT (Flow Thread) threads PR1819911
- SRX:MNHA:ICL:[Longevity] - MNHA Conn State and ICL are down after 48+ hours of device being up with background traffic. PR1822662
- On SRX4600 platforms with heavy traffic, the FPGA drops packets PR1823577

- The rpd crash is observed during upgrade or restart PR1826194
- On SRX platforms MLD groups are successfully formed however egress traffic is not being forwarded as expected PR1828211
- The SRX1500 drops the packet if MTU matches the MRU of the receiving device PR1831955
- The IDP security-package install is throwing 'Attack DB Update Failed' error and AppID stops working PR1832094
- Custom application detection fails for L4 traffic after upgrade due to uncompiled signatures PR1833667
- AE interfaces not coming up if configured with flexible-vlan-tagging and output-vlan-map PR1838033
- Traffic loss due to tunnel establishment failure in HA setup PR1839090
- Load balance hash-key forwarding persists when switching to Layer 3-only PR1842873
- Split brain condition will be seen in SRX4600 configured in Chassis Cluster under certain conditions PR1843413
- Application crash is observed due to insufficient memory when a large number of JFlow entries are created PR1843679
- Unnecessary trace log files related to licenses are generated PR1845079
- SRX PFE crash is observed with source-identity enabled PR1845506
- Auto-re-enrollment for local certificate once fail, not trigger again on SRX platforms PR1845573
- Security-metadata streaming is impacted due to dynamic-filter issue PR1845645
- Packet drops are observed in the VPLS environment on SRX380 platforms in packet mode PR1845997
- FPC0 will not transition to Online and may generate chassis alarm "FPC 0 Hard errors" in SRX4600 devices deployed in chassis cluster PR1846340
- Core being generated for some processes while using license feature PR1848160
- Local or peer device's interface reflects down after SRX380's reboot PR1848557
- It is not recommended to restart chassisd using CLI command "restart chassis-control" in MNHA setup PR1849108
- Reth Reserved buffer increases when reth interface is activated PR1849364

- The commit command failed due to a speed mismatch between the Ten-Gigabit Ethernet (XE) port and the Aggregated Ethernet (AE) interface to which it belongs PR1851261
- Traffic reduction observed for SWP sessions when traffic hits SWP as passthrough. PR1851686
- Flexible-vlan-tagging option is missing under interface hierarchy on SRX3xx series PR1853238
- PIM IP ESP packet fragments dropped in SRX platform PR1854130
- The nsd process crashes on SRX platforms during cluster reboot, failover, or policy addition causes traffic outage PR1857379
- The chassisd process crash is seen after the device reboot when chassisd stalls after configuration commit PR1857833
- Security log report messages w.r.t logical system is not generated PR1860597
- Packet drops can occur when packets are received with a size equal to the default MRU PR1863576
- CoS shaping is not functional on IRB interfaces when the SRX1600 is in switching mode PR1868103
- TCP RST packet gets dropped when used with rst-invalidate-session PR1873583
- Commit Delay Due to Incomplete MACsec Pre-Shared Key Configuration PR1873885
- Unexpected primary role assignment on SRX after node0 reboot PR1877323
- ISSU getting aborted due to configuration-synchronize failure on Junos SRX platforms PR1882569

Infrastructure

- 24.4R2: SecPDT: SRX5600: SPC3 pics are going offline in primary node after installing 24.4R2.1 image with feature configurations PR1879079

Intrusion Detection and Prevention (IDP)

- Not able to download IDP signature via routing instance PR1883645

J-Web

- Created address-sets in global address book is not visible in J-Web PR1805828
- [SRX Jweb] Junos image upload progress message is not displayed on Branch SRX platform PR1844395
- [Jweb] Gratuitous ARP Count shows 0 for redundancy group 1+ when the default gratuitous-arp-count value is used PR1845747
- Unable to load J-Web after upgrading SRX when time zone is set to GMT+x or GMT-x. PR1851362
- VPN failures on SRX due to file descriptor issue PR1858466
- Upgrade and Downgrade will fail from J-Web in SRX4600 PR1876075

Network Management and Monitoring

- SNMPV3 Engine-ID does not update to MAC address as configured PR1866948

Platform and Infrastructure

- The self-generated traffic on Junos platforms use the incorrect source IP with ECMP configuration PR1849296

Routing Policy and Firewall Filters

- The "show security match-policies" command results in a timeout error PR1809563
- [SRX] - RE and PFE policy out of sync with specific configuration. PR1837182
- Security flow sessions are impacted during ISSU on SRX platforms PR1838698
- The mgd process crash is observed during large amount of configurations PR1847877
- Wrong service-name display in SRX RT_FLOW traffic log. PR1859554
- Core is generated on the SRX Secondary node when performing an upgrade PR1859767

- Deny traffic log message is not generated for persistent nat traffic PR1869988
- Protocols involved with TCP/IP on a lsi interface have issues as TCP 3-way handshake cannot be completed PR1871431

Routing Protocols

- The rpd crash on commit when configuring router-advertisement with DNS search label under 3 characters PR1847811
- Updating a source-file to load ROAs should be done by changing the name of the source file PR1853025

Services Applications

- On-Box IPv6 packet capture support PR1880090

Subscriber Access Management

- Junos OS and Junos OS Evolved: Vulnerability in the RADIUS protocol for Subscriber Management (Blast-RADIUS) (CVE-2024-3596) PR1822300

User Interface and Configuration

- XML namespace string in rpc-reply tag for system-uptime-information was changed to represent the full version name. PR1842868

VLAN Infrastructure

- On SRX platforms, STP multicast packets are discarded, causing PVST to fail to converge between switches PR1831324

- Traffic drops are observed when SRX380 platform is configured in l2 transparent-bridge mode PR1852047
- PFE crash due to invalid cached next hop during reinjection on SRX5k PR1856200

VPNs

- Master-encryption-password is not accessible when system is in FIPS mode PR1665506
- The flowd process crashes on SRX5K platforms with multiple line cards in MNHA scenario PR1839665
- ICL link encryption should be used for connection between pub-broker sub-broker with loopback interface IP's should be used with to avoid IPsec session sync failure between master and backup MNHA devices. PR1840788
- MNHA with SRG1 IPSEC : "show chassis high-availability information" cli says SRG1 control plane state as Ready eventhough ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not syncing between Master and Standby MNHA peers. PR1840803
- FIPS-CC:SRX-SME(Berkeley-FreeBSD12): IPSEC sa_config entries on node0 PFE are empty when configured from secondary node. PR1846168
- IKED core might be observed during a restart or failover event. PR1848834
- SRX fails to renegotiate VPN with the correct gateway when the active tunnel goes down PR1851652
- Recommended command to failover from Primary to Backup node PR1861056
- On rare circumstances the kmd or iked process crash will be observed on using the third-party library API PR1864322
- Post reboot , IPSec VPN is not coming up over MNHA active/active deployment PR1864758
- Tunnel sync failure on backup node post 'restart chassis-control' in MNHA Active-Active mode PR1866890
- Type 5 EVPN traffic is dropped on SRX when PMI is disabled or not supported PR1867040
- IPSec tunnel inactive after multiple srg failovers on SRX platforms PR1868453

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the upgrade and downgrade support policy for Junos OS for SRX Series Firewalls. Upgrading or downgrading Junos OS might take several minutes, depending on the size and configuration of the network.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.
- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 8: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Junos OS Release Notes for vSRX

IN THIS SECTION

What's New

There are no new features or enhancements to existing features in this release for vSRX.

What's Changed

IN THIS SECTION

Learn about what changed in this release for vSRX.

Chassis Clustering

- With vSRX 3.0 in Layer 2 chassis cluster mode, use the VirtIO type interface as a redundant Ethernet (reth) interface child to automatically utilize the reth's virtual MAC address. This setup ensures that during a failover, the device does not need to update the child MAC address, enhancing failover efficiency and reducing downtime.

VPNs

- **Support for hmac-sha-384/512 authentication in PMI (SRX Series Firewalls and vSRX 3.0)**—You can configure hmac-sha-384 and hmac-sha-512 authentication algorithms with PowerMode IPsec (PMI) when running IPsec VPN with the iked process.

  [See PowerMode IPsec.]

Known Limitations

Learn about known limitations in this release for vSRX.

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

Platform and Infrastructure

- In the case of MNHA GCP deployment, if a name-server should be configured, then it should be configured along with google's metadata DNS server (169.254.169.254). PR1829939

Open Issues

Learn about open issues in this release for vSRX.

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

General Routing

- On Junos SRX5600 and vSRX3 platforms while upgrading from an older JUNOS version to 22.4R3-S1 or 22.4R3-S2, the upgrade process can fail as the rpd crashes as part of validation process. This is seen if the router config has Multicast/Internet Group Management Protocol (IGMP) or Broadband Edge configuration.PR1810817
- Found that for this tenant_id : s3idh8g4cbe4p5pk we had 64 feeds in SecProfiling category, but only 19 feeds are stored in CDB - secintel_feeds. Because of this only 19 feeds were listed on UI. But while creating a new feed, it is checking if new SecProfiling feeds can be created for the tenant_id in schedule DDB table . Since we have already 64 (which is the max number of feed per tenant)feeds in DDB table, it throws an error - Feed creation error: Feed count limit(64) reached for category: SecProfiling. After running the scripts to create feeds, we need to have scripts to delete the feeds from DDB too so that the data will be accurate during testing. I have removed unwanted entries from DDB table(Now only 20 feeds for the tenant). From now new feeds can be created for Adaptive Threat Profiling sectionPR1819444
- As per OpenSSH 9.0/9.0p1 release notes: "This release switches scp(1) from using the legacy scp/rcp protocol to using the SFTP protocol by default." In this case, since we are running OpenSSH 9.0 and above- OpenSSH_9.7p1 , this uses the "SFTP" protocol by default when scp command is invoked from shell. However, vSRX3.0 supports the "SCP" protocol by default when scp command is invoked. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other options/arguments Note: Incoming SCP connections from outside hosts that are running OpenSSH version 9.0/9.0p1 could fail since sftp-server is disabled by default in Junos OS . Hence, users should either use the -O option on remote host while initiating scp file transfer OR enable sftp-server in the Juniper configuration. To enable sftp-server in Juniper configuration, use the following hierarchy: "set system services ssh sftp-server"PR1827152
- On SRX3xx series configured with native-vlan-id, after upgrading an SRX3xx series device to Junos version 23.4R1 or higher, the native-vlan-id option disappears from the interface settings. If native-

vlan-id was set before the upgrade, the device keeps the setting but it doesnt apply it to the interface. Trying to delete native-vlan-id causes a syntax error. The native-vlan-id feature doesn't work, and if a custom VLAN ID (other than 1) was used then traffic for that VLAN will be affected.PR1847366

Network Address Translation (NAT)

- The existing RSI misses out on few important information from NAT plugin, which can now be collected via a new RSI CLI command - "request support information security-components nat". This will provide more data and help in better debugging.PR1825372

Resolved Issues

Learn about the issues fixed in this release for vSRX.

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

Flow-Based and Packet-Based Processing

- In vSRX orphan backup sessions will exhaust session resources due to high backup session timeout value PR1846897
- Type 5 VXLAN traffic drops are observed when SRX run as L3-VNI gateway and the ingress and egress traffic goes to the same Type-5 VXLAN peer PR1847419
- Data Plane CPU on one device spikes up to 95% during primary node system reboot in SRX cluster PR1856521
- SRX platforms drops MPLS traffic when "gre-performance-acceleration" knob is enabled PR1876356

General Routing

- Interface speed changes when added to aggregated-ethernet bundle on vSRX3.0 platform PR1789508
- Crash dump on DNSF plugin observed on SRX platforms PR1816951
- RTO traffic loss and accumulation of session on secondary node is observed when RTO traffic not evenly distributed to all FLT (Flow Thread) threads PR1819911
- IKE SAs tunnel is down for IPv6 with IKEv1 on NFX350 PR1832087

- Dedicated-offload-cpu requires a full restart of vSRX 3.0 in 24.4R1 PR1842550
- Auto-re-enrollment for local certificate once fail, not trigger again on SRX platforms PR1845573
- vSRX3.0 kernel panic when deployed in Qemu version 8.1 and above PR1845886
- PIM IP ESP packet fragments dropped in SRX platform PR1854130
- Split brain scenario is observed on vSRX3.0 with public cloud MNHA deployment PR1855010
- Cloud Instances (GCP/Azure/AWS): Missing vCPU After Downgrading from Image 25.2 to Lower Versions PR1871397
- The srxpfe process crash is observed on vSRX platform after set disable on the ge- interface and then rollback PR1874848
- On vSRX3.0 platforms, MNHA link fails to come up when MNHA ICL tunnel is enabled alongside dedicated-offload-cpu PR1875491
- [SRX_TYPE_5_USECASE] When source and dest VRF is present in match criteria of a security policy, policy match does not work for vxlan traffic PR1884150

Platform and Infrastructure

- FTP default mode changed from active to passive on 24.2R2 PR1874525

Routing Policy and Firewall Filters

- Failed inter-process communication results in higher heap and buffer usage which impacts the functionality of processes PR1823591

Routing Protocols

- Updating a source-file to load ROAs should be done by changing the name of the source file PR1853025

Subscriber Access Management

- Junos OS and Junos OS Evolved: Vulnerability in the RADIUS protocol for Subscriber Management (Blast-RADIUS) (CVE-2024-3596) PR1822300

VPNs

- ICL link encryption should be used for connection between pub-broker sub-broker with loopback interface IP's should be used with to avoid IPsec session sync failure between master and backup MNHA devices. PR1840788
- L3MNHA with SRG1 IPSEC : "show chassis high-availability information" cli says SRG1 control plane state as Ready eventhough ICL connection between Pub-Broker Sub-broker is not established properly and IPsec sessions are not syncing between Master and Standby MNHA peers. PR1840803
- IPSEC tunnel distribution table on the RE is not cleaned up hitting SRXPFE coredump eventhough DPD is configured. PR1850526
- On vSRX 3.0 platform IPSec tunnels do not redistributed with dedicated-offload-cpu knob enabled PR1860693

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 24.2R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3,18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

Check this using the following command:

```
show system storage | match " /var$" /dev/vtbd1s1f
 2.7G        82M        2.4G        3%  /var
```

Using the `request system storage cleanup` command might help reach that percentage.

- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the `request system software add /var/host-mnt/var/tmp/<upgrade_image>`
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.
- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

NOTE: For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 24.2R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem             Size       Used      Avail  Capacity   Mounted on
       /dev/vtbd0s1a          694M       433M       206M       68%  /
       devfs                  1.0K       1.0K         0B      100%  /dev
       /dev/md0               1.3G       1.3G         0B      100%  /junos
       /cf                    694M       433M       206M       68%  /junos/cf
       devfs                  1.0K       1.0K         0B      100%  /junos/dev/
```

```
        procfs                  4.0K       4.0K          0B      100%  /proc
        /dev/vtbd1s1e           302M        22K       278M        0%  /config
        /dev/vtbd1s1f           2.7G        69M       2.4G        3%  /var
        /dev/vtbd3s2             91M       782K        91M        1%  /var/host
        /dev/md1                302M       1.9M       276M        1%  /mfs
        /var/jail               2.7G        69M       2.4G        3%  /jail/var
        /var/jails/rest-api       2.7G        69M       2.4G      3%  /web-api/var
        /var/log                2.7G        69M       2.4G        3%  /jail/var/log
        devfs                   1.0K       1.0K          0B      100%  /jail/dev
        192.168.1.1:/var/tmp/corefiles       4.5G       125M       4.1G    3%  /var/crash/
corefiles
        192.168.1.1:/var/volatile       1.9G       4.0K       1.9G    0%  /var/log/host
        192.168.1.1:/var/log       4.5G       125M       4.1G     3%  /var/log/hostlogs
        192.168.1.1:/var/traffic-log       4.5G       125M       4.1G    3%  /var/traffic-log
        192.168.1.1:/var/local       4.5G       125M       4.1G    3%  /var/db/host
        192.168.1.1:/var/db/aamwd       4.5G       125M       4.1G    3%  /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G       125M       4.1G    3%  /var/db/secinteld
```

3. Optionally, free up more disk space, if needed, to upload the image.

```
root@vsrx> request system storage cleanup
        List of files to delete:
        Size Date       Name
        11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
        259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
        494B Sep 25 14:15 /var/log/interactive-commands.0.gz
        24.2K Sep 25 14:15 /var/log/messages.0.gz
        27B Sep 25 14:15 /var/log/wtmp.0.gz
        27B Sep 25 14:14 /var/log/wtmp.1.gz
        3027B Sep 25 14:13 /var/tmp/BSD.var.dist
        0B Sep 25 14:14 /var/tmp/LOCK_FILE
        666B Sep 25 14:14 /var/tmp/appidd_trace_debug
        0B Sep 25 14:14 /var/tmp/eedebug_bin_file
        34B Sep 25 14:14 /var/tmp/gksdchk.log
        46B Sep 25 14:14 /var/tmp/kmdchk.log
        57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
        42B Sep 25 14:13 /var/tmp/pfe_debug_commands
        0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Sep 25 14:14 /var/tmp/policy_status
        0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
        Delete these files ? [yes,no] (no) yes
```

```
<
output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 24.2R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE.tgz /var/crash/corefiles/
```

5. From operational mode, install the software upgrade package.

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 24.2 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
```

```
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
==========================================
Installing Host OS ...
upgrade_platform: -------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
```

```
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-24.2-2024-06-06.0_RELEASE_24.2_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 24.2R1 for vSRX.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade, the original image is removed by default as part of the upgrade process.

6. Log in and use the `show version` command to verify the upgrade.

```
--- JUNOS 24.2-2024-06-06.0_RELEASE_24.2_THROTTLE Kernel 64-bit
JNPR-11.0-20240606.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 24.2-2024-06-06.0_RELEASE_24.2_THROTTLE
JUNOS OS Kernel 64-bit  [20240606.170745_fbsd-builder_stable_11]
JUNOS OS libs [20240606.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20240606.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20240606.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20240606.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20240606.170745_fbsd-builder_stable_11]
```

```
JUNOS py extensions [20240606.110007_ssd-builder_release_174_throttle]
JUNOS py base [20240606.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20240606.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20240606.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20240606.110007_ssd-builder_release_174_throttle]
JUNOS libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20240606.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20240606.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20240606.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20240606.110007_ssd-builder_release_174_throttle]
JUNOS modules [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20240606.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20240606.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20240606.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20240606.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20240606.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20240606.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

We have two types of releases, standard EOL and EEOL:

- Standard End of Life (EOL) releases have engineering support for twenty four months after the first general availability date and customer support for an additional six more months.

- Extended End of Life (EEOL) releases have engineering support for sixty months after the first general availability date and customer support for an additional six more months.

> **NOTE**: The sixty months of support for EEOL releases is introduced in Junos OS 23.2 release and is available for all later releases. For releases prior to 23.2, the support for EEOL releases continues to be thirty six months.

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases.

Table 9: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
Standard End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	60 months	End of Engineering + 6 months	Yes	Yes

For more information about standard EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide.

Documentation Updates

This section lists the errata and changes in Junos OS Release 24.4R1 for the vSRX documentation.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

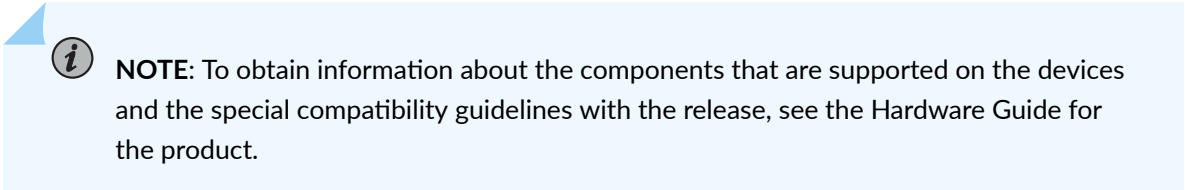
  https://apps.juniper.net/feature-explorer/

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  https://prsearch.juniper.net/InfoCenter/index?page=prsearch

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home



- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  https://pathfinder.juniper.net/compliance/

Requesting Technical Support

IN THIS SECTION

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services 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 https://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/

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

23 December 2025—Revision 10, Junos OS Release 24.4R2.

30 October 2025—Revision 9, Junos OS Release 24.4R2.

23 October 2025—Revision 8, Junos OS Release 24.4R2.

30 September 2025—Revision 7, Junos OS Release 24.4R2.

9 September 2025—Revision 6, Junos OS Release 24.4R2.

8 September 2025—Revision 5, Junos OS Release 24.4R2.

28 August 2025—Revision 4, Junos OS Release 24.4R2.

15 August 2025—Revision 3, Junos OS Release 24.4R2.

14 August 2025—Revision 2, Junos OS Release 24.4R2.

31 July 2025—Revision 1, Junos OS Release 24.4R2.