# Release Notes

Published
2025-07-10

## Junos OS Release 24.4R1®

## 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 24.4R1. 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

**IN THIS SECTION**



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

### 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.]

### Additional Features

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

- **Enhanced Address Detection for Reliable Connectivity (ACX5448-M, MX10008, MX10016, SRX5800, and QFX10008)**—We've improved our network address detection process to deliver more reliable connectivity and uninterrupted performance. This update prevents disruptions caused by duplicate address detection (DAD) failures under rare network conditions. By integrating advanced algorithms and unique identifiers, we reduce false detections and ensure smooth data flow, keeping your network running seamlessly.

## What's Changed

IN THIS SECTION



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

## EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file (`/var/log/syslog`).

## Forwarding and Sampling

- Support added for interface-group match condition for MPLS firewall filter family.

## General Routing

- **Non-revertive switchover for sender based MoFRR**— In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, i.e. traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  [See min-rate.]

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- **Change to the commit process**—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the `commit activate` command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the `clear system commit prepared` command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after `commit prepare` and then issue a `commit`, the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular `commit` operation.

  [See Commit Preparation and Activation Overview.]

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## Routing Protocols

- **Update to IGMP snooping membership command options**— The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**— The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family`

field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

[See show system information and show version.]

## Known Limitations

**IN THIS SECTION**



Learn about known limitations 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

- ACX7024 ports support 10G/1G/25G multi-rate. When peering with other platform or other vendor devices. For example using SFP-LX10 for 1G connection, the link might remain physically down. The reason is auto-negotiation is not supported in ACX7024 PFE due to vendor limitation. In order to make it work, user has to explicitly configure speed or duplex on both sides, and disable auto-negotiation on the peer side. PR1759804

## 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

- 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
- ACX710 Junos OS Platforms reports error clksyncd-service subsystem is not responding to management requests after any new configuration commit causing clksyncd CLI to stuck affecting IPC (Interprocess communication). PR1829340

## Network Management and Monitoring

- Issue: 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

- The KRT queue will be stuck on Junos OS ACX710 platform. PR1787707
- ACX2200 l2circuit hot-standby mode fails to forward the traffic after consecutive neighbor failover and link cutover. PR1797017
- Interfaces fail to coming up on ACX7024, ACX7509, and ACX7348 devices after deleting the routing-instance with DHCPv6 and adding new configuration on same interface. PR1806148
- EVPN-ELAN Multihoming BUM(Broadcast, Unknown Unicast, and Multicast) traffic with IPV6 MPLS underlay is not sent with ESI label to one peer. PR1807188
- Multi-protocol label switching Experimental (MPLS EXP) bit marking not working as expected causing the traffic to be wrongly classified. PR1809169
- ACX710 PTP ports marked 'passive' instead of 'primary' during T-GM selection. PR1810429
- Label corruption is seen in l2circuit redundancy when the primary l2circuit is reachable through the backup. PR1811884
- [ACX7000 Series] DHCPv4/v6 packets might be dropped because DHCP packets are not routed to kernel after initial jdhcpd starts. PR1816246

- Traffic blackholing will be observed in the l2circuit scenario when a non-active path is shut or disabled. PR1816807
- ACX platforms running EVPN-VXLAN in DCI stitching environments will experience traffic outage. PR1817677
- The ARP packet is not sent toward the EVPN core when the route for the destination IP for Layer 3 traffic is not present. PR1817707
- Network Protocol Outage on ACX Junos OS platforms due to SER of Memory ECC Parity Errors. PR1823195
- ACX5448-M - SFP-T flapping issues. PR1828714
- Configuration Archival does not work using SFTP when using the mgmt_junos routing-instance on ACX5448. PR1833705
- Packets are flooding through all local interfaces in a VPLS instance when HQoS scheduler is configured. PR1841079

## Class of Service

- Multiple adjacencies might get dropped over AE interfaces. PR1828018

## Interfaces and Chassis

- The LFM session flaps will be observed at random. PR1811734

## Subscriber Access Management

- authd core after running ZTP. PR1812697

# 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 example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

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. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

You can directly upgrade from Junos OS releases 23.2, 22.4, 22.3 to Junos OS release 24.2R1. For more details, see Juniper Support Portal.

**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 cRPD

IN THIS SECTION

# What's New

IN THIS SECTION



Learn about new features introduced in this release for cRPD.

## 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.]

# What's Changed

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

# Known Limitations

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

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 cRPD.

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

## Resolved Issues

Learn about the issues fixed in this release for cRPD.

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

### Interfaces

- Modifying show interfaces script in cRPD. PR1820367

### MPLS

- MPLS option listed in CLI for interface family configuration to add filter. PR1832515

### Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) PR1826678

### Routing Protocols

- BGP OutQ counter of one of the BGP peers gets stuck after system reboot or restart routing or clear bgp neighbor. PR1788543

# Junos OS Release Notes for cSRX

IN THIS SECTION

# What's New

IN THIS SECTION



Learn about new features introduced in this release for cSRX.

## Content Security

- **Web proxy support for Content Security Sophos 2.0 antivirus and reputation-based file blocking (cSRX, SRX Series Firewall, and vSRX)**—Content Security Sophos 2.0 antivirus now supports web proxy. In addition, we introduce the following file reputation groups to control traffic and provide more control over security:

  - Malware
  - Potentially unwanted applications
  - Unknown
  - Known good or clean

  The Sophos antivirus blocks the traffic if the file reputation belongs to the malware group and permits the known good or clean group traffic. You can define the action for the potentially unwanted applications and unknown group traffic based on your requirements.

  [See Sophos Antivirus Protection Overview, server (Security Sophos Engine Antivirus), sophos-engine, notification-options (Security Antivirus), show security utm anti-virus status, and show security utm anti-virus statistics.]

## Intrusion Detection and Prevention

- **Support logging for exempt rule matching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Use exempt rule logging in the IDP system to monitor and analyze traffic patterns, detect potential security threats, and troubleshoot network issues. Administrators can examine logs to gain insights into traffic exempt from IDP rules and make informed network policy decisions. Enable logging functionality for

exempt rules at the rule level for fine-grained monitoring and analysis of security events, enhancing system visibility.

[See Support logging for exempt rule matching.]

- **IDP intelligent offload per protocol (cSRX, SRX Series Firewalls, and vSRX 3.0)**—The protocol-specific Intelligent-Offload Configuration feature in IDP enables administrators to set inspection depth limits for different protocols. Administrators can use this capability to enable or disable offloading on a per-protocol basis and to configure specific offload limits for protocols such as SSH and FTP. This flexibility optimizes resource usage and ensures efficient session inspections.

  Use the options in the `set security idp sensor-configuration global intelligent-offload-tunable` CLI command to modify the offload settings, specify the protocol, and adjust the offload limit.

  [See Intrusion Detection and Prevention Overview.]

## Network Address Translation (NAT)

- **Monitor subscriber port utilization (cSRX, MX240, MX480, MX960, SRX1500, SRX1600, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX3.0)**–You can monitor and manage port utilization when deploying Carrier Grade Network Address Translation (CGNAT).

  Configure threshold limits to receive notifications when port or port block usage exceeds the configured thresholds.

  - If a pool is configured as Port Block Allocation (PBA) and a subscriber uses more port blocks than the threshold, a notification is generated.
  - For Deterministic NAT (DETNAT) pools, if a subscriber uses more ports than the threshold in the allocated block, a notification is generated.

  The system log messages are:

  - RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING

    `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_RAISE: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 90%, current: 100%`

  - RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR

    `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 50%, current: 25%`

  - RT_SRC_NAT_SUBS_POOL_ALARM_RAISE

    `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING: Subscriber IP: 10.1.1.2, NAT pool: pool-name, threshold alarm [raise, clear] suppressed for 2 times in last 10 seconds`

[See jnxJsSrcNatSubThresholdStatus, jnxJsNAT, Monitor Subscriber Port Utilization Using Carrier Grade NAT, subscriber-pool-utilization-alarm, and pool-utilization-alarm (Security Source NAT Pool).]

## Platform and Infrastructure

- **Data Plane Development Kit (DPDK) library upgrade (cSRX)**—You can now use the DPDK 23.11.2 version to build cSRX images.

  [See cSRX Deployment Guides and DPDK Release 23.11 — Data Plane Development Kit 23.11.2.]

- **Linux LTS22 OS upgrade (cSRX)**— cSRX now supports Linux LTS22 operating system version. This support enhances the performance and reliability of your network operations.

  See [cSRX Deployment Guides.]

## VPNs

- **Migration of policy-based VPNs to route-based VPNs (cSRX, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Migrate policy-based VPNs to route-based VPNs when you run the IPsec VPN service with the iked process. You must configure multiple VPN objects on a shared point-to-point `st0` logical interface to perform the migration.

  [See Shared Point to Point st0 Interface and Migrate Policy-Based VPNs to Route-Based 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).]

## 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 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 24.4R1, 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

## Hardware

**IN THIS SECTION**

## New EX4000 switches (EX Series)

We introduce the latest set of switches in the EX4000 switch series – EX4000-8P, EX4000-12P, EX4000-12T, EX4000-24P, EX4000-24T, EX4000-48P, EX4000-48T, EX4000-12MP, EX4000-24MP, and EX4000-48MP. The cloud-native switches can be managed in Juniper Mist Cloud, enabling simplicity of deployment, configuration, and troubleshooting.

**Table 2: Features Supported on EX4000 Switches**

| Feature | Description |
|---|---|
| Access and authentication | • Support for 802.1X authentication. [See 802.1X Authentication.]<br>• Support for captive portal authentication. [See Captive Portal Authentication.] |
| Chassis | Support for chassis management features, such as:<br>• PSU, fan, and temperature sensor monitoring.<br>• Power management for PSUs and fans. When one fan fails, the switch can function with the other fan until fire shutdown temperature is reached.<br>• Fan speed adjustment based on the temperature readings or values reported by sensors. The system initiates shutdown when the temperature exceeds the fire shutdown threshold.<br>[See show chassis temperature-thresholds.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| CoS | Support for the following ACL and Class of Service Features:<br>• Port ACLs (ingress and egress)<br>• VLAN ACLs (ingress and egress)<br>• Routed ACLs (ingress and egress)<br>• Filter based forwarding (FBF)<br>• Multi-Destination CoS<br>• CoS on interfaces, RVIs, LAGs<br>• L2 CoS (classification, rewrite, queuing)<br>• L3 CoS (classification, rewrite, queuing)<br>• Strict priority and low latency queuing<br>• Scheduled deficit weighted round robin (SDWRR) egress scheduling<br>• Policers (srTCM, trTCM)<br>[See Junos OS CoS for EX Series Switches Overview.] |
| DDoS | Support for distributed denial of service (DDoS) protection.<br>[See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| DHCP | • EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-24P, EX4000-24T, EX4000-48P, and EX4000-48T support the following DHCP features:<br>  • DHCPv4 and DHCPv6 client<br>  • DHCPv4 and DHCPv6 server<br>  • DHCPv4 and DHCPv6 relay agent<br>[See DHCP User Guide.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| Hardware | The cloud-native, low-cost, enterprise-grade switches support the following components and cooling feature:<br>• Ports:<br>  • EX4000-12MP — 8x1G, 4x2.5G, PoE++ 60 W<br>  • EX4000-24MP — 20x1G, 4x2.5G, PoE++ 60 W<br>  • EX4000-48MP — 40x1G, 8x2.5G, PoE++ 60 W<br>  • EX4000-8P - 8x1G PoE+ 30 W<br>  • EX4000-12P - 12x1G PoE+ 30 W<br>  • EX4000-12T - 12x1G<br>  • EX4000-24P - 24x1G PoE+ 30 W<br>  • EX4000-24T - 24x1G<br>  • EX4000-48P - 48x1G PoE+ 30 W<br>  • EX4000-48T - 48x1G<br>• Virtual Chassis ports:<br>  • EX4000-12MP — Two 10G SFP+ (numbered 0 and 1)<br>  • EX4000-24MP — Two 10G SFP+ (numbered 0 and 1)<br>  • EX4000-48MP — Two 10G SFP+ (numbered 0 and 1)<br>  • EX4000-8P - Two 10G SFP+ uplink ports (numbered 2 and 3) that can be converted to Virtual Chassis ports using CLI.<br>  • EX4000-12P - Two 10G SFP+ (numbered 0 and 1) |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| | • EX4000-12T - Two 10G SFP+ (numbered 0 and 1)<br>• EX4000-24P - Two 10G SFP+ (numbered 0 and 1)<br>• EX4000-24T - Two 10G SFP+ (numbered 0 and 1)<br>• EX4000-48P - Two 10G SFP+ (numbered 0 and 1)<br>• EX4000-48T - Two 10G SFP+ (numbered 0 and 1)<br>• Uplink ports:<br>  • EX4000-12MP — Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-24MP — Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-48MP — Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-8P — Two 1G RJ45 non-POE ports (numbered 0 and 1)<br>  • EX4000-12P - Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-12T - Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-24P - Two 1G/10G SFP+ (numbered 2 and 3)<br>  • EX4000-24T - Two 1G/10G SFP+ (numbered 2 and 3) |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| | • EX4000-48P - Two 1G/10G SFP+ (numbered 2 and 3)<br>• EX4000-48T - Two 1G/10G SFP+ (numbered 2 and 3)<br>• Power supply<br>  • All the switches have internal fixed power supplies.<br>• Cooling<br>  • EX4000-12MP — Natural convection cooling, fanless.<br>  • EX4000-24MP — Two inbuilt fans<br>  • EX4000-48MP — Three inbuilt fans<br>  • EX4000-8P - Natural convection cooling, fanless.<br>  • EX4000-12P - Natural convection cooling, fanless.<br>  • EX4000-12T - Natural convection cooling, fanless.<br>  • EX4000-24P - Two inbuilt fans<br>  • EX4000-24T - One inbuilt fan<br>  • EX4000-48P – Three inbuilt fans<br>  • EX4000-48T - One inbuilt fan |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| Interfaces | • Port Speed on Network Interfaces:<br>  • EX4000-12MP, EX4000-24MP, and EX4000-48MP support two PICs each.<br>  • PIC 0 speed configuration on:<br>  • EX4000-12MP—Four 100-Mbps/1-Gbps/2.5-Gbps ports and eight 10-Mbps/100-Mbps/1-Gbps ports.<br>  • EX4000-24MP—Four 100-Mbps/1-Gbps/2.5-Gbps ports and twenty 10-Mbps/100-Mbps/1-Gbps ports.<br>  • EX4000-48MP—Eight 100-Mbps/1-Gbps/2.5-Gbps ports and forty 10-Mbps/100-Mbps/1-Gbps ports.<br>  • PIC 1 on all the three switches comprises of four 1-Gbps/10-Gbps ports.<br>• Each of the EX4000-8port, EX4000-12port, EX4000-24port, and EX4000-48port models provide two fixed uplink ports supporting 1GbE or 10GbE SFP+ transceivers. In addition, the EX4000-12port, EX4000-24port, and EX4000-48port models include two additional 1GbE/10GbE SFP+ ports for Virtual Chassis connections. You can reconfigure these ports for use as network ports.<br>The supported speeds for the EX4000 switch models are as follows:<br>  • EX4000-8P: 8 x 1GbE PoE+ ports;, 2 x 1GBaseT ports, and 2 x 1/10G SFP+ uplink ports |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| | • EX4000-12T: 12 x 1GbE non-PoE access ports; 2 x 1/10G SFP+ uplink ports; and 2 x 10G SFP+ VC ports.<br>• EX4000-12P: 12 x 1 GbE PoE+ access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-12MP: 8 x 1GbE PoE++ access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-24T: 24 x 1GbE non-PoE access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-24P: 24 x 1GbE, PoE+ access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-24MP: 4 x 2.5 MGig access ports, 20 x 1GbE POE++ access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-48: 48 x 1GbE non-PoE access ports, 2 x 1/10G SFP+ uplink ports, and 2 x 10G SFP+ VC ports<br>• EX4000-48P: 48 x 1GbE PoE+ access ports, 2 x 1/10G SFP+ uplink ports, 2 x 10G SFP+ VC ports<br>• EX4000-48MP: 8 x 2.5 MGig, 40 x 1GbE PoE++ access ports, 2 x 1/10G SFP+ uplink ports and 2 x 10G SFP+ VC ports<br>[See Port Speed and Network Interfaces for EX Series.]<br>• Perpetual and Fast PoE support— All the ports of EX4000-12MP, EX4000-24MP, EX4000-48MP, |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| | EX4000-24P, EX4000-48P, EX4000-8P, and EX4000-12P switches support PoE and PoE++.<br><br>If you enable perpetual PoE, power to the connected power device remains uninterrupted even when the switch is rebooting. Perpetual PoE and fast PoE are independent of each other and can coexist. When you power cycle the switch, fast PoE is applicable, if enabled. When you reload the switch by using a Junos CLI reboot command, perpetual PoE is applicable, if enabled.<br><br>[ See Understanding PoE on EX Series Switches.] |
| Layer 2 features | • Support for Layer 2 features.<br><br>[See Ethernet Switching User Guide, Security Services Administration Guide, and Spanning-Tree Protocols User Guide.]<br><br>• Use the `interface-name` and `ip-address` options to configure the management address on the switch.<br><br>[See Configuring LLDP (CLI Procedure).]<br><br>• Support for Layer 2 multicast features.<br><br>[See Multicast Overview and Understanding Multicast Snooping.] |
| Layer 3 features | Support for Layer 3 features and interior gateway protocols (OSPF, IS-IS, RIP, and ECMP).<br><br>[See Understanding OSPF Configurations and BGP Overview.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| Network management and monitoring | • Port mirroring and analyzers, both local and remote.<br><br>[See Port Mirroring and Analyzers.]<br><br>• sFlow support<br><br>[See sFlow Technology Overview .]<br><br>• Support for secure packet capture (PCAP) to Cloud using JTI. Use secure packet capture by including the **/junos/system/linecard/packet-capture** resource path using a Junos remote procedure call (RPC). |
| Optics | Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available<br><br>[See Hardware Compatibility Tool.] |
| Resiliency | We support resiliency for platform components on EX4000 switches. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.<br><br>[See Resiliency.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| Routing Policy and Firewall Filters | • Support for filter based forwarding.<br>• Support for policers (Single Rate Three Color Marker, Two Rate Three Color Marker).<br>• Firewall filter support for port, VLANs, and routed interfaces on ingress and egress.<br>[See Routing Policies, Firewall Filters, and Traffic Policers User Guide |
| Security | • EX4000-12MP, EX4000-24MP, EX4000-48MP, EX4000-8P, EX4000-12P, EX4000-12T, EX4000-24P, EX4000-24T, EX4000-48P, and EX4000-48T support the following security features:<br>  • DHCP snooping (DHCPv4 and DHCPv6)<br>  • Dynamic Address Resolution Protocol (ARP) inspection<br>  • Neighbor discovery inspection<br>  • DHCP option 82<br>  • DHCPv6 option 18 and option 37<br>  • Lightweight DHCPv6 relay agent<br>  • Stateless address autoconfiguration (SLAAC) snooping<br>  • IPv6 Router Advertisement (RA) Guard<br>[See Security Services Administration Guide.] |

**Table 2: Features Supported on EX4000 Switches *(Continued)***

| Feature | Description |
|---|---|
| Services Applications | RPM IPv4 traffic probe support with the tcp-ping, icmp-ping, icmp-ping-timestamp, udp-ping, and udp-ping-timestamp probe types. Probes use software timestamping only.<br><br>[See Understanding Real-Time Performance Monitoring on EX and QFX switches.] |
| Software installation and upgrade | • The EX4000 switches support the `request system firmware upgrade` command to upgrade firmware.<br><br>[See request system firmware upgrade.]<br><br>• Support for PHC.<br><br>[See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]<br><br>• Support for ZTP.<br><br>[See Zero Touch Provisioning.]<br><br>• Support for SZTP.<br><br>[See Secure Zero Touch Provisioning and Generate Voucher Certificate.] |
| Virtual Chassis | From Junos 24.4R1-S2, EX4000 switches support virtual chassis.<br><br>[See Understanding EX Series Virtual Chassis.] |

## New EX4100-H Switches (EX Series)

We introduce the EX4100-H-12MP, EX4100-H-24MP and EX4100-H-24F industrial ruggedized switches. This is a convection-cooled, fanless switch, with an operational temperature range of −40°C through 75°C under various conditions. This temperature-hardened switch can be deployed inside enclosures (indoor or outdoor) with proper airflow. The switches are manufactured to operate reliably under extended temperature ranges. Some common examples where EX4100-H switches are deployed are smart cities and safe cities, transportation (outdoor or traffic signals), factory floors, defense networks (outdoors with extended temperature range) and so on.

- **External third-party 12 V PSU support on the EX4100-H-12MP switch** - From Junos 24.4R1-S2, the EX4100-H-12MP switch will support an external third-party 12 V PSU to power-on the switch. It is used in cases where there is no requirement for the switch to supply PoE. Junos OS monitors each PSU slot's feed status. Major CLI enhancements include:

  - New command `set chassis fpc fpc_slot ignore-poe-feed-status` to use a 12V-only third-party PSU and clear the Feed 54V not connected alarm.
  - `show chassis environment` displays PSU slot status.
  - `show chassis environment pem` displays individual power feeds.
  - `show chassis power-budget-statistics` displays the power budget based on available PSU PoE feeds.
  - `show chassis hardware` displays the PSU type.

  Additional features include PSU and temperature monitoring, N+1 power redundancy, and alarm triggers for temperature thresholds.

  [ See temperature-sensor, fpc (Chassis), and 12 V external PSU support on EX4100-H-12MP.]

**Table 3: Features Supported on EX4100-H Switches**

| Feature | Description |
|---|---|
| Access and authentication | • Support for 802.1X authentication.<br>[See 802.1X Authentication.]<br>• Support for captive portal authentication.<br>[See Captive Portal Authentication.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Chassis | • Support for environment monitoring, chassis and systems alarm management. Monitoring of power entry modules (PEMs) and board temperature sensors.<br>• *N*+1 power redundancy, online insertion and removal (OIR), and use of different PSU types (AC/DC) as part of PSU management.<br>• Monitoring of temperature and humidity sensors. Red alarms are raised when the temperature crosses the set threshold. Red or yellow alarms are raised when humidity crosses the set thresholds. The system shuts down when the board temperature sensors cross the set threshold. Use the `show chassis environment` and `show chassis alarms` commands to check these alarms.<br>• SNMP support.<br>• Support for dry-contact alarm.<br>• 12V-only PSU support (EX4100-H-12MP)— From Junos 24.4R1-S2, the EX4100-H-12MP device supports a 12V-only power supply unit (PSU) for system power-on and normal operation, excluding PoE features. Junos OS monitors each PSU slot's feed status. Major CLI enhancements include:<br>  • New command `set chassis fpc fpc_slot ignore-poe-feed-status` to use a 12V-only third-party PSU and clear the Feed 54V not connected alarm.<br>  • `show chassis environment` displays PSU slot status.<br>  • `show chassis environment pem` displays individual power feeds.<br>  • `show chassis power-budget-statistics` displays the power budget based on available PSU PoE feeds.<br>  • `show chassis hardware` displays the PSU type.<br>[See 12-V Only Power Supply Unit Support for EX4100-H-12MP, EX4100-H Chassis, and temperature-sensor.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Class of Service (CoS) | • Support for CoS configuration.<br><br>[See Junos OS CoS for EX Series Switches Overview.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| EVPN | • Support for EVPN-VXLAN group-based policies. You can use group-based policies (GBPs) for different levels of access control for endpoints and applications within the same VLAN. The switch also supports the GBP feature for locally switched traffic on VXLAN access ports.<br><br>[See Micro and Macro Segmentation using Group Based Policy in a VXLAN.]<br><br>• Support for the following Layer 2 VXLAN gateway services in an EVPN-VXLAN network:<br><br>  • 802.1X authentication, accounting, central web authentication (CWA), and captive portal<br><br>  • CoS<br><br>  • DHCPv4 and DHCPv6 snooping, dynamic Address Resolution Protocol (ARP) inspection (DAI), neighbor discovery inspection, IP and IPv6 source guard, and router advertisement (RA) guard (no multihoming)<br><br>  • Firewall filters and policing<br><br>  • Storm control, port mirroring, and MAC filtering<br><br>[See EVPN Feature Guide.]<br><br>• Support for Layer 3 VXLAN gateway in EVPN-VXLAN centrally routed bridging (CRB) overlay or edge-routed bridging (ERB) overlay networks on standalone switches or Virtual Chassis. The switch supports the following features:<br><br>  • Default gateway using IRB interfaces to route traffic between VLANs. [See Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network.]<br><br>  • IPv6 data traffic routed through an EVPN-VXLAN overlay network with an IPv4 underlay. [See Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| | • EVPN pure Type 5 routes. [See Understanding EVPN Pure Type-5 Routes.]<br><br>The Virtual Chassis doesn't support EVPN-VXLAN multihoming. You can use the standalone switch as an EVPN-VXLAN provider edge (PE) device in multihoming use cases. We support the following Layer 2 VXLAN gateway features in an EVPN-VXLAN network:<br><br>• Active/active multihoming<br><br>• Proxy ARP use and ARP suppression, and Neighbor Discovery Protocol (NDP) use and NDP suppression on non-IRB interfaces<br><br>• Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding<br><br>[See EVPN Feature Guide.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Hardware | • The EX4100-H-12MP has the following port configuration:<br>  • Four PoE++ enabled and MACsec-enabled RJ-45 Ethernet ports that support 100-Mbps, 1-Gbps, and 2.5-Gbps speeds.<br>  • Eight PoE++ enabled RJ-45 Ethernet ports that support 10-Mbps, 100-Mbps, and 1-Gbps speeds<br>  • Two 1/10GbE SFP+ stacking/uplink ports<br>  • Two 1/10GbE SFP+ MacSec-enabled uplink ports<br>• The EX4100-H-24MP has the following port configuration:<br>  • Eight PoE++ enabled RJ-45 Ethernet ports that support 100-Mbps, 1-Gbps, and 2.5-Gbps speeds<br>  • Sixteen PoE++ enabled RJ-45 Ethernet ports that support 10-Mbps, 100-Mbps, and 1-Gbps speeds<br>  • Four 1/10GbE SFP+ stacking/uplink ports<br>  • Four 1/10GbE SFP+ MacSec-enabled uplink ports<br>• The EX4100-H-24F has the following port configuration:<br>  • Twenty four 1 GbE SFP ports<br>  • Four 1/10GbE SFP+ stacking/uplink ports<br>  • Four 1/10GbE SFP+ MacSec-enabled uplink ports<br>[See EX4100-H Hardware Guide .] |
| High availability and resiliency | • Resiliency support for inter-integrated circuit (I2C), disk failure, and disk health.<br>[See High Availability User Guide.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Interfaces | • Network Interfaces Support -<br>  • EX4100-H-12MP supports three PICs. The PIC speeds are as follows:<br>  • PIC 0 with four 100-Mbps/1-Gbps/2.5-Gbps and eight 10-Mbps/100-Mbps/1-Gbps ports (downlink ports)<br>  • PIC 1 with two 1GbE/10GbE ports<br>  • PIC 2 with two 1GbE/10GbE ports (uplink ports)<br>  [See Port speed.]<br>  • EX4100-H-24MP and EX4100-H-24F support three PICs each, with the following speed configurations:<br>  • Twenty-four downlink ports (ports 0–23) on PIC 0:<br>  • EX4100-H-24MP—Eight 100-Mbps/1-Gbps/2.5-Gbps ports and sixteen 10-Mbps/100-Mbps/1-Gbps ports.<br>  • EX4100-H-24F—Twenty-four 100-Mbps/1-Gbps ports (10-Mbps, 100-Mbps, and 1-Gbps on tri-rate SFP optics).<br>  • Four stacking/network ports (ports 0–3) on PIC 1 that support 1-Gbps and 10-Gbps speeds.<br>  • Four uplink ports (ports 0–3) on PIC 2 that support 1-Gbps and 10-Gbps speeds.<br>  [See Network Interfaces for EX Series, Understanding HiGig and HGoE Modes in a Virtual Chassis, and Port Speed.]<br>• Perpetual and Fast PoE suport. EX4100-H supports PoE and PoE ++. If you enable perpetual PoE, power to the connected power device remains uninterrupted even when the switch is rebooting. Perpetual PoE and fast PoE are independent of each other and can coexist. When you power cycle the switch, fast PoE is applicable, if enabled. When you reload the switch through a |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| | Junos CLI reboot command, perpetual PoE is applicable, if enabled.<br><br>[See Understanding PoE on EX Series Switches.] |
| Junos telemetry interface | EX4100-H Series routers now allow subscription to the OpenConfig root resource path /state/chassis/ to export statistics for dry contact alarms and relative humidity sensors. The following paths are supported:<br><br>• For dry contact alarm sensors:<br>  • `/state/chassis/modules/module[name='FPC 0']/fpm/alarm-port/input-port[index='0']/`<br>  • `/state/chassis/modules/module[name='FPC 0']/fpm/alarm-port/input-port[index='1']/`<br>  • `/state/chassis/modules/module[name='FPC 0']/fpm/alarm-port/output-port[index='0']/`<br>• For humidity sensors: `/state/chassis/modules/module[name='FPC 0']/environment/sensors/sensor[name='Humidity Sensor 1']/`<br><br>For a complete list of sensors supported, see Junos YANG Data Model Explorer. |
| Layer 2 features | • Support for Layer 2 features.<br><br>[See Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation, Layer 2 Bridge Domains Overview, and Understanding Layer 2 Learning and Forwarding.]<br><br>• Support for Layer 2 multicast features.<br><br>[See Multicast Overview and Understanding Multicast Snooping.]<br><br>• Use the `interface-name` and `ip-address` options to configure the management address on the switch.<br><br>[See Configuring LLDP (CLI Procedure) .] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Layer 3 features | • Support for Layer 3 features and interior gateway protocols (OSPF, IS-IS, RIP, and ECMP) for IPv4 and IPv6.<br><br>[See Understanding OSPF Configurations and BGP Overview.] |
| MACsec | Support for Media Access Control Security (MACsec) in static connectivity association key (CAK) mode with GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 and GCM-AES-XPN-256 encryption.<br><br>[See Configuring MACsec.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Network management and monitoring | • Support for the following Ethernet OAM link fault management (LFM) and CFM features:<br>  • Monitor faults by using the continuity check message (CCM) protocol to discover and maintain adjacencies at the VLAN or link level.<br>  • Discover paths and verify faults by using the Link Trace Message (LTM) protocol to determine the path taken from an endpoint to a destination MAC address.<br>  • Isolate faults by using loopback messages.<br>[See Ethernet OAM and CFM for Switches and OAM Link Fault Management.]<br>• Support for IEEE 802.1ag CFM on service provider interfaces and Q-in-Q (point-to-point) interfaces.<br>[See Introduction to OAM Connectivity Fault Management (CFM).]<br>• Support for Juniper Mist Wired Assurance. Juniper EX4100 Series switches can be automatically on-boarded to the Juniper Mist Cloud using a single activation code, and the switch interfaces automatically provisioned. This is part of Wired Assurance, which provides automated operations and enables the use of service level expectations (SLEs) for IoT devices, Juniper Mist access points, and other network devices.<br>[See Juniper AI-Driven Enterprise and Overview of EX Series Switches and the Juniper Mist Cloud.]<br>• Support for:<br>  • Spanning-tree protocols. [See Spanning Tree Protocol Instances and Interfaces.]<br>  • sFlow network monitoring technology. [See sFlow Monitoring Technology.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| | • Local and remote port mirroring, and remote port mirroring to an IP address (GRE encapsulation). [See Port Mirroring and Analyzers.] |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| Software installation and upgrade | • Support for DHCP option 43 suboption 8 to provide proxy server information in phone-home client. During the bootstrapping process, the phone-home client (PHC) can access the redirect server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 to deliver the details of IPv4 and/or IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the **phc_vendor_specific_info.xml** or the **phc_v6_vendor-specific_info.xml** file located in the **/var/etc/** directory with the vendor-specific information.<br><br>Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client<br><br>• Support for phone-home client (PHC). The PHC can securely provision an EX4100 Virtual Chassis without the need for user interaction.<br><br>[See Provision a Virtual Chassis Using the Phone-Home Client.]<br><br>• Secure boot support to authenticate and verify the loaded software image while also preventing software-based attacks.<br><br>[See Secure Boot.]<br><br>• Support ZTP. Use zero-touch provisioning (ZTP) to install or upgrade the software on your device with minimal manual intervention.<br><br>[See Zero Touch Provisioning.]<br><br>• Support for SZTP. You can 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 the remote network device is accessed for initiating ZTP.<br><br>To enable mutual authentication, you need a unique digital voucher, which is generated based on the DevID (Digital Device ID or Cryptographic Digital Identity) of the network device. The |

**Table 3: Features Supported on EX4100-H Switches *(Continued)***

| Feature | Description |
|---|---|
| | DevID is embedded inside the Trusted Platform Module (TPM) 2.0 chip on the network device. Juniper Networks issues a digital voucher to customers for each eligible network device.<br><br>[See Secure Zero Touch Provisioning and Generate Voucher Certificate.] |
| Timing | • Support for Precision Time Protocol (PTP) transparent clock.<br><br>[See PTP Transparent Clocks.] |
| Uplink failure detection | • Support for debounce interval configuration. You can configure the debounce interval, which is the time (in seconds) that elapses before the downlink interfaces are brought up after a state change of the uplink interfaces.<br><br>You can configure the `debounce-interval` statement at the [`edit protocols uplink-failure-detection group` *`group-name`*] hierarchy level.<br><br>[See Uplink Failure Detection.] |
| Virtual Chassis | • Support for Virtual Chassis.<br><br>[See Understanding EX Series Virtual Chassis.] |

## Higher PoE budget (EX4400)

With the introduction of the EX4400-48MXP and EX4400-48XP switches, we now support up to 3600W of PoE power.

EX4400-48P, EX4400-24P, EX4400-24MP, and EX4400-48MP models already support up to 2200 W PoE budgets when powered by two 1600 W AC power supplies.

[See EX4400 Switch Hardware Guide].

## Dynamic Host Configuration Protocol

- **DHCP Snooping trusted mode support on a vlanVLAN (EX Series, QFX Series)**—Use the `trust-all` configuration option for DHCP snooping to configure all interfaces within a VLAN as trusted interfaces. This configuration enhances network security by ensuring that only trusted interfaces can relay DHCP messages, preventing unauthorized devices from acting as DHCP servers

- **DHCP Relay `no-snoop`(QFX Series)**—We introduce a new `no-snoop` knob that enables all DHCP unicast packets to be stopped from going to the CPU and only handle hardware forwarding.

  [See Understanding DHCP Relay `no-snoop`.]

## EVPN

- **Filter-based forwarding for GBP-tagged traffic (EX4100, EX4400, EX4650, and QFX5120)**—You can now forward traffic to a specified next hop if the group-based policy (GBP) tags assigned to that traffic match the GBP tags specified in the filter. Use this feature to apply different routing treatment between the specified tagged traffic and regular traffic.

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

- **Longest prefix match in IP-based GBP firewall filters (EX4100, EX4400, EX9204, EX9208, EX9214, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, and QFX5120)**—IP-based group-based policy (GBP) firewall filters now honor the best match rather than the first match. The order of IP address firewall terms in an IP-based GBP firewall filter is no longer relevant. Instead, the filter evaluates all IP address terms and selects the longest prefix match.

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

## J-Web

- **Support for EX4100-H-12MP switch (EX Series)**—You can configure, monitor, and manage EX4100-H-12MP switches using J-Web. To configure the EX4100-H-12MP switch, you must connect the Ethernet cable from the PC's Ethernet port to the port labeled **MGMT** on the switch's front panel. The chassis viewer on the Dashboard page supports both the standalone device view and the Virtual Chassis configuration view (graphical view of each member switch).

  [See Dashboard for EX Series Switches, Connecting and Configuring an EX Series Switch (J-Web Procedure), and Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure).]

- **Support for EX4400-48XP and EX4400-48MXP switches (EX Series)**—You can configure, monitor, and manage EX4400-48XP and EX4400-48MXP switches using J-Web. To configure these switches, you must connect the Ethernet cable from the PC's Ethernet port to the port labeled **CON** on the switch's rear panel. The chassis viewer on the Dashboard page supports both the standalone device view and the Virtual Chassis configuration view (graphical view of each member switch).

[See Dashboard for EX Series Switches, Connecting and Configuring an EX Series Switch (J-Web Procedure), and Configuring a Virtual Chassis on an EX Series Switch (J-Web Procedure).]

## Junos Telemetry Interface

- **Native sensor support for Layer 2 learning MAC table and MAC-IP table (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, EX4400-24P, EX4400-24MP, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48Y, and QFX5120-48Y-VC)**—Junos OS supports native telemetry data streaming for Layer 2 learning MAC and MAP-IP table sensors with Google protocol buffer (GBP) data encoding. You can create a subscription in PERIODIC or ON_CHANGE mode using Juniper's proprietary Remote Procedure Call (gRPC) service or gRPC Network Management Interface (gNMI). Use the resource path **/state/routing-instances/routing-instance/l2-learning/mac-table/** in a subscription to stream data. This feature is based on the new data model **junos-state-l2-learning.yang**.

  [See Junos YANG Data Model Explorer.]

- **Stream data from a device to a collector using basic Junos Telemetry Interface infra sensors and new component environment sensors—** Junos OS supports these new sensors:

  Relative humidity sensor-

  ```
  /components/component[name='FPC0']/properties/property[name='moisture']/
  ```

  Two input and one output dry contact sensors-

  ```
  /components/component[name='FPC0']/properties/property[name='alarm-port-output0']
  /components/component[name='FPC0']/properties/property[name='alarm-port-input0']
  /components/component[name='FPC0']/properties/property[name='alarm-port-input1']
  ```

  You can also display the dry contact and relative humidity information using the operational mode commands `show chassis environment` and `show chassis craft-interface`.

  [For state sensors, see Junos YANG Data Model Explorer.

## Layer 2 VPN

- **Loop detection for Layer 2 network (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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)**—We've expanded loop detection to Layer 2 (L2) networks, regardless of whether EVPN is configured or not. In earlier releases, we supported

enhanced loop detection only in EVPN-VXLAN networks. This feature detects the following types of Ethernet loops:

- A loop between two interfaces in different Ethernet segments (ESs). This loop is typically caused by miswiring fabric components.
- A loop between two interfaces with the same Ethernet segment identifier (ESI). This loop is typically caused by miswiring a third-party switch to the fabric.

To enable loop detection for a logical interface or for all logical interfaces, use the `loop-detect` statement at the `[edit protocols]` hierarchy level.

[See loop-detect.]

## Multicast

- **Limit unknown multicast traffic on multicast-router interfaces (EX Series)**—Limit the flooding of L2 multicast streams to multicast-router interfaces on a per VLAN or bridge domain level. Limit unknown multicast traffic by restricting the flooding of multicast data to the multicast-router interface based on IGMP or Multicast Listener Discovery (MLD) join messages to efficiently utilize bandwidth. To enable this feature, use the `no-flood-to-multicast-router-interfaces` configuration statement.

  In an Ethernet VPN (EVPN) environment, prevent unknown multicast streams from being sent to EVPN Provider Edges (PEs) by sending EVPN Type-3 routes with multicast extended community flags and IGMP/MLD snooping proxy flags set.

  [See Restrict Flooding of Unknown Multicast Traffic to the Multicast-router Interface in an L2 environment.]

- **Enhancement to L3 multicast operational commands (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, EX4650, MX960, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—The show instance command now extends to all routing instances for the following commands. Previously, only specific Protocol Independent Multicast (PIM)-enabled routing instances were displayed.

  - `show pim join instance all`
  - `show pim rps instance all`
  - `show pim statistics instance all`
  - `show multicast route instance all`
  - `show multicast statistics instance all`

  The `show pim statistics` output will display `V2 Sparse Join` and `V2 Sparse Prune` counters.

The `show igmp statistics` output will also display the `V1/V2/V3 Membership Query` field.

[See `show pim statistics`, `show multicast statistics`, and `show igmp statistics`.]

## 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.]

## 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.]

## Additional Features

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

- **Backup liveness detection on EVPN dual-homed peers** (EX9204, EX9208, and EX9214)

  [See Backup Liveness Detection on EVPN Dual Homing, node-detection (EVPN-VXLAN), and bfd-liveness-detection (EVPN Node Detection).]

- **EVPN loop detection** (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-12P, EX4100-H-12P-DC, EX4100-H-24F, EX4100-H-24F-DC, EX4100-H-24P, EX4100-H-24P-DC, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4600-VC, EX4650, and EX4650-48Y-VC)—We've added support for monitoring all VLANs on a logical interface with the `vlan-id all` configuration statement at the `[edit protocols loop-detect]` hierarchy level. This enhancement detects network loops across multiple VLANs and interfaces, improving network stability and performance.

  The listed devices show the following additional behavioral changes for this feature:

  - The `revert-interval` configuration is not effective for scale loop-detect sessions, making them non-revertive. You must issue the `clear loop-detect enhanced interface` command to clear the loop condition.

  - The receive statistics for loop-detect PDUs does not increment for scale loop-detect sessions during a loop condition.
  - Only a 1-second transmit interval is supported for scale loop-detect sessions.

  [See EVPN-VXLAN Lightweight Leaf to Server Loop Detection and loop-detect (EVPN).]

- **EVPN-VXLAN to EVPN-VXLAN seamless stitching for EVPN Type 5 routes** (EX9204, EX9208, and EX9214).

  [See Understanding EVPN Pure Type 5 Routes.]

- **Filter-based forwarding using group-based policy (GBP) tags tags** (EX4100-48P, EX4400-48F, EX4650, and QFX5120-48T).

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

- **Support for additional firewall matches** (EX4100-24P and EX4400-48F). We've added support for the `source-port`, `destination-port`, `ip-source-address`, `ip-destination-address`, `source-prefix-list`, and `destination-prefix-list` firewall filter match conditions for egress port firewall filters and egress VLAN firewall filters. You must use the `egress-l2-extended-match` configuration statement to enable these firewall filter match conditions.

  [See egress-l2-extended-match.]

- **Supported transceivers, optical interfaces, and DAC cables (EX Series and QFX Series)**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **PoE and PoE++ support** (EX4100-H-12MP)—We have added PoE and PoE++ features in EX4100-H-12MP. If the perpetual PoE is enabled, power to the connected power device (PD) remains uninterrupted even when the PSE switch is rebooting. Perpetual PoE and Fast PoE are independent to each other and can co-exist. When the switch goes for power cycle, Fast PoE will be applicable, if enabled. When switch goes for reload through Junos CLI reboot command, Perpetual PoE will be applicable, if enabled.

  [See Understanding PoE on EX Series Switches.]

- **AR integrated with OISM in an EVPN-VXLAN ERB fabric** (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48MXP, EX4400-48XP, EX4400-48P, and EX4400-48T).

  - We support AR with OISM on these devices only with VLAN-based and VLAN-aware MAC-VRF EVPN instances.
  - You can configure the AR leaf role on these devices when they are also acting as OISM border leaf or server leaf devices.

- You can configure the standalone AR replicator role on other devices in the EVPN-VXLAN network that support the AR replicator role.

[See Assisted Replication Multicast Optimization in EVPN Networks and Optimized Inter-Subnet Multicast in EVPN Networks.]

## What's Changed

**IN THIS SECTION**



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

## EVPN

- EVPN system log messages for CCC interface up and down events—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file `/var/log/syslog`.

## Forwarding and Sampling

- Support added for interface-group match condition for MPLS firewall filter family.

## General Routing

- Non-revertive switchover for sender based MoFRR—In earlier Junos OS releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, that is, traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  [See min-rate.]

- For MPC5E line card with flexible-queuing-mode enabled, queue resources are shared between scheduler block 0 and 1. Resource monitor CLI output displays an equal distribution of the total available and used queues between scheduler blocks. This correctly represents the queue availability to the Routing Engine.

  [See show system resource-monitor and show system resource-monitor ifd-cos-queue-mapping fpc.]

- Change to the commit process—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

  [See Commit Preparation and Activation Overview.]

- Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json` command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and the PyEz displays all the duplicate keys with the enhanced tags.

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- Support added for interface-group match condition for MPLS firewall filter family.

- **Change to the commit process**—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

  [See Commit Preparation and Activation Overview.]

- **Option `allow-transients` is set by default for the EZ-LAG commit script**—The EZ-LAG feature simplifies setting up EVPN multihoming configurations using a set of configuration statements and a commit script. The commit script applies transient configuration changes, which requires the `allow-transients` system commit scripts option to be set. Now the default system configuration sets the `allow-transients` option at the EZ-LAG commit script file level, removing the need to set this option manually. In earlier releases where this option isn?t set by default, you must still configure the option explicitly either globally or only for the EZ-LAG commit script.

  [See Easy EVPN LAG Configuration Overview.]

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## Routing Protocols

- Update to IGMP snooping membership command options— The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not

visible when ? was issued to view all possible completions for the `show igmp snooping membership` command.

[See show igmp snooping membership.]

- MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)— The `source-address` configured for `proxy` and `l2-querier` under the `[mld-snooping]` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier".

  [See source-address.]

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

## 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.

## EVPN

- After a reboot during recovery process, the ESI LAGs come up before the BGP sessions, and routes or ARP entries are not synchronized. PR1487112

## General Routing

- On all platforms running Junos OS or Junos OS Evolved, in a Q-in-Q environment, if xSTP is enabled on an interface that has a logical interface with vlan-id-list configured, then, it will only run on those logical interfaces whose vlan-id range includes native-vlan-id configured. All other xSTP will be in discarding state. This might lead to traffic drop. PR1532992
- Tail drop is seen in WRED configuration statistics. PR1549910

## Interfaces and Chassis

- **Support for low power idle mode (EX4400-48T, EX4400-48P, EX4400-24T, and EX4400-24P)**— Starting in Junos OS Release 21.1R1, the 1-Gbps or 100-Mpbs port switches to low power idle (LPI) mode based on the following conditions:.

  When a port operates at 1-Gbps speed and no traffic is either received or transmitted, then the port enters LPI mode. If the 1-Gbps port transfers unidirectional or bidirectional traffic, then the port will not enter LPI mode.

  When a port operates at 100-Mbps speed, the port switches to LPI mode, based on the direction of the traffic. The `show interfaces interface-name extensive` command displays `RX LPI` when there is no RX traffic and `TX LPI` when there is no TX traffic.

  You can view the interface that is in LPI mode by executing the `show interfaces interface-name extensive` command. The output field `IEEE 802.3az Energy Efficient Ethernet` displays the status of the LPI mode.

  [See show interfaces extensive .]

## User Interface and Configuration

- Unsupported options can be seen under "restart" command. PR1545558
- Python script is not supported in ZTP workflow. Python can run (during ZTP) only in few QFX Series based flex images. PR1547557

## Open Issues

IN THIS SECTION



1845365

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

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- When TISSU is upgraded from Junos OS 22.4 release and later, the box come up as backup Routing Engine. PR1703229
- Carrier tranistions is not setting properly for channelized ports on non-DUT Lagavulin for QSFP28-100G-AOC-30M 740-064980 of FINISAR. PR1723924

- 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-VC. PR1745855
- EX4300MP: VC member status toggling between "Inactive" and "NotPrsnt" state after member downgradePR1751871
- "Error:tvp_optics_eeprom_read: Failed to read eeprom for link" logs might be seen for some time during system reboot or pfe restart in EX3400. There is no functional impact due to these logs.PR1757034
- During device reboot, mge connected ports on the peer goes up after 90s into reboot. PR1767347
- 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
- Local/Remote fault insertion from TG is failing. PR1789999
- 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
- Third party (BRCM) vendor api bcm_plp_mode_config_get returning error code of phy unavailability for pic 0 mgig phy during phy init. No Functional impact. PR1812228
- Autoneg error log observed in case of jack-out followed by jack in(JiJO) of SOURCE PHOTONICS and 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 between SFP-T and switch that is, PHY82756 does not 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 Junos OS QFX Series and EX Series platforms in an EVPN-VXLAN Centrally-Routed Bridging (CRB) scenario where the ingress leaf switch is configured with ESI (Ethernet Segment Identifier) lags (that is, the server is multihomed), if there is an overlap between ESI lag(s) trunk ID with physical port number(s) and overlap of destination MAC (DMAC) between virtual gateway address (VGA) MAC address 00:00:5e:00:01:01 (CRB setup with VGA / GW is on spine) with Virtual Router Redundancy Protocol (VRRP) MAC (specifically for the VRRP group 1 MAC address 00:00:5e:00:01:01) on the physical ports of the Leaf switches, then traffic loss will be observed for the inter-VLAN traffic.PR1820830

- On a working VC system, if a dc-pfe process restarts for any reasons, then there is a possibility of some interfaces not getting created after the dc-pfe restart.PR1823688
- 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. For this to happen, a speed mismatched configuration is needed, where a 1G speed or a 25G speed is configured on the PIC 2. PR1831409
- 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
- PEM mismatch alarms are cleared from the master after rebooting a Virtual Chassis member containing an unsupported mixed AC/DC PSU combination. PR1845365
- On all Junos OS platforms when speed is changed on an interface which is part of aggregated Ethernet bundle, interface will be removed and added with the updated speed. When some other operation such as interface disable is configured along with speed change on the interface in the same commit, then the interface is not removed and added to the bundle, it can cause other aggregated Ethernet interfaces flap and traffic drop.PR1845370
- Baseline configuration commit will take more time when the device has 256000 MAC configurations configured under groups.PR1845657
- FXPC core file is seen intermittently during device reboot operation. No functional impact is seen on generating FXPC core file. PR1855408
- PCT: Commit error seen while configuring system syslog host with routing instance. PR1850071
- On Junos OS platforms, the standby router goes into the error state when switchover is performed. This will not impact the traffic. PR1847307

## High Availability (HA) and Resiliency

- GRES is not supporting 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

- Management interface does not get IP even if the interface is bound .This issue is seen when a powercycle is triggered and service can easily be restored by restarting dhcp-service. CLI command to restart dhcp service is `restart dhcp-service`. PR1854827

## Platform and Infrastructure

- Upgrading EX4300 switches from Junos OS 21.2R3-SX to 21.4R3-SX might 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. PR1794342

## Routing Protocol

- CLI /RPC `show bgp group rib-sharding all` or `get-bgp-group-information` failure with XML CRITICAL ERROR and ODL validation failure. PR1826803

## 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.

## EVPN

- Error messages are observed after performing a VLAN name change with EVPN configuration PR1806660

## Forwarding and Sampling

- The fxpc process crashes on Junos OS platforms when VLANs are deleted and configured. PR1831770

## General Routing

- A few line cards will be stuck in the 'Present' state and later go 'Offline'. PR1631579
- When TISSU upgrade is done from Junos OS 22.4 release and later, the box come up as backup Routing Engine.PR1703229
- The port class is not captured in cint trace output for individual ports. PR1786399
- Master FPC taking 20 sec time to shut backup FPC's network port after backup FPC reboot in a VC set-up PR1788328
- [EX3400] LX/FX SFP Swap leads to traffic drop. PR1794986
- ARP won't be forwarded in VLAN associated VNI in VxLAN Fabric. PR1801237
- The default port behaviour is not working as expected after deleting VOIP (Voice over IP) configuration on an access interface PR1802455
- On EX4300-MP platforms in non-mixed VC mode, when the VC connection is established between the platforms, the ports don't pass traffic, which leads to minimum traffic loss.PR1805100
- Interfaces remain down on EX4400-48F platform after replacing a 100MB SFP with 1GB SFP. PR1805370

- When VC-mode is set to HGOE and converting port type from vc-port to network port, traffic loss is observed PR1806262
- Hot swapping 1G SFPT optics ports are not coming up. PR1810482
- Breakage in the CLI `show forwarding-options load-balance source-address X destination-address X source-port X destination-port X` on VMX/MX480/MX960. PR1810653
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario PR1812482
- The output of `show chassis routing-engine` does not show the standard documented outputs after a reboot event or a GRES event. PR1812514
- When frames above 9080 bytes are sent across interfaces with 10m/100m speed between EX4300-MP, then we start seeing traffic loss even at 6M to 8Mbps rate. PR1812891
- Multi-rate Gigabit Ethernet (mge) port on EX4100 and EX4400 platforms does not receive or forward traffic. PR1814093
- Wrong PSU state is updating in the mist. PR1814463
- When power devices (PDs) are connected to all the power over ethernet (PoE) ports with LLDP enabled, the last port is not powered up. PR1814715
- DHCP snooping issue is observed on access ports with IRB and VXLAN configuration. PR1816445
- For Junos OS platforms, the OSPF neighborship gets stuck in EXSTART state after performing NSSU. PR1817034
- The l2ald crash is observed when adding scaled EVPN-VXLAN configuration on Junos OS platforms. PR1817705
- Switch port status is changed to unauthorized, when a supplicant client attempts to authenticate using 802.1X standard with EAP-TLS certificate. PR1819462
- L2TP processing issue on EX Series and QFX Series platforms with tagged CDP VTP and UDLD frames. PR1821012
- All Junos and Junos Evolved platforms the RAIDUS (Remote Authentication Dial-In User Service) attribute NAS-Port-Type which specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber is missing in the authentication attempt.PR1822101
- Intermittent alarms related to fan overspeed value can be observed on EX4100 platform. PR1822363
- MAC address learning fails when Flexible Ethernet Services Encapsulation is enabled on Junos QFX5K and EX4K platforms after a reboot. PR1822608

- dfw ERROR is seen whenever collecting RSI. PR1823280
- EX4400-48MXP/48XP CPU hog by thread CMQFX and task ACQUIRE_FP_LOCK during PIC offline and online. PR1823394
- While performing a 4x25g channelization configuration on the 1x100GE PIC, certain error logs are printed multiple times. PR1823743
- In virtual-chassis after routing-engine switchover traffic of type 5 routes of EVPN-VXLAN are not getting forwarded PR1823764
- Restricted proxy ARP feature does not work as expected. PR1824023
- Rebooting one linecard or FPC will cause the virtual-chassis on the EX4K and QFX5K devices to forward traffic in backup RTG interface PR1824750
- EX4400 series: Offline and then an online of PIC 2 installed with a 1x100GE Uplink module configured for virtual-chassis link causes the link to remain down PR1826147
- On all EX4400 platform, all time sensitive protocols are getting flapped due to process call getting stuck in System Management Bus (SMBus).PR1826615
- Even though installed the license to both primary and secondary, alarm LED might be lit with yellow on backup. PR1827641
- EX4400-48MP ping rapid count with high values stops when phone-home is configured. PR1828735
- The dot1x client does not get authenticated and gets stuck in the connecting state when a new dot1x profile is assigned along with a newly created VLAN PR1830067
- Commit error on using more than 31 characters authentication-key-chain-name. PR1830395
- 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
- On Junos EX platforms, the PFE's (Packet Forwarding Engine) handling of NEWSYSLOGD signals during UKERN file archiving is inefficient, leading to repeated memory allocations and subsequent memory leaks.PR1831813
- On Junos EX4100 and EX4400 platforms, switch core dump when user commits a command to ignore a "power entry module" alarm. PR1833698
- On EX Series platforms with AP45 connected to MGE interfaces, the interfaces are not working after upgrading to 23.4 R2-S2.1. PR1836616
- On Junos EX4100, EX4400, EX4650 and QFX5120 platforms, in an Ethernet VPN Virtual Extensible LAN (EVPN-VXLAN) setup, when GBP (Group Based Policy) is configured with 'ingress-enforcement'

a delay is observed in GBP installation after device reboot or link with ESI (Ethernet Segment Identifier) flaps. This leads to traffic disruption until the policy is installed.PR1839916

- PFE process crash is observed when web-management is not configured in a CWA setup. PR1840988
- On Junos EX4400-48F platform, specific to the EX4400-48F (ports 0-35) SKU, not applicable to any other SKU (Stock Keeping Unit) , where SFP-100BASE-BX10 optics are used between two EX4400-48F ports, traffic blockage occurs. The link comes up, but no traffic (e.g., ping) passes through.PR1843585
- On EX4100 platforms,When deactivating/activating IRB interfaces on vlans with vni enabled, error message will be observed.PR1846286
- On Junos platforms, specifically on EX and QFX series aggregated interfaces configured without address-family results in reachability issues.PR1847159
- Since 1G is also a default speed for 10G uplink modules after the mix speed mode commit, this change was needed.PR1848338
- In EX4100-H-12MP/EX4100-H-24MP: PoE ports will go down when below operations are performed 1. PSU removal with any PSU (AC or DC) combination from slot 0 or 2. Insert only PSU (AC/DC) in slot 1 and slot 0 to be emptyPR1855409
- On Junos OS EX4000 and QFX5120 platforms, the system fails to retrieve the necessary analyzer details. This prevents the port mirroring action from being applied in the filter entry. Consequently, the system defaults to the reject action, causing the traffic to be dropped, and packet captures do not appear.PR1856361

## J-Web

- Reload or refresh the Jweb page showing the "Empty reply from server" error. PR1832731

## Layer 2 Ethernet Services

- Switch provisioned via ZTP going unreachable due to DHCP misbehaviour on upgrading to Junos OS Release 21.4R3-S6. PR1808289
- DHCP relay option "allow-server-change" does not work as expected in trusted server group PR1833148

- Unable to assign an IP address on management interface with DHCP configuration even if DHCP is bound after a power cycle. PR1854827

## Platform and Infrastructure

- RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596). PR1802329
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos OS platforms PR1826666
- An Authentication Bypass by Spoofing vulnerability in the RADIUS protocol of cRPD 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.PR1826678
- [EX4000] user root is shown as incorrect after powercycle of the device. PR1855393

## Routing Protocols

- Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511). PR1815253

## Subscriber Access Management

- authd process crashes when radius-server-name is configured. PR1818321

## User Interface and Configuration

- The mgd process crashes while using an FQDN in conjunction with the ephemeral configuration database. PR1825728

# 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**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 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**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 |

Table 5: EOL and EEOL Releases *(Continued)*

| Release Type | End of Engineering (EOE) | End of Support (EOS) | Upgrade/ Downgrade to subsequent 3 releases | Upgrade/ Downgrade to subsequent 2 EEOL releases |
|---|---|---|---|---|
| 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

IN THIS SECTION

Learn about new features introduced in this release for Juniper Secure Connect.

## VPNs

- **Juniper® Secure Connect integration with JIMS (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The SRX Series Firewalls can send Juniper Secure Connect's remote access VPN connection state events to Juniper® Identity Management Service (JIMS) using the push to identity management (PTIM) solution. By default, Junos OS enables this feature when you use `identity-management` at the `[edit services user-identification]` hierarchy level.

  You can use the following options to configure this feature:

  - `no-push-to-identity-management` at the `[edit security ike gateway` *`gateway-name`* `aaa]` hierarchy level to disable the iked process communication with JIMS.

  - `user-domain` at the `[edit security remote-access profile` *`realm-name`* `options]` hierarchy level to optionally configure the domain alias name.

  See [Juniper Secure Connect Integration with JIMS, identity-management, and profile (Juniper Secure Connect).]

- **SAML-based user authentication in Juniper® Secure Connect (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Juniper Secure Connect remote access VPN supports user authentication using Security Assertion Markup Language (SAML) version 2. To perform the remote user authentication using SAML, run the VPN service using the iked process on your firewall and ensure you have the SAML-supported Juniper Secure Connect application.

  Configure SAML service provider and identity provider settings at the `[edit access saml]` hierarchy level. Enable SAML settings in the access profile configuration using the `set access profile` *`profile-name`* `authentication-order saml` command.

  See [SAML Authentication in Juniper Secure Connect, saml, authentication-order (access-profile), saml (Access Profile), saml-options, show network-access aaa saml assertion-cache, show network-access aaa statistics, request network-access aaa saml load-idp-metadata, request network-access aaa saml export-sp-metadata, clear network-access aaa saml assertion-cache, clear network-access aaa saml idp-metadata, and clear network-access aaa statistics.]

## What's Changed

IN THIS SECTION



Learn about what changed in this release for Juniper Secure Connect.

## VPNs

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon` *`name`* `term` *`name`* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (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 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 24.4R1, click the group by release link. You can collapse and expand the list as needed.

- MX150
- MX204
- MX240
- MX304
- MX480
- MX960
- MX2008
- MX2010
- MX2020

- MX10003
- MX10004
- MX10008
- MX10016
- vMX

## Chassis

- **Enabling runtime hot-swap of LMICs (MX304)**—We support graceful insertion and removal of line-card MICs (LMICs) on the MX304 device during runtime. You can use the new CLI command `set chassis fpc slot mic slot power off` to power off the MIC. You can power on the MIC by deleting this power-off configuration. Power management operations on multiple LMICs occur sequentially. To view the MIC status, you can use the new command `show chassis fpc mic-status`.

  [See fpc (Chassis), request chassis mic, show chassis fpc, and show chassis hardware.]

- **Runtime hot-swap of LMICs allows monitoring services to gracefully stop and restart (MX304)**—Monitoring services such as inline active flow monitoring, inline monitoring services, video monitoring, Routing-Engine-based sampling, and FlowTapLite gracefully stop when you take the Packet Forwarding Engine offline and replace the line-card MIC (LMIC). These services gracefully become operational again after you've replaced the LMIC and brought the Packet Forwarding Engine back online. You can use the new CLI command `set chassis fpc slot mic slot power off` to take the Packet Forwarding Engine offline. You can bring the Packet Forwarding Engine back online by deleting this power-off configuration.

  [See fpc (Chassis), request chassis mic, show chassis fpc, and show chassis hardware.]

- **Effects of runtime hot-swap of LMICs on port mirroring (MX304)**—Hot-swapping line-card MICs (LMICs) causes the Packet Forwarding Engine to go offline and come back online again. Port mirroring reacts to the hot-swap of LMICs in the following ways:

  - If the Packet Forwarding Engine hosting the output mirroring destination interface (MDI) goes offline, traffic from the input mirroring interface is not mirrored. Mirroring resumes when the Packet Forwarding Engine hosting the MDI comes back online.

  - In a port-mirroring next-hop-group or next-hop-subgroup scenario, if a Packet Forwarding Engine hosting MDIs goes offline, the MDIs associated with the offline Packet Forwarding Engine are pruned from the member list. Those associated MDIs are added back to the member list when the Packet Forwarding Engine hosting the MDIs comes back online.

  - If the Packet Forwarding Engine hosting the mirroring interface goes offline, traffic entering, leaving, and mirrored at the interface stops. Ingress and egress mainline traffic and mirroring resume when the Packet Forwarding Engine hosting the mirroring interface comes back online.

[See fpc (Chassis), request chassis mic, show chassis fpc, and show chassis hardware.]

- **Optics EM policy support (MX10004 and MX10008)**—The Junos Environment Monitoring (EM) policy now includes optics temperature sensors for MX10004 and MX10008 routers with MX10K-LC9600 line card. The policy includes the following features:

  - The Optics EM policy incorporates periodically polled temperature readings of optical modules in the system to automatically manage the fan speed
  - Junos OS will automatically trigger optics shutdown for 100GbE and 400GbE optics when the Fire Shutdown threshold is breached. Auto-recovery is not supported for optics disabled by the EM policy. To re-enable the optics, use the `request interface optics-reset` command or perform soft optics insertion and removal (OIR).
  - The Optics EM policy is enabled by default on all 100GbE and 400GbE optics that are Multi-source Agreements (MSA) compliant and support diagnostic EEPROM with temperature monitoring. This policy is not applicable for loopback optics and direct attach copper (DAC) cables.

  To disable EM policy, use the following CLI command:

  - `set chassis fpc fpc_slot pic pic_slot port port_no no-temperature-monitoring`

    It explicitly disables the EM policy on specific WAN ports.

  To view temperature threshold values and fan speed, use the following CLI commands:

  - `show chassis temperature-thresholds` displays the optics temperature threshold values.
  - `show chassis environment` displays the optics temperature.
  - `show chassis fan` displays the fan status and speed

  [See temperature-sensor.]

- **Low-power mode environment monitoring policy profile for noise reduction (MX10004 and MX10008)**—We provide support to reduce the operational noise levels when you use 100GbE ports on MX10004 and MX10008 devices with the LC9600 line card installed. With this feature, you can maintain low device noise levels without compromising cooling efficiency. Use the `set chassis fpc-empolicy-profile low-power-mode` command to enable this feature. You can then use the `show chassis temperature-thresholds` or `show chassis fan` command to view the updated fan speed details.

  [See Low-Power Mode EM Policy Profile for Noise Reduction.]

- **Source Redundancy and Feed Redundancy support (MX10004 and MX10008)**—We provide N+1 power redundancy support on MX10004 and MX10008 routers with the JNP10K-PWR-AC3H power supply modules (PSMs). You can enable either source redundancy or feed redundancy for the PSM.

[See Power Redundancy for Third-Generation Power Supply Modules.]

- **Resiliency support (MX10004 and MX10008)**—We support resiliency for JNP10K-PWR-AC3H power supply modules (PSMs) on MX10004 and MX10008 devices. Resiliency enables the system to monitor component health, alert you of errors, and take appropriate action to restore normal operation based on error severity.

  [See Resiliency, thermal-health-check, and watchdog (PSM).]

## Connected Security Distributed Services (CSDS) Architecture

- **CSDS Architecture (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The Connected Security Distributed Services (CSDS) Architecture delivers a scalable, distributed security architecture design that fully decouples the forwarding and security services layers. In this design, MX Series routers serve as intelligent forwarding engines for load balancing while SRX Series Firewalls help expand your data centers securely. The solution supports carrier-grade NAT (CGNAT), IPsec VPN, and stateful firewall security services.

  The architecture ensures redundancy in forwarding and services layers. It uses ECMP-based consistent hashing for the routers, and Multinode High Availability for the physical and virtual firewalls.

  You can manage nodes with Junos Node Unifier (JNU) and orchestrate vSRX Virtual Firewalls with Junos Device Manager (JDM).

  [See Connected Security Distributed Services Architecture Deployment Guide, and Release Notes: Connected Security Distributed Services Architecture.]

- **Junos Node Unifier support in CSDS for unified CLI management (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—We support centralized management of devices in the Connected Security Distributed Services (CSDS) Architecture with the Junos Node Unifier (JNU) single-touchpoint solution. The JNU topology uses MX Series routers as JNU controllers, and SRX Series Firewalls and Junos Device Manager (JDM) as JNU satellites. From the controller, you can perform the following operations on the satellites:

  - Configure and manage the nodes using Junos OS configuration commands.
  - Run Junos OS operational mode commands.

  [See Junos Node Unifier for CSDS, request jnu satellite sync, show chassis jnu satellite, and jnu-management.]

## Content Security

- **Increased source IP prefix limit and HTTPS traffic control (MX480, MX960, and MX2020 with MX-SPC3 service card**—Increase the limit of source IP prefixes from 10 to 48 to include a broader range

of subscriber source IP addresses in web content filtering policies. This update enhances flexibility and control over web content filtering, enabling more precise access management. Additionally, use a new CLI command `disable-https-filtering` to allow specific HTTPS traffic to bypass the default TCP-Reset behavior, offering customization of web filtering settings. The default behavior remains unless configured otherwise.

[See URL Filtering Overview .]

## EVPN

- **Longest prefix match in IP-based GBP firewall filters (EX4100, EX4400, EX9204, EX9208, EX9214, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, and QFX5120)**—IP-based group-based policy (GBP) firewall filters now honor the best match rather than the first match. The order of IP address firewall terms in an IP-based GBP firewall filter is no longer relevant. Instead, the filter evaluates all IP address terms and selects the longest prefix match.

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

- **XML-based support information (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You now have the option of providing xml-based output of the "reqeust support information evpn-vxlan" command. You can do so from the CLI using `request-support-information evpn-vxlan-xml | gzip > <filename>`.

  [See request support information.]

## High Availability

- **ISSU support for MIC (MX240, MX480, MX960, and MX2020)**—You can use in-service software upgrade (ISSU) to ensure seamless Modular Interface Card (MIC) upgrades on the listed MX Series routers. This feature upgrades the system with minimal traffic disruption and no impact on the control plane. MICs support 10 1GbE or 10 10GbE interfaces, ensuring flexibility and reducing downtime during upgrades, while maintaining system stability and performance across these chassis models.

- **S-BFD support for SRv6 TE paths (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You can enhance continuity checks for SRv6 traffic engineering (TE) paths by configuring Seamless BFD (S-BFD). S-BFD sessions monitor the state of SRv6 paths, ensuring that paths remain active only when S-BFD sessions are up.

  You can configure S-BFD by using the `sbfd` configuration statement at the `[edit protocols source-packet-routing source-routing-path` *`name`* `primary` *`name`* `bfd-liveness-detection]` hierarchy level. You can also use the `destination-ipv6-local-host` option for the `sbfd` statement to enforce the use of an IPv6 local host address for S-BFD responders that support only IPv6 local host addresses.

  [See sbfd]

## Junos OS API and Scripting

- **API traffic statistics for PRPD flex routes (MX304, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You can view detailed traffic statistics for programmable RPD (PRPD) flex routes within the RouteGetStats API. The output and behavior of the API mirror Junos OS CLI output and behavior when you use the `show programmable-rpd statistics flex-routes` command.

  [See show programmable-rpd statistics.]

## Junos Telemetry Interface

- **OpenConfig sensor support for ZR and ZR+ optical transceivers on MPC10 line cards (MX2010 and MX2020)**—Junos OS supports data streaming new leaves for ZR and ZR+ optics. You can create a subscription in INITIAL_SYNC or TARGET_DEFINED mode using Juniper's proprietary Remote Procedure Call (gRPC) service or gRPC Network Management Interface (gNMI). Use these resource paths in a subscription to stream data:

  - **/components/component/transceiver/state/** new leaves `fec-mode`, `fec-status`, `module-functional-type`, `fault-condition`, `fec-uncorrectable-blocks`, and `fec-corrected-bits`
  - **/components/component/transceiver/physical-channels/channel/state/** new leaves `output-frequency` and `associated-optical-channel`
  - **/components/component/optical-channel/state/** leaves `frequency` and `line-port`

  This feature is based on data models **openconfig-terminal-device.yang** (version 1.8.0), **openconfig-platform-transceiver.yang** (version 0.8.0), and **openconfig-transport-types.yang** (version 0.14.0).
  [For sensors, see Junos YANG Data Model Explorer. For CLI operational mode commands, see show interfaces diagnostics optics (Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, 100-Gigabit Ethernet, and Virtual Chassis Port) and show interfaces extensive.]

- **Backup next-hop group sensor support (MX960)**—You can use this feature to send telemetry data for the backup next-hop group from your device to the collector. The feature supports streaming and ON_CHANGE subscriptions through Juniper's proprietary Remote Procedure Call (gRPC) or gRPC Network Management Interface (gNMI). Enable the feature by adding the `backup-next-hop-group` configuration statement at the `[edit system fib-streaming model ocaft]` hierarchy level.

  Removing this configuration disables the feature:

  ```
  delete system fib-streaming model ocaft backup-next-hop-group
  ```

  [See Configuring Prefix Filtering, prefix-list, show fib-streaming state, and Junos YANG Data Model Explorer.]

- **Stream data from a device to a collector using basic Junos Telemetry Interface infra sensors and new component environment sensors—** Junos OS supports these new sensors:

Relative humidity sensor-

```
/components/component[name='FPC0']/properties/property[name='moisture']/
```

Two input and one output dry contact sensors-

```
/components/component[name='FPC0']/properties/property[name='alarm-port-output0']
/components/component[name='FPC0']/properties/property[name='alarm-port-input0']
/components/component[name='FPC0']/properties/property[name='alarm-port-input1']
```

You can also display the dry contact and relative humidity information using the operational mode commands `show chassis environment` and `show chassis craft-interface`.

[For state sensors, see Junos YANG Data Model Explorer.

## MACsec

- **MACsec authentication and encryption (MX10004 and MX10008)**—You can enable MACsec on links connecting switches or routers using certificate-based authentication and encryption. Connected devices can mutually authenticate using 802.1X over Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) and dynamically derive the connectivity association key (CAK) for encryption. This configuration enhances security by ensuring that only authenticated devices can communicate and that data is encrypted during transmission.

  [See Understanding Media Access Control Security (MACsec).]

## MPLS

- **MPLS Support on IRB Interfaces (MX240, MX304, MX480, MX960, MX10004, and MX10008)**—With MPLS support for Integrated Routing and Bridging (IRB) interfaces, you can integrate routing and switching over an MPLS core. Us this feature to enhance traffic forwarding, support VLAN-based routing, and maintain MPLS label switching. Optimize path selection, reduce forwarding delays, and ensure compatibility with complex MPLS topologies.

  Previously, MPLS encapsulation was not supported on IRB interfaces. Now, IRB interfaces can encapsulate MPLS labels, ensuring interoperability and full MPLS functionality.

- **SRv6-TE tunnels with micro-SIDs in PCEP (MX960)**—Enhance traffic engineering and network optimization by enabling the reporting, delegating, and creatingcreating SRv6-TE tunnels with micro-SID configurations tunnels. You can report and delegate static SRv6-TE tunnels with micro-SID configurations to a PCE and initiate these tunnels through PCE, improving control and management. Key functionalities include reporting static SRv6-TE tunnels with micro-SIDs to the PCE, delegating

their management, and creating them with proper SID structure and endpoint behavior checks. Extended CLI commands support these features, facilitating effective configuration and monitoring.

[See SRv6-TE Tunnels with micro-SIDs in PCEP.]

## Multicast

- **Enhanced MVPN provider tunnel selection criteria (MX Series)**—We support the following enhanced MVPN provider tunnel selection criteria to fine tune multicast path-selection across the core network.
  - Regular Expression for selecting RSVP tunnels for ingress replication.
  - Colored inet.3 table for ingress replication.
  - Root Address for MLDP P2MP tunnels.

  [See Provider Tunnel Selection In Ingress Replication.]

- **Enhancement to L3 multicast operational commands (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, EX4650, MX960, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—The show instance command now extends to all routing instances for the following commands. Previously, only specific Protocol Independent Multicast (PIM)-enabled routing instances were displayed.
  - `show pim join instance all`
  - `show pim rps instance all`
  - `show pim statistics instance all`
  - `show multicast route instance all`
  - `show multicast statistics instance all`

  The `show pim statistics` output will display `V2 Sparse Join` and `V2 Sparse Prune` counters.

  The `show igmp statistics` output will also display the `V1/V2/V3 Membership Query` field.

  [See `show pim statistics`, `show multicast statistics`, and `show igmp statistics`.]

## Network Address Translation (NAT)

- **Monitor subscriber port utilization (cSRX, MX240, MX480, MX960, SRX1500, SRX1600, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX3.0)**–You can monitor and manage port utilization when deploying Carrier Grade Network Address Translation (CGNAT).

Configure threshold limits to receive notifications when port or port block usage exceeds the configured thresholds.

- If a pool is configured as Port Block Allocation (PBA) and a subscriber uses more port blocks than the threshold, a notification is generated.
- For Deterministic NAT (DETNAT) pools, if a subscriber uses more ports than the threshold in the allocated block, a notification is generated.

The system log messages are:

- RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_RAISE: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 90%, current: 100%`
- RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 50%, current: 25%`
- RT_SRC_NAT_SUBS_POOL_ALARM_RAISE

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING: Subscriber IP: 10.1.1.2, NAT pool: pool-name, threshold alarm [raise, clear] suppressed for 2 times in last 10 seconds`

[See jnxJsSrcNatSubThresholdStatus, jnxJsNAT, Monitor Subscriber Port Utilization Using Carrier Grade NAT, subscriber-pool-utilization-alarm, and pool-utilization-alarm (Security Source NAT Pool).]

- **Distinct NAT ports for the same IP address on PCP and DS-Lite (MX240, MX480, and MX960)** —Junos OS Release 24.4R1 supports distinct NAT port and pool mapping for Port Control Protocol (PCP) and Dual-Stack Lite (DS-Lite).

  The PCP and DS-Lite can use the same NAT IP address with different port and NAT pools if the traffic originates from the same subscriber.

  Ensure that PCP and DS-Lite are configured with:

  - Address pooling, or address pooling paired (APP)
  - Endpoint independent mapping (EIM)
  - Endpoint independent filtering (EIF)

  You must configure the `allow-distinct-port-pools` at `[set services nat source]` hierarchy to assign same NAT IP address with different ports from different NAT pools.

  [See allow-distinct-port-pools, Port Control Protocol and IPv6 Dual-Stack Lite.]

## 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.]

## Precision Time Protocol (PTP)

-

## 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.

## 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.]

## 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.]

## 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.]

## 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.

- **BGP autodiscovery underlay in EVPN-VXLAN** (MX304, MX960, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)

  [See BGP Auto-Discovered Neighbors.]

- **Online insertion and removal (OIR) support for shared bandwidth, percentage, logical interface, physical interface, and hierarchical policers on interface-specific or shared firewall filters** (MX304).

  [See Chassis.]

- **QSFP-100G coherent ZR optics performance monitoring** (MX304). Monitor the performance of QSFP-100G coherent ZR optics and receive threshold-crossing alert (TCA) information to efficiently manage the optical transport link. Accumulate performance metrics into 15-minute and 1-day interval bins. Use the `show interfaces transport pm` command to view current and historical performance data.

  [See optics-options, and show interfaces transport pm.]

- **Supported transceivers, optical interfaces, and DAC cables (MX10004, MX10008)**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **Enhanced Address Detection for Reliable Connectivity (ACX5448-M, MX10008, MX10016, SRX5800, and QFX10008)**—We've improved our network address detection process to deliver more reliable connectivity and uninterrupted performance. This update prevents disruptions caused by duplicate address detection (DAD) failures under rare network conditions. By integrating advanced algorithms and unique identifiers, we reduce false detections and ensure smooth data flow, keeping your network running seamlessly.

## What's Changed

**IN THIS SECTION**

User Interface and Configuration | 95

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

## EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file **/var/log/syslog**.

## Forwarding and Sampling

- Support added for interface-group match condition for MPLS firewall filter family.

## General Routing

- Starting from Junos 21.4R1 platforms with the following Routing Engines which have Intel CPUs with microcode version 0x35 observe the error warning, "000: **Firmware Bug**: TSC_DEADLINE disabled due to Errata; please update microcode to version: 0x3a (or later)" on the console. RE-S-X6-64G RE-S-X6-128G REMX2K-X8-64G RE-PTX-X8-64G RE-MX2008-X8-64G RE-MX2008-X8-128G.

- **Non-revertive switchover for sender based MoFRR**—In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, i.e. traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under `protocols mvpn hot-root-standby min-rate`.

  [See min-rate.]

- For MPC5E line card with flexible-queuing-mode enabled, queue resources are shared between scheduler block 0 and 1. Resource monitor CLI output displays an equal distribution of the total

available and used queues between scheduler blocks. This correctly represents the queue availability to the routing engine.

[See show system resource-monitor and show system resource-monitor ifd-cos-queue-mapping fpc.]

- By default, host-generated outbound PTP traffic is assigned to the default network control (NC) forwarding class, which is assigned to queue 3 by default. You can change both the forwarding class and queue assignment for host outbound traffic.

  [See Changing the Default Queuing and Marking of Host Outbound Traffic.]

- **Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)**—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json` command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and the PyEz displays all the duplicate keys with the enhanced tags.

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- Support added for interface-group match condition for MPLS firewall filter family.

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## Routing Protocols

- **Update to IGMP snooping membership command options—**The `instance` option is now visible when issuing the `show igmp snooping membership` command. Earlier, the `instance` option was available but not visible when ? was issued to view all possible completions for the `show igmp snooping membership` command.

[See show igmp snooping membership.]

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

## 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

- 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
- 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 controller while using application match as any or any SRX default application. PR1847209

## 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

## 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. PR1765052

## Forwarding and Sampling

- After switchover in MX2010 platform , test configuration is removed with load update and then rollbacked. During rollback commit , configuration commit failed with below error: error: commit-check-daemon : Invalid XML from dfwd error: configuration check-out failedPR1829614

## General Routing

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs.PR1492605
- 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
- Probe status is showing "Unhelpful,abort" while running P2mp LSP traceroute.PR1697658
- 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
- The fec-codeword-rate data with render type decimal64 is rendered as string in grpc python decoder.PR1717520
- Error message might occur once in a while with full scale during negative scenarios like `clear bgp neighbor all` with all the services like EVPN, vrf etc being present.PR1744815
- MX480 CommonDiag:: JDE3(volt_services_show_clients) failing on MPC7e. PR1747033

- MX2010 Diagnostics::Jde3Diag(phy_reg_access) test is failing. PR1747297
- 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
- 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
- On all Junos and Junos Evolved platforms, repd core observed (in the "from" release) during unified ISSU.PR1797189
- 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 RE. PR1799451
- MPC11 In-Service-Software-Upgrade command fails from release 24.1R1 to 24.2R1 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
- M/Mx: IS-IS session over MPC11 cards flapped due to "3-Way handshake failed" during unified ISSU (FRU upgrade stage - reboot phase). PR1809351
- The `set chassis no-reset-on-timeout` is a debug command for SPC3 to prevent it from rebooting in case of issue. It is not to be set during normal operations since SPC3 might need reboots to come online. PR1809929
- [MX] : [UT] During RE reboot with PTP FPGA, Correctable and uncorrectable AER errors seen. Issue seen with Doon RCB as well. PR1817097
- 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 does not support AN and this mismatch is causing the traffic loss. This needs feature enhancement PR1817992
- 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 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

- CLI /RPC "show bgp group rib-sharding all"/"get-bgp-group-information" failure with XML CRITICAL ERROR and ODL Validation failure. PR1826803
- On MX platforms with MS-MPC and CGNAT (Carrier-Grade Network Address Translation) 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. So to use the legacy "SCP" protocol from shell, please use the -O command line option For example: scp -O other 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
- MX304: show chassis synchronization extensive CLI output shows syncE is locked to both primary and secondary sources after switching between primary and secondary sources in hybrid mode. The issue is only with CLI display. No functional impact. The Clock Event" field in both primary and secondary source is shown as Locked which is wrong. The trigger for this scenario is - set the primary interface port down so that syncE switches to secondary source and then bring back the primary interface either through port down or LMIC offline and online. PR1841695
- When trying to console into the GNF using a non-root user in Juniper Device Manager JDM users are not able to console. PR1842451
- IPv4 frame routes which are not using /32 prefix length do not get applied. PR1855891
- On Junos MX Series routers with MS-MPC/MS-MIC cards, when `clear service sessions` are executed from multiple windows (approximately 5 terminals), the PIC reboots and eventually all the service traffic will be impacted.PR1827806
- When performing ISSU on MX-series routers from 23.4R1 to 24.4R1, repd will core in master RE during image validation phase and RE goes to # prompt. PR1855947

## 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 KB26616 resolution rib policy is required to apply as a work-around. PR1754351
- OSPF neighborship goes down after NSR (Nonstop routing) switchover due to link flapping on Junos OS Evolved platforms with dual Routing Engine and IPsec configuration. PR1848313

## Interfaces and Chassis

- Junos MX | iflset stats not getting cleared after issuing clear interfaces stats all and clear interfaces interface-set statistics all CLI command. PR1741282

## Layer 2 Ethernet Services

- On MX104 platforms, when ALQ (Active-Lease Query) enabled with DHCPv6 (Dynamic Host Configuration Protocol ) relay agent configuration, ALQ syncing for DHCPv6 TCP (Transmission Control Protocol) connection will not work due to issues while processing the ALQ messages and TCP handshake messages at peer. PR1727624
- 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 (> 5 secs). 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

## MPLS

- While performing unified 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 Management and Monitoring

- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358
- Issue: 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
- Native junos modules in hello-message and yang modules in /var/run/db/yangs are not same. The build failure is due to a mismatch between the native Junos modules in the hello message and YANG modules in /var/run/db/yangs, causing the test to fail with a difference in lengths: 229 != 230. PR1816904

## Platform and Infrastructure

- On Junos platforms , the standby router goes into the error state when the switchover is performed. This will not impact the traffic. PR1847307

## 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

## Subscriber Management and Services

- In Routing Engine show subscribers extensive shows ACTIVE state, and that resembles the IPDEMUX ifl (and SDB Session state) but the Pseudo IFL is not getting propagated when we take out the V6 family configuration. For V6 session it gives a deceiving notion on the health of the session ( `show subscribers extensive` shows state is ACTIVE where as flow is NOT present in PFE). Following CLIs need to be configured to have the FLOW propagated to the PFE. set dynamic-profiles ip-demux-profile interfaces demux0 unit "$junos-interface-unit" family inet6 demux-source $junos-subscriber-ipv6-address set dynamic-profiles ip-demux-profile interfaces demux0 unit "$junos-interface-unit" family inet6 unnumbered-address "$junos-loopback-interface IPDEMUX IFL / SDB Session has no dependency in terms of control plane "state machine" with the corresponding Pseudo IFL. Trying to tailor the state of IPDEMUX ifl / SDB Session w.r.t the pseudo ifl state increases complexity and introduces dependancy.PR1817549
- DHCPv6 BLQ query is not working if queried with server address/server group since relay id information is not passed as part of query. PR1839348

## User Interface and Configuration

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

## 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.

## Class of Service (CoS)

- Multiple adjacencies may get dropped over AE interfaces PR1828018
- FC id goes out of sync between the RE and PFE impacting all CoS features using FC id PR1836528

## EVPN

- The rpd process will crash when TTE is enabled with EVPN-VPWS or EVPN-ELAN configured PR1808180

- EVPN over MPLS IPv6/SRv6: PMSI attribute carrying wrong flags with value 0x20 (bit 2). PR1814525
- [Junos OS Evolved] LACP on non-DF ACX router comes out of "out-of-sync" state by deactivating one of the EVPN instances, causing CE device to move to Collecting distributing PR1816672
- Deactivating protocol evpn in a routing-instance configured with 'vrf-target auto' leads to the rpd crash on both REs PR1821582
- Continuous kernel log messages are observed once the EVPN-VXLAN fabric is up PR1826772
- GBP tags remain in place even after GBP tag assignment firewall filter is removed or deletion of mac-ip entry on specific Junos EX and QFX platforms with EVPN-VXLAN PR1830126
- [EVPN] The one of routing-instances configuration changing affects whole LACP state under "lacp-oos-on-ndf"(LACP out-of-sync) and EVPN "single-active" conditions. PR1832785

## Flow-based and Packet-based Processing

- When using IPv6 Multi-path BGP with MX configured with EVPN, transit SFW traffic experiences packet drops during IPv6 Neighbor discovery refresh. PR1817211

## Forwarding and Sampling

- Firewall filter having 'then routing-instance' term will not work properly after deactivate/activate routing-instance being done. PR1810237
- Empty commit is behaving as commit full after the system was upgraded PR1818988
- A BFD flap and subsequent impact in the traffic is seen when BGP FlowSpec session goes down or withdrawal of all BGP FlowSpec routes making entries on netflow.0 table to zero at once PR1827439
- Incorrect color-aware srTCM marking with yellow packet loss priority PR1837840

## General Routing

- A few line cards will be stuck in the 'Present' state and later go 'Offline' PR1631579

- On MX10004/MX10008/MX10016 chassis running Junos LC480 may reboot when "request system firmware" CLI command is executed to get the firmware information PR1696186
- Support of "no-confirm" option in EVO ISSU PR1713589
- Observing core with rpd with BGP flowspec if secondary-independent-resolution is configured PR1722715
- JDI-RCT:M/Mx: SMPC crash @ hostif_clear_toe_interrupts, toe_interrupt_handler after fpc restart scenario . PR1733053
- Telemetry data is not exported in an IS-IS scaled Segment Routing scenario PR1745615
- Junos OS: Due to a race condition AgentD process causes a memory corruption and FPC reset (CVE-2024-47494) PR1769294
- Junos vmhost upgrade will continue to reboot the box even if the upgrade has failed due to tar errors when the reboot option is used PR1770585
- FPC gets stuck at 100% utilization after upgrade from 21.2R1 or below to 21.3R1 or higher release PR1777139
- MX304 not reachable with the power-off failure on the PIC PR1784438
- The KRT queue will be stuck on Junos ACX710 platform PR1787707
- Traffic drop due to mac-validate failure on MX platforms PR1788669
- An enhancement to modify the output and alarm when an interface is down due to XCVR over temperature PR1789622
- "JTASK_NO_SOCKACCEPT: Process events: no read/accept method for MGMT socket -1" logs may be seen in the messages file or an external syslog server PR1795659
- Traffic impact during ISSU across FPCs on Junos MX platforms PR1796770
- The system goes into a bad state when an SFB ungraceful offline happens due to a fatal Interrupt PR1798780
- VNF OVS Interface failure with high memory PR1799045
- The "show chassis synchronization clock-module | display xml validate" get "INVALID" output PR1799397
- Traffic loss observed when we configure more then 256 terms in Fast-lookup-filter PR1799457
- Traffic impact on SPC3-PIC due to high throughput and bursty traffic PR1799512

- On Junos platforms the telemetry subscribe to path": "/components/component[name='Routing Engine0']/state/memory/utilized is not working as expected PR1800754
- PEM1 alert is going to clear immediately, and alarm LED was not lit after the power cable/PEM was removed. PR1800855
- The RE switchover will not be triggered in case of clock failure on SCBE3-MX PR1801284
- Memory Leak in the rpd Process During Protocol Deactivation/Activation PR1801382
- SFB PCIE switch temp sensors yellow alarm falsely reported at high altitude and high temp operating conditions PR1801778
- The optics temperature sensor name renamed from 'et-x/y/z' to 'xcvr-x/y/z' PR1802195
- AFTD crash may be observed when a MAJOR CMERROR that affects only one of the slice of a multi-slice PFE is triggered PR1802243
- SFB ungraceful offline followed by master SPMB reboot results in traffic drops due to fabric Link errors PR1802259
- MPLSoUDP route issue preventing LSP establishment PR1803578
- Traffic loss is observed along with error messages on Junos MX platforms with MPC1 to MPC9, LC2101, LC480 (including MX204, MX10003) during any transport LSP change operation PR1804263
- The rpd process crash can be seen in restoration to baseline configuration in scaled scenario PR1804363
- NSD validation failure results into upgrade failure for Junos MX platforms PR1804616
- The rpd process crashes during rpd restart on Junos and Junos Evolved platforms PR1805427
- Return Error for unsupported options with GNMI RPCs PR1805445
- MX platforms with with MPC10,MPC11,LC9600 and MX304 we observe IPv6 unilist next-hops are missing PR1806717
- Partial traffic blackhole will be observed during the time of FPC crash due to interfaces not going down PR1806787
- SFB power off/unplug followed by ungraceful SPMB restart leads to SPMB crash PR1807410
- [MX] daemon.err rshd[618008]: Second port outside reserved range. PR1807939
- Feature names used across licensing alarms and logs generated. PR1808084
- Openconfig data type value is streaming in gnmi update as float_val instead of bytes_val PR1808259

- CPU utilization of the rpd process stays high on all Junos and Junos OS Evolved platforms PR1808463
- The error message "sysctl kern.corefile not supported" is seen for multiple daemons during daemon initialisation PR1808481
- Traffic loss occurs if persistent link error is seen on a fabric plane to PFE, after restarting or rebooting another FPC in a different slot PR1808923
- On Junos MX204 platform and platforms with MPC7E/8E/9E, JNP10K-LC2101, JNP10003-LC2103, JNP10K-LC480 line cards, the interface goes down when re-initialisation issue occurs, causing 'Avago SERDES' EA (Eagle ASIC) chip crash PR1809306
- Ethernet interfaces configured with loopback option remains down after multiple iteration of line card boot is performed PR1809511
- The l2ald core is observed due to stale IFD entry PR1810013
- [MX960] An explanation of the following messages VBFMAN:SEND_CLIENT: PacketL2Inject Failed. error:Invalid argument and VBFMAN:PFE_EVENT_BULKING: Sending of PFE event bulked message to SMGD Failed len:0 PR1810029
- The "unknown-unicast-forwarding" feature is allowed to be configured even though it is not supported for the target platform. PR1810120
- With debug level mesages are enabled, macsec logs are printed even when macsec is not enabled PR1810259
- Error messages "dot1xd[xxxx]: %DAEMON-3-DOT1XD_MACSEC_GENCFG_ERROR: rtslib_gencfg operation failed ifd" seen after GRES PR1810563
- EVPN-VXLAN : Breakage in the cli "show forwarding-options load-balance source-address X destination-address X source-port X destination-port X" on VMX/MX480/MX960 PR1810653
- The rpd crash is observed due to the segmentation fault on Junos OS Evolved platforms PR1810866
- The rpd process crashes if the configuration changes rapidly when Tactical TE is enabled PR1811005
- In Junos MX platforms specifically MX2010 and MX2020 with SFB2 Fabric installed replacing MPC9E linecards with MPC6E linecards results in all SFB2 fabric get into check state and FPCs becomes destination error and offline PR1811474
- Intermittent SFB I2C failure Alarm and Alarm cleared after 3 polls of 5 seconds due to ZF0 VDD 0.75V intermittent access failure PR1811485
- XSTP reconverges after GRES (Graceful routing-engine switchover) with NSB (nonstop bridging) enabled if l2cpd in master is restarted before switchover PR1811511

- The LLDP neighborship does not recover on AE interfaces PR1811545
- ARP and ND entries are not in sync across the EVPN-VXLAN peers which leads to traffic drops PR1811556
- The rpd process crash is observed when there are catastrophic changes under the particular routing instance configuration PR1812009
- On MX2K, offline manually SFB2 or SFB3 or Plane to recover from a fabric link training failure, fabric mananger is not able to turn off the fabric links on a neighbor slot FPC PR1812046
- Persistent link error in one fabric plane towards some PFE could causes traffic blackholing from non-native LC PFE towards that remote PFE over all fabric planes PR1812276
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario PR1812482
- Batch commit is not working in HA. PR1813367
- With 24.2R1 software release, some of the 100G and 400G links may remain DOWN after LC4800 FPC restart PR1814101
- The dot1x authentication fails for VoIP traffic PR1814502
- Faulty MPC8 or MPC9 line cards can lead to spontaneous chassisd crash on certain Junos MX platforms PR1814801
- jnxSpSvcSetIfMemoryZone SNMP mib always returns 0 for service-set memory usage zone PR1814935
- JDI-RCT:M/Mx: after unsupported card is offlined during ISSU validation in MX router, fabric planes are stuck in check state PR1815125
- Premature graceful RE switchover causes traffic blackhole during software upgrade on PTX platforms with dual RE PR1815152
- The collector will see duplicate entries during the init sync of gNMI subscription on Junos and Junos Evolved platforms PR1815195
- MAC addresses learnt on interfaces part of VLAN with MAC limiting by interface and "drop-and-log" action configured are cleared after VLAN description is changed PR1816049
- PFE core is observed due to PCIE link was down PR1816148
- XQSS_CMERROR errors will be seen which might disable PFE PR1816378
- JNP10K-LC480 Linecard fails to come online after restart due to CM Errors PR1816506

- Traffic blackholing will be observed in the l2circuit scenario when a non-active path is shut or disabled PR1816807
- IIC access error during commit operation cause false positive alarms in devices PR1816912
- The latest GNMI specification decrements the streaming of float_val types. Instead double_val type should be streamed. PR1817267
- The l2ald crash is observed when adding scaled EVPN-VXLAN configuration on Junos platforms PR1817705
- Product annotation is missing for sensors on the MX, PTX, and EX92XX platforms PR1817967
- On Junos OS Evolved platforms, any new L2 functionality doesn't work when ELP configuration is not present on the connected device(s) PR1818022
- [LC480] STS LED may display incorrectly PR1818475
- Fan Tray Outer Fan running at over speed alarm is reporting after upgrade PR1818517
- Configuration commit fails due to mustd process crash PR1818692
- The "preserve-nexthop-hierarchy" knob configured with VPLS , brings down the L3 protocol sessions running over the IRB interface PR1818978
- SRv6 to SRMPLS tunnel config changes cause rpd restart PR1819019
- The SNMP jnxFruRemoval/insertion trap OID is not being sent correctly when the FTC module or the fan tray module is inserted or removed PR1819263
- BMP gets stuck and does not send data to BMP collector PR1819305
- Switch port status is changed to unauthorized, when a supplicant client attempts to authenticate using 802.1X standard with EAP-TLS certificate PR1819462
- Multiple processes on both the REs are crashing PR1820001
- The JTI/UDP export format prompts "gpb-sdm" as a possible completion on executing "set services analytics export-profile profile name format gpb command PR1820510
- Commit check does not display error while configuring "format gpb-gnmi" and "transport udp" for export-profile in Telemetry PR1820774
- Per-Segment-list telemetry for colored tunnel doesn't work PR1820791
- Traffic drop is seen in an EVPN multihoming scenario when mac-pinning is enabled PR1820882
- Error messages "aft-proxy: IfdEtherGetInfoRequest: Not available MACsec data for:et-x/x/x" seen during macsec configuration init time PR1821862

- The PFE becomes inactive or disabled when running multicast in a video monitoring setup PR1822738
- Few flows for BUM traffic gets dropped when a mix of MPC1-9 and MPC10 and above is used PR1822793
- Aggregated ethernet interface flaps can be seen when IRB interface is activated or deactivated PR1822911
- Authentication failure will be seen for routing protocols when MD5 is configured for routing protocols and PCEP on Junos OS Evolved platforms post reboot PR1823220
- Interface will flap immediately on MX platform with MPC2 or MPC3 after FPC restart or router boot up PR1823373
- Licensing usage is not set post reboot until there is an empty commit is done PR1823449
- New threshold values are set as LC4800 is not NEBS acoustic compliance PR1824343
- The traffic is getting duplicated when VPLS to EVPN transition is performed PR1824739
- Interface queue stats are not showing for an IFD after switching the interface mode PR1825420
- The rpd crash is observed during upgrade or restart PR1826194
- The error messages will be observed while configuring native sensor paths PR1826196
- The PFE gets disabled due to large number of fabric self ping errors PR1827058
- Even though installed the license to both Master and Backup, Alarm LED might be lit with yellow on Backup. PR1827641
- Potential Traffic will be seen on GRES/L2ALD Restart/GR due to Shadow INH Change PR1828519
- In a high scaled and heavy loaded scenario, l2ald process may hang when Asptra is polling. PR1828741
- AFT: si- based Inline NPTv6 is not working, PPE Trap generated PR1828985
- A new CLI implementation for show command to view satellites in csds deployments. PR1829571
- The flowd process crashes in scaled scenario when subscribers exceed maximum session limit for NAPT44 on MX platforms with MX-SPC3 PR1829633
- Sourceport-ID comparison resulting in higher value for MPC7E compared to MPC5E for distributed PTP architecture PR1830281
- Commit error on using more than 31 characters authentication-key-chain-name PR1830395

- I2C failure messages may flood after plug/unplug the SFP multiple times PR1831605
- Telemetry streaming will not happen because the resource path is not valid PR1831841
- The soft minor alarm 'QoS License(289) usage requires a license' is raised on the device PR1832769
- Configuration Archival does not work using SFTP when using the mgmt_junos routing-instance on ACX5448 PR1833705
- The flowd process crash during TCP Packet Processing PR1834248
- The RPD crashes after executing "show krt error-statistics errorno X" PR1834859
- All PTX-EVO platforms doesn't support CFM Performance Monitoring Loss Measurement SLA iterator feature PR1836228
- The Subscriber Sessions will stuck in the terminated state and the final accounting will be delayed PR1839200
- RLT ifl remains down after RLT unit interface configuration is modified PR1840734
- Due to high bursty traffic, PIC on MX-SPC3 might go down. PR1841859
- Unable to console to VNF from JDM PR1842451
- CFM session flaps continuously upon committing CFM inline mode and CFM sessions related configuration together PR1842542
- Unnecessary trace log files related to licenses are generated PR1845079

## Interfaces and Chassis

- On Junos Evolved and Junos MX platforms with MPC10E/11E/LC9600 line cards traffic drop is seen due to changes in delay measurement profile PR1809956
- The LFM session flaps will be observed at random PR1811734
- FPC keeps crashing when the OAM connectivity-fault-management sla-iterator-profile data-tlv-size is set to more than 100 PR1820187
- After RE switchover the VRRP master and backup router will start functioning as master routers PR1822867

## Intrusion Detection and Prevention (IDP)

- Not able to update IDP signature DB when using Proxy server PR1822319

## Layer 2 Features

- VPLS traffic will be impacted when routing-engine switchover happens due to master routing-engine reboot in NSR scenario PR1793342
- RPD process terminates abnormally on MX480/MX10008 platforms by misconfiguration involving both BGP VPLS and LDP VPLS PR1813574

## MPLS

- The rpd process crashes with LDP entropy-label policy configuration with "from instance routing-instance-name. PR1812545
- LSP keep retrying over the transit router marked as "overload" resulting in traffic drops or using the suboptimal path for the LSP PR1814358
- MPLS LDP sessions are not established when container-lsp is configured with an already existing lsp-template PR1817712
- LSP re-optimization issue has been observed PR1819948
- The detour path is not coming up when the detour hop limit is set to 255 PR1820893
- Bypass re-optimisation not taking SRLG or fate-sharing into account when protected link is down PR1823215
- In a scenario involving NG-MVPN and point-to-multipoint LDP LSP the LDP point-to-multipoint FEC may remain in an inactive state on the PE after uplink interfaces flap PR1835938

## Network Address Translation (NAT)

- Commit error is observed on Junos platforms with MS-MPC or SPC3 when last octet of source-ip of jflow-log collector is above 223 PR1817417

## Network Management and Monitoring

- The eventd crashes if eventd traceoptions is enabled PR1795952
- The lo0 interface entries are missing from Junos 'ipNetToPhysicalTable' walk output PR1807176
- The "snmp packet-size size" command not working for SNMPv3 PR1817865
- In all Junos and Junos OS Evolved platforms, with Multinode High Availability configured, node configuration on primary might differ from backup due to configuration synchronization failure at the time of commit PR1819656

## Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596) PR1802329
- DDOS related Error messages can be seen on MX platforms PR1807538
- 500 concurrent probes supported on Junos TVP platforms instead of standard 2000 probes for other Junos Platforms PR1808361
- Few error messages will be seen while deleting multiple EVPN Routing Instances. PR1808643
- Traffic drop is observed after any add/change/delete event on IRB interfaces inside a VPLS deployment PR1814521
- Enabling "preserve-nexthop-hierarchy" knob under "l2-circuit resolution" stanza causes multicast traffic to be replicated several times PR1818853
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos platforms PR1826666

## Routing Policy and Firewall Filters

- OSPF neighbourship with IPsec authentication goes down after RE switchover PR1807830

## Routing Protocols

- Memory leak in rpd due to deactivation and activation of routing-instances, interfaces and protocols PR1761191
- Leaked routes via BGP rib-group remains in hidden state even though "loops" is configured with any value greater than one PR1771344
- BGP OutQ counter of one of the BGP peers gets stuck after system reboot/restart routing/clear bgp neighbor PR1788543
- BGP routes may not get advertised when always-wait-for-krt-drain is configured with BGP sharding PR1793714
- BGP multipath selects wrong interface with "Multiple Single-Hop EBGP sessions on different links using the same IPv6 Link-Local Address" PR1807504
- Junos OS and Junos OS Evolved: When BGP traceoptions is enabled, receipt of specially crafted BGP packet causes RPD crash (CVE-2024-39525) PR1807533
- The rpd crash is observed for the leaked ISIS SRv6 locator route holding a stale pointer PR1808185
- BGP routes with next hops as link-local address are not installed PR1810617
- An interface with a lower MTU size is causing a rpd crash PR1810993
- Improper maximum value for limit-bandwidth of policy-statement PR1811862
- The rpd process crash is observed when policy condition is applied to the route with a next-hop interface having nonzero logical unit PR1812844
- No new MoFRR back up path selected after changing the metric of back up PR1812857
- Local repair does not happen if BFD is configured on MX platforms with MPC7E line card PR1813841
- Incorrect counting of vrf-scale numbers for license warnings will be seen on all platforms PR1814012
- Junos OS and Junos OS Evolved: With BGP traceoptions enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39515) PR1814083
- RPD Core in BGP Multipath Config PR1814263
- Junos OS and Junos OS Evolved: With certain BGP options enabled, receipt of specifically malformed BGP update causes RPD crash (CVE-2024-39516) PR1815222
- Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511) PR1815253

- The rpd crashes when stale label entry keeps increasing when knob stale-labels-holddown-period is configured PR1817834
- BGP-LU Label is incorrect after convergence PR1818545
- PIM Prune is not sent to upstream PR1819741
- Unexpected behaviour after BGP sessions reset for catastrophic BGP configuration changes PR1826685
- Traffic impact due to BGP route stuck in hidden state PR1826686
- OSPF LSA flooding is impacted after database recovers from 'ignore' state when 'database-protection' is triggered PR1827435
- [MX] Memory leak observed in so_in6 and TED-INFRA-COOKIE leading to RPD crash PR1828209
- ISIS adjacency part of an igp-instance gets stuck in 'Initializing' state after the rpd restart PR1830989
- The 'overload advertise-high-metrics' does not work after the graceful restart for ISIS PR1837289
- The rpd crash after enabling ISIS with authentication keychain PR1839917
- IPv6 BGP neighbors flapping intermittently when NSR is activated PR1840929
- Meta: Traffic drop seen after GR GRES. PR1841108

## Subscriber Access Management

- Address preservation for delegated prefixes does not work for subscribers in VRF PR1777967
- authd core after running ZTP PR1812697
- authd process crashes when radius-server-name is configured PR1818321
- The authd process crash is seen when subscriber management is enabled PR1826901
- CoS rewrite functionality not working when having BBE subscriber on Static Vlan interface. PR1802202
- The process bbe-smgd crash will be observed in the Subscriber login/logout scenario. PR1811787
- PFCP Association stuck in disconnecting state for BNG CUPS platforms. PR1812890
- Extensible Subscriber Services Manager (ESSM) sessions gets disconnected when PFE encounters an issue for any service or subscriber session PR1814017

- 'show system subscriber-management route summary' displays a negative gateway route count in the new master RE after UP-GRES PR1814125
- L2BSA sessions remain down when port messages from ANCP neighbor are dropped in a scaled scenario after ISSU followed by GRES PR1814300
- The aftd process crash is seen on certain MX platforms with subscriber management enabled PR1814341
- The bbe-smgd crash is seen on MX platforms. PR1815502
- Multiple BBE daemons getting killed automatically on MX platforms. PR1818781
- The bbe-smgd daemon memory leak will be seen when ACI VLAN parsing fails. PR1821021
- The jnxSubscriberPortTerminatedCounter shows incorrect values for interfaces PR1824274
- On MX304 DHCP Vlan Creation Fails for EVPN VPWS when PIC0 is not Installed. PR1825417
- The subscribers get stuck post GRES switchover. PR1826324
- An Enhancement to 'show ancp subscriber detail' command to display port-up/down timestamp and port-down cause. PR1841954
- Redundancy Support for New Consumer Services / BNG Licensing on Junos MX platforms. PR1787234
- After L2 failover, client receives DHCP attributes from the main pool configured instead of the linked pool and linked address-assignment pool name is not synced to DHCP binding on backup BNG having ALQ in BBE subscriber management scenario PR1799888
- The client session is logging out as DHCP renewal is not successful PR1801142
- jdhcpd cores when 'show dhcpv6 server binding' command is executed PR1816995
- DHCP asymmetric-lease-time is slow processing large scale requests to terminate 64K subscribers. PR1817227
- jdhcpd core dumps may be seen on ALQ setups when subscriber synchronization is done PR1818919
- DHCP ALQ process crashes to recover from memory leak. PR1825998
- DHCP relay option "allow-server-change" does not work as expected in trusted server group PR1833148

## User Interface and Configuration

- The commit fails error can be seen when configuration is modified after commit prepare PR1799215
- The system scripts refresh will fail when using load CLI option PR1821845
- The mgd process crashes while using an FQDN in conjunction with the ephemeral configuration database PR1825728

## VPNs

- MPLS LSP tied to an l2circuit is not honoring the configured transport class PR1834625

## 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.

Starting in Junos OS 17.4R1 release, FreeBSD 11.x is the underlying OS for all Junos OS platforms which were previously running on FreeBSD 10.x based Junos OS. FreeBSD 11.x does not introduce any new Junos OS related modifications or features but is the latest version of FreeBSD.

The following table shows detailed information about which Junos OS can be used on which products:

| Platform | FreeBSD 6.x-based Junos OS | FreeBSD 11.x-based Junos OS |
|---|---|---|
| MX5, MX10, MX40,MX80, MX104 | YES | NO |
| MX240, MX480, MX960,<br>MX2010, MX2020 | NO | YES |

## Basic Procedure for Upgrading to Release 24.2R1

**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 FreeBSD 11.x-Based Junos OS

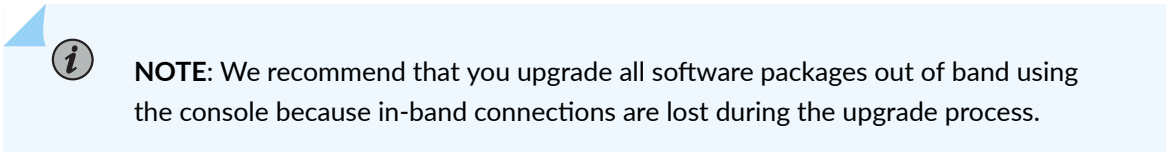
Products impacted: MX240, MX480, MX960, MX2010, and MX2020.

To download and install FreeBSD 11.x-based 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-x86-32-20.4R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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-x86-32-20.4R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-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*

Do not use the `validate` option while upgrading from Junos OS (FreeBSD 6.x) to Junos OS (FreeBSD 11.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 11.x, and Junos OS (FreeBSD 6.x) would not be able to run these programs. You must run the `no-validate` option. The `no-validate` statement disables the validation procedure and allows you to use an import policy instead.

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**: After you install a Junos OS Release 24.2R1 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the jinstall package that corresponds to the previously installed software.

**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.

## Procedure to Upgrade to FreeBSD 6.x-Based Junos OS

Products impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.x-based 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:

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-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 OS package):

```
user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-limited-signed.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*

The validate option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.

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**: After you install a Junos OS Release 24.2R1 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

## 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**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.

## 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)

- **Many-to-one source NAT for multicast traffic (NFX150, NFX250, and NFX350)**—Adds support for source Network Address and Port Translation (NAPT) for multicast data traffic.

  [See show security nat source summary and show security nat source paired-address.]

## What's Changed

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

## Known Limitations

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.

## 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 NFX platforms, when one partition supports a Junos OS Release 23.4R1 image (supported on LTS19 operating sytem) and the other partition supports an image older than Junos OS Release 23.4R1 (supported on WRL8 operating system), the `request vmhost reboot disk` command is not executed as expected.

  As a workaround, upgrade both the partitions with same image versions PR1753117.

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

# 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.

## General Routing

- The dcpfe process on the NFX350 platforms crashes when the device undergoes a shutdown or a reboot.PR1807738
- On NFX250 and NFX350 platforms, the command `clear interfaces statistics all` is not executed within the expected time (i.e. 1-2 seconds). There is no traffic impact due to this issue.PR1818888

## High Availability (HA) and Resiliency

- When high availability (HA) is enabled and fabric links are configured on NFX devices ( NFX150, NFX250 and NFX350 with nfx-3 software package), the fabric link monitored status is displayed as Down leading to an FL status. PR1794559

## VNF

- On all the NFX platforms with LTS19 image, the VNF (Virtual Network Function) OVS (Open vSwitch) interfaces fail to come up when more than 4Gb of memory is allocated to the VNF. This affects the traffic flow.PR1799045

# 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**Table 7: 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 |

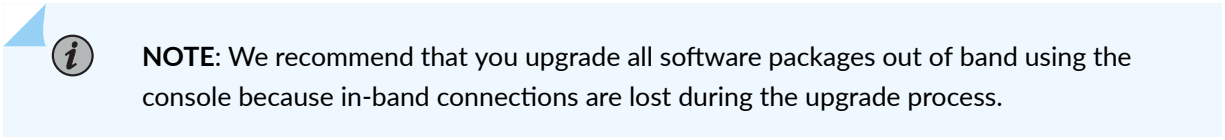
For more information about EOL and EEOL releases, see https://www.juniper.net/support/eol/junos.html.

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 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 24.4R1, 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

## Application Identification (AppID)

## Chassis

- **New CLI commands for chassis management error configuration (QFX10008 and QFX10016)**—You can configure the severity, threshold, and action for chassis management errors at the `[edit chassis sib]` hierarchy level. You can also use the `reset-count` option to configure the number of times the chassis management error can reset a Switch Interface Board (SIB).

  [See reset-count and error.]

## Dynamic Host Configuration Protocol

- **DHCP Snooping trusted mode support on a vlanVLAN (EX Series, QFX Series)**—Use the `trust-all` configuration option for DHCP snooping to configure all interfaces within a VLAN as trusted interfaces. This configuration enhances network security by ensuring that only trusted interfaces can relay DHCP messages, preventing unauthorized devices from acting as DHCP servers

- **DHCP Relay `no-snoop`(QFX Series)**—We introduce a new `no-snoop` knob that enables all DHCP unicast packets to be stopped from going to the CPU and only handle hardware forwarding.

  [See Understanding DHCP Relay `no-snoop`.]

## EVPN

- **Filter-based forwarding for GBP-tagged traffic (EX4100, EX4400, EX4650, and QFX5120)**—You can now forward traffic to a specified next hop if the group-based policy (GBP) tags assigned to that traffic match the GBP tags specified in the filter. Use this feature to apply different routing treatment between the specified tagged traffic and regular traffic.

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

- **Longest prefix match in IP-based GBP firewall filters (EX4100, EX4400, EX9204, EX9208, EX9214, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, and QFX5120)**—IP-based group-based policy (GBP) firewall filters now honor the best match rather than the first match. The

order of IP address firewall terms in an IP-based GBP firewall filter is no longer relevant. Instead, the filter evaluates all IP address terms and selects the longest prefix match.

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

- **GBP tagging and policy enforcement (QFX5120-48T and QFX5120-48YM)**—GBP tagging and policy enforcement are now supported on QFX5120-48T and QFX5120-48YM switches.

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

- **XML-based support information (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—You now have the option of providing xml-based output of the "reqeust support information evpn-vxlan" command. You can do so from the CLI using `request-support-information evpn-vxlan-xml | gzip > <filename>`.

  [See request support information.]

## Junos Telemetry Interface

- **Native sensor support for Layer 2 learning MAC table and MAC-IP table (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, EX4400-24P, EX4400-24MP, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, QFX5120-32C, QFX5120-48Y, and QFX5120-48Y-VC)**—Junos OS supports native telemetry data streaming for Layer 2 learning MAC and MAP-IP table sensors with Google protocol buffer (GBP) data encoding. You can create a subscription in PERIODIC or ON_CHANGE mode using Juniper's proprietary Remote Procedure Call (gRPC) service or gRPC Network Management Interface (gNMI). Use the resource path **/state/routing-instances/routing-instance/l2-learning/mac-table/** in a subscription to stream data. This feature is based on the new data model **junos-state-l2-learning.yang**.
  [See Junos YANG Data Model Explorer.]

- **Stream data from a device to a collector using basic Junos Telemetry Interface infra sensors and new component environment sensors—** Junos OS supports these new sensors:

  Relative humidity sensor-

  ```
  /components/component[name='FPC0']/properties/property[name='moisture']/
  ```

  Two input and one output dry contact sensors-

  ```
  /components/component[name='FPC0']/properties/property[name='alarm-port-output0']
  /components/component[name='FPC0']/properties/property[name='alarm-port-input0']
  /components/component[name='FPC0']/properties/property[name='alarm-port-input1']
  ```

You can also display the dry contact and relative humidity information using the operational mode commands `show chassis environment` and `show chassis craft-interface`.

[For state sensors, see Junos YANG Data Model Explorer.

## Multicast

- **Enhancement to L3 multicast operational commands (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, EX4650, MX960, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—The show instance command now extends to all routing instances for the following commands. Previously, only specific Protocol Independent Multicast (PIM)-enabled routing instances were displayed.

  - `show pim join instance all`
  - `show pim rps instance all`
  - `show pim statistics instance all`
  - `show multicast route instance all`
  - `show multicast statistics instance all`

  The `show pim statistics` output will display `V2 Sparse Join` and `V2 Sparse Prune` counters.

  The `show igmp statistics` output will also display the `V1/V2/V3 Membership Query` field.

  [See `show pim statistics`, `show multicast statistics`, and `show igmp statistics`.]

- **New option introduced for the `show route snooping` command (QFX5110 and QFX5120-32C)** —We now support the `instance` *`instance-name`* option for the show route snooping command. This displays details of all instances when used without the instance name and details of a specific instance when used with the instance name.

  [See show route snooping | Junos OS | Juniper Networks.]

## 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.]

## Additional Features

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

- **BGP autodiscovery underlay in EVPN-VXLAN** (MX304, MX960, QFX5120-32C, QFX5120-48T, QFX5120-48Y, and QFX5120-48YM)

  [See BGP Auto-Discovered Neighbors.]

- **Filter-based forwarding using group-based policy (GBP) tags tags** (EX4100-48P, EX4400-48F, EX4650, and QFX5120-48T).

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

- **L2PT with Q-in-Q over VXLAN tunnels in EVPN-VXLAN bridged overlay networks** (QFX5110, QFX5110-VC, QFX5200, and QFX5210).

  [See Layer 2 Protocol Tunneling over VXLAN Tunnels in EVPN-VXLAN Bridged Overlay Networks, Examples: Tunneling Q-in-Q Traffic in an EVPN-VXLAN Overlay Network, and l2pt (Destination Tunnels).]

- **Nonrevertive preference-based EVPN DF election** (QFX5120-32C, QFX5200)

  [See EVPN Multihoming Designated Forwarder Election, preference (DF Election), and df-election-type.]

- **Supported transceivers, optical interfaces, and DAC cables (EX Series and QFX Series)**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **Enhanced Address Detection for Reliable Connectivity (ACX5448-M, MX10008, MX10016, SRX5800, and QFX10008)**—We've improved our network address detection process to deliver more reliable connectivity and uninterrupted performance. This update prevents disruptions caused by duplicate address detection (DAD) failures under rare network conditions. By integrating advanced algorithms and unique identifiers, we reduce false detections and ensure smooth data flow, keeping your network running seamlessly.

# What's Changed

IN THIS SECTION



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

## EVPN

- **EVPN system log messages for CCC interface up and down events**—Devices will now log EVPN and EVPN-VPWS interface up and down event messages for interfaces configured with circuit cross-connect (CCC) encapsulation types. You can look for error messages with message types EVPN_INTF_CCC_DOWN and EVPN_INTF_CCC_UP in the device system log file (`/var/log/syslog`).

## Forwarding and Sampling

- Support added for interface-group match condition for MPLS firewall filter family.

## General Routing

- Starting from Junos 21.4R1 platforms with the following Routing Engines which have Intel CPUs with microcode version 0x35 observe the error warning, "000: **Firmware Bug**: TSC_DEADLINE disabled due to Errata; please update microcode to version: 0x3a (or later)" on the console. RE-S-X6-64G RE-S-X6-128G REMX2K-X8-64G RE-PTX-X8-64G RE-MX2008-X8-64G RE-MX2008-X8-128G.

- **Non-revertive switchover for sender based MoFRR**— In earlier Junos releases, source-based MoFRR ensured that the traffic reverted to the primary path from the backup path, when the primary path or session was restored. This reversion could result in traffic loss. Starting in Junos OS 22.4R3-S1, source-based MoFRR will not revert to the primary path, that is, the traffic will continue to flow through the backup path as long as the traffic flow rate on the backup path does not go below the configured threshold set under cli protocols mvpn hot-root-standby min-rate cli.

- For MPC5E line card with flexible-queuing-mode enabled, queue resources are shared between scheduler block 0 & 1. Resource monitor CLI output displays an equal distribution of the total available and used queues between scheduler blocks. This correctly represents the queue availability to the routing engine.

  [See show system resource-monitor and show system resource-monitor ifd-cos-queue-mapping fpc.]

- **Change to the commit process**—In prior Junos OS and Junos OS Evolved releases, if you use the commit prepare command and modify the configuration before activating the configuration using the commit activate command, the prepared commit cache becomes invalid due to the interim configuration change. As a result, you cannot perform a regular commit operation using the commit command. The CLI shows an error message: 'error: Commit activation is pending, either activate or clear commit prepare'. If you now try running the commit activate command, the CLI shows an error message: 'error: Prepared commit cache invalid, failed to activate'. You then must clear the prepared configuration using the clear system commit prepared command before performing a regular commit operation. From this Junos and Junos OS Evolved release, when you modify a device configuration after 'commit prepare' and then issue a 'commit', the OS detects that the prepared cache is invalid and automatically clears the prepared cache before proceeding with regular 'commit' operation.

  See [ Commit Preparation and Activation Overview.]

- In a firewall filter configured with a port-mirror-instance or port-mirror action, if l2-mirror action is also configured, then port-mirroring instance family should be any. In the absence of the l2-mirror action, port-mirroring instance family should be the firewall filter family.

- **Option `allow-transients` is set by default for the EZ-LAG commit script**—The EZ-LAG feature simplifies setting up EVPN multihoming configurations using a set of configuration statements and a commit script. The commit script applies transient configuration changes, which requires the `allow-transients` system commit scripts option to be set. Now the default system configuration sets the `allow-transients` option at the EZ-LAG commit script file level, removing the need to set this option manually. In earlier releases where this option isn?t set by default, you must still configure the option explicitly either globally or only for the EZ-LAG commit script.

  [See Easy EVPN LAG Configuration Overview.]

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## Routing Protocols

- **Update to IGMP snooping membership command options**— The `instance` option is now visible when issuing the `show igmp snooping membership ?` command. Earlier, the `instance` option was available but not visible when `?` was issued to view all possible completions for the `show igmp snooping membership` command.

  [See show igmp snooping membership.]

- **MLD snooping proxy and l2-querier source-address (ACX7024, ACX7100-32C, EX4400-24MP, PTX10001-36MR, QFX5120-32C, and QFX5130-32CD)**— The `source-address` configured for `proxy` and `l2-querier` under the `mld-snooping` hierarchy should be an IPv6 link-local address in the range of fe80::/64. The CLI help text has been updated to "Source IPv6 link local address to use for proxy/L2 querier". In earlier releases, the CLI help text read, "Source IP address to use for proxy/L2 querier."

  [See source-address.]

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family`

field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

[See show system information and show version.]

## 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

## Open Issues

**IN THIS SECTION**

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 OS, 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
- 4x25G channelized interfaces are not coming up after optics hot swap. PR1719758
- When the remote end server or system reboots, QFX5100 platform ports with SFP-T 1G inserted might go into a hung state and remain in that state even after the reboot is complete. This might affect traffic after the remote end system comes online and resumes traffic transmission. PR1742565
- In a QFX51200-48YM-8C VC setup, after a primaryship switch over fan tray of linecard might not be displayed in show chassis hardware and show chassis environment. There is no functional impact. PR1758400
- 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 OS QFX5100 and EX4600 Platforms, high storage utilisation 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
- On all Junos OS QFX5000 platforms, with ECMP (Equal Cost Multi Path) configured, when there is any routing protocol change (like ISIS cost metric change), the protocol traffic on the network is dropped. PR1823601

- The QFX10002-60C platforms migiht 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
- On QFX5210/AS7816 platforms, when using forwarding-options custom profile , the PFE `show pfe route summary hw` outputs will differ as compared to the actual capacity of the HW for IPV4/IPV6 LPM route installation. As a result, when trying to scale to the maximum supported limits that are shown in the PFE output, will result in route installation errors/table full errors in the PFE. PR1841913
- There exists a hidden CLI upgrade option to do "clean-install". Using CLI upgrade with this option will do a "nist" compliant secure-erase for SATA disks. This method of CLI upgrade needs to be used with caution since this will wipe clean all configs/logs/files on the SATA FS and re-install the image. PR1847058
- On Junos OS EX4000 and QFX5120 platforms, the system fails to retrieve the necessary analyzer details. This prevents the port mirroring action from being applied in the filter entry. Consequently, the system defaults to the reject action, causing the traffic to be dropped, and packet captures do not appear.PR1856361

## 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

## User Interface and Configuration

- On all Junos OS platform, 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

- JDI_REG::QFX5200:: After ISSU upgrade, device is hanged and not able to perform any operations until USB recovery done on device. PR1703229
- JUNOS_REG: QFX5110-48S : "mge" interface is going down after performing soft OIR. PR1757704
- 100G optics set to CAUI4 on Junos QFX5200-32C platforms. PR1758868
- Interface flap occurring unexpectedly on Junos OS QFX platforms. PR1777336
- QFX5000 : The pps rate for egress interface becomes zero after removing one of VCP ports. PR1786119
- The port class is not captured in cint trace output for individual ports. PR1786399
- Nexthop is not getting uninstalled from FPC and is throwing errors causing traffic drop. PR1789507
- Layer 3 multicast traffic gets dropped when a BD is configured with IRB as the source interface. PR1793772
- The 100G VCP will go down upon restarting or upgrading the device. PR1796218

- Auto-channelization is showing inconsistent behaviour on QFX platforms when there is fault on the channels. PR1799073
- The default port behaviour is not working as expected after deleting VOIP (Voice over IP) configuration on an access interface. PR1802455
- VRRP Gateway IP Unreachability. PR1802615
- When VC-mode is set to HGOE and converting port type from vc-port to network port, traffic loss is observed. PR1806262
- VRRP multicast packets coming from external hosts connected to the EVPN-VXLAN fabric might get duplicated on QFX10000 platforms. PR1808040
- CPU utilization of the rpd process stays high on all Junos OS platforms. PR1808463
- The Layer 3 Multicast traffic will be dropped in an OISM scenario when an egress interface is configured with native-vlan /Access mode. PR1808816
- The "unknown-unicast-forwarding" feature is allowed to be configured even though it is not supported for the target platform. PR1810120
- IPv6 NS packets not forwarded to access port due to VXLAN snoop entry. PR1810169
- Link won't come up on bounce of fec91 on QFX5120 platform. PR1810740
- Multiple services and protocols does not work on the backup member with 100G port used as VC interconnect port on QFX5110-48S. PR1811701
- Persistent MAC getting stuck in the SRP state results in traffic loss in the EVPN-VxLAN scenario. PR1812482
- IPv6 transit traffic is getting impacted in a rare scenario with Longest Prefix Match (LPM) profile configuration. PR1813250
- Configuring Multiple VLAN-ID-list on an interface will not program all the VLANs on QFX5110 devices. PR1813454
- The traffic loss is observed if both Layer 3 unicast and VTEP next hop are used to reach same destination. PR1814387
- ARP resolution issues might happen when VxLAN and non-VxLAN are both configured on the same ifd but different ifl. PR1815250
- MAC addresses learnt on interfaces part of VLAN with MAC limiting by interface and "drop-and-log" action configured are cleared after VLAN description is changed. PR1816049
- DHCP snooping issue observed on Access Ports with IRB and VXLAN configuration. PR1816445

- EVO(EVPN Fabric): DHCP packets are getting relayed even after deleting the dhcp relay configuration from the leaf. PR1817061
- On Junos OS Evolved platforms, any new Layer 2 functionality doesn't work when ELP configuration is not present on the connected device(s). PR1818022
- On QFX10002-60C, after upgrading or rebooting, random failures might occur on 10G links. PR1818082
- On Junos QFX5000 series platforms multicast traffic impact is observed after device reboot. PR1818740
- An error log message is seen for every DHCP transaction. PR1818909
- Traffic received over the Type-5 tunnel is getting dropped due to the network port not having the correct flags set in the pure Type-5 EVPN-VXLAN scenario. PR1819073
- Egress-link-protection in combination with IGMP/MLD snooping breaks snooping functionality. PR1820318
- Traffic drop is seen in an EVPN multihoming scenario when mac-pinning is enabled. PR1820882
- L2TP Processing Issue on QFX platforms with Tagged CDP VTP and UDLD frames. PR1821012
- Traffic loss is seen in an EVPN-VXLAN scenario when an Layer 2 underlay interface is configured using a service provider style. PR1821549
- QFX : dfw ERROR is seen whenever collecting RSI. PR1823280
- In virtual-chassis after routing-engine switchover traffic of type 5 routes of EVPN-VXLAN are not getting forwarded. PR1823764
- Restricted Proxy ARP feature does not work as expected. PR1824023
- Rebooting one linecard or FPC will cause the virtual-chassis on the QFX5000 devices to forward traffic in backup RTG interface. PR1824750
- IPv6 PTP packets are getting dropped resulting in PTP synchronization issues. PR1827299
- ARP not learned on Switch Leading to Traffic Drop in EVPN-VXLAN setup. PR1827648
- Junos OS QFX5000 configured with l2circuit stops forwarding traffic on IFD with vlan-ccc encapsulation subunit when deleting or adding one of the IFLs. PR1830828
- The "unknown-unicast-forwarding" feature is allowed to be configured even though it is not supported for the target platform. PR1831498
- VXLAN overlay traffic is tagged with a native VLAN when an underlay NNI is configured with a native VLAN on all Junos QFX5000 platforms. PR1834627

- On all Junos OS QFX5000 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
- Traffic drops are observed in the EVPN-VxLAN scenario due to VPLAG flaps. PR1842475
- Unnecessary trace log files related to licenses are generated. PR1845079

## EVPN

- Error messages are observed after performing a VLAN name change with EVPN configuration. PR1806660
- EVPN-VXLAN Egress Link Protection Incompatibility with STP Affecting FRR Performance. PR1815823
- Command `set protocols evpn designated-forwarder-preference-least` is not working well. PR1823351
- Continuous kernel log messages are observed once the EVPN-VXLAN fabric is up. PR1826772

## Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596). PR1802329
- Console login fails when authentication-order is configured under 'system services' hierarchy on all Junos OS platforms. PR1826666

## Routing Protocols

- Junos OS: Multiple vulnerabilities resolved in OpenSSL (CVE-2024-4741, CVE-2024-2511). PR1815253
- eBGP sessions not going down after deleting confederation AS number. PR1826529

## User Interface and Configuration

- The commit fails error can be seen when configuration is modified after commit prepare. PR1799215
- The mgd process crashes while using an FQDN in conjunction with the ephemeral configuration database. PR1825728

## Virtual Chassis

- QFX5120 Virtual Chassis (VC) drops Address Resolution Protocol(ARP) packets from remote leaf. PR1773425

## 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**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 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 24.4R1-S3

SUMMARY

IN THIS SECTION



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

### Interfaces

- **Port profile mode with predefined profiles and customizable port speeds (SRX4700)**—You can activate a set of ports using predefined Port Profiles (A through E, C as default), each with default port speeds, providing a structured configuration approach. After activation, you have the flexibility to manually adjust the speed of individual ports, enhancing customization compared to PIC mode. This feature supports various configurations, including up to 1x400G, 6x100G, and 8x50G port arrangements, depending on the profile selected. See Port Speed on SRX4700 Firewalls.

# 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 SRX4700 Firewall**—The SRX4700 is a 1-RU fixed form-factor firewall offering next-generation firewall capabilities. The SRX4700 targets medium to large enterprise edge, campus edge, data center edge firewall, data center core firewall, and secure VPN concentrator or router for distributed enterprise use cases. These use cases include SD-WAN, and service provider roaming firewall, N6/Gi firewall, distributed security gateway, and core security gateway.

**Table 9: SRX4700 Firewall Feature Support**

| Feature | Description |
|---|---|
| Chassis | • Chassis management support. The SRX4700 supports chassis management features, such as:<br>  • Facilitate maintenance and system upgrades.<br>  • Manage voltage and temperature sensors to improve system reliability and stability.<br>  • Offer clear visual indicators through LED control for system components, aiding quick diagnostics and status evaluations.<br>  • Optimize thermal management by adjusting fan speeds based on conditions, extending hardware lifespan, and assuring optimal operating conditions. Use the `show chassis enhanced-temperature-thresholds` command to view the temperature threshold values.<br>[See show chassis enhanced-temperature-thresholds and Chassis-Level User Guide.] |
| Class of service (CoS) | • Support for CoS<br>[See Understanding Class of Service.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| Hardware | • The SRX4700 is a compact 1-RU form factor, high-performance, next generation firewall offering scalable security services. The firewall supports 1.4-Tbps Internet mix (IMIX) throughput, making it ideal for service providers, cloud providers, and large enterprises. In addition, enterprises can deploy the SRX4700 as data center core and data center edge firewalls and as a secure SD-WAN hub.<br><br>The SRX4700 is a 1-U chassis with the following ports:<br><br>• Two 400GbE QSFP-DD ports<br>• Ten 100GbE QSFP28 ports<br>• Sixteen 50GbE SFP56 ports<br>• Two 1GbE SFP HA ports<br><br>[See SRX4700 Firewall Hardware Guide.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| High availability (HA) and resiliency | • Support for BFD<br>  • Support up to 3 x 300-millisecond (ms) failure detection time<br>  • Support up to 100 BFD sessions<br>  [See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.]<br>• Support for Multinode High Availability (MNHA) in active/backup mode in routing, hybrid, and default gateway deployments.<br>  [See Multinode High Availability.]<br>• Support for IPsec VPN tunnels in an MNHA setup<br>  [See IPsec VPN Support in Multinode High Availability.]<br>• Resiliency support for platform components on SRX4700 devices<br>  [See Resiliency.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| Install and Upgrade | • Support for firmware (`jfirmware`)<br><br>[See Installing and Upgrading Firmware, request system firmware upgrade, and show system firmware.]<br><br>• Support for BIOS, Secure Boot, and bootloader<br><br>[See Upgrading the Boot Loader on SRX Series Devices and Junos OS Overview.]<br><br>• Support for secure zero-touch provisioning (SZTP)<br><br>[See Secure Zero Touch Provisioning and Generate Secure ZTP Vouchers.]<br><br>• Support for switching between SZTP and ZTP<br><br>[See Switching between Secure Zero Touch Provisioning and Zero Touch Provisioning.] |
| Interfaces | • Port configuration and supported speeds. SRX4700 features a Packet Forwarding Engine logically divided into two identical Physical Interface Cards (PICs).<br><br>Each PIC provides 14 front-panel ports configured with a mix of high-speed interfaces (1x400GbE, 5x100GbE, and 8x50GbE) ensuring a high-density networking solution for various high-throughput applications.<br><br>[See Port Speed on SRX Series Firewalls.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| Junos telemetry interface | Support for telemetry streaming with operational state sensors under the following resource paths:<br>• **/junos/events**<br>• **/junos/task-memory-information/**<br>• **/interfaces/**<br>• **/components/**<br>• **/network-instances/network-instance/protocols/protocol/bgp/**<br>• **/network-instances/network-instance/protocols/protocol/isis/levels/level/**<br>• **/network-instances/network-instance/protocols/protocol/isis/interfaces/interface/**<br>• **/network-instances/network-instance/mpls**<br>• **/lacp/**<br>• **/lldp/**<br>• **/arp-information/**<br>• **/nd6-information/**<br>• **/ipv6-ra/**<br>[See Junos YANG Data Model Explorer.] |
| J-Web | • J-Web support.<br>You can monitor, configure, troubleshoot, and manage SRX4700 Firewalls using J-Web.<br>[See The J-Web Setup Wizard, Dashboard Overview, Monitor Interfaces, and About Reports.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

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

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| MACsec | • Support for Media Access Control Security (MACsec) on physical interfaces for Layer 3 traffic.<br><br>This implementation of MACsec supports:<br><br>• Alignment with IEEE 802.1AE and IEEE 802.1X-2010 standards<br><br>• Static connectivity association key (CAK) mode with preshared keys (PSKs)<br><br>• Switch-to-switch port protection<br><br>• The encryption types GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128, and GCM-AES-XPN-256<br><br>• Revenue port in standalone mode<br><br>[See Configuring MACsec.] |
| Optics | • Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available<br><br>[See Hardware Compatibility Tool.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| Services applications | • Express Path<br>[See Express Path Overview and enhanced-mode.]<br>• Support for Application Layer Gateway (ALG)<br>[See ALG Overview.]<br>• Support for DNS<br>[See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.]<br>• Support for user authentication<br>[See User Authentication Overview.]<br>• Support for security policies<br>[See Configuring Security Policies.]<br>• Support for security zones<br>[See Security Zones.]<br>• Support for Network Address Translation (NAT)<br>[See NAT Configuration Overview.]<br>• Support for screens options for attack detection and prevention<br>[See Screens Options for Attack Detection and Prevention.]<br>• Support for traffic processing<br>[See Traffic Processing on SRX Series Firewalls Overview.]<br>• Support for integrated user firewall<br>[See Configure Integrated User Firewall.] |

**Table 9: SRX4700 Firewall Feature Support *(Continued)***

| Feature | Description |
|---|---|
| | • Support for PowerMode IPsec (PMI)<br>[See PowerMode IPsec.]<br>• Support for DHCP<br>[See DHCP Overview.]<br>• Support for GTP and SCTP<br>[See Monitoring GTP Traffic and SCTP Overview.]<br>• Support for on-box reporting<br>[See report (Security Log).]<br>• Support for inline active flow monitoring<br>[See Understand Inline Active Flow Monitoring.]<br>• Support for TWAMP<br>[See Understand Two-Way Active Measurement Protocol.]<br>• Support for RPM<br>[See Real-Time Performance Monitoring for SRX Devices.]<br>• Support for logical systems<br>[See Logical Systems Overview.] |

## Application Identification (AppID)

- **Application signature package enhancements (SRX Series Firewalls)**—We've enhanced the application signature package feature to:
  - Facilitate two types of downloads—major version (IDP signatures, IDP detector, and application identification protobundle) and minor version (regular signature updates).
  - Enable the application signature engine to communicate the status back to the signature package server for installation success or failure (update failures or package errors). The engine stops the installation when errors occur, reverts to the previous version, and reports the status to the

server. If multiple devices report a faulty application signature package, the server analyzes the data, marks the package as invalid, and prevents future downloads.

See [ Predefined Application Signatures for Application Identification].

- **Enhancements to application identification (SRX Series Firewalls and vSRX Virtual Firewall)** —We've introduced the following enhancements to application identification:
  - Offline installation of an application signature package from a local TAR file
  - CLI command or system log message that generates a list of deprecated application groups
  - Improvements in the policy lookup process for micro-applications.

  See [Predefined Application Signatures for Application Identification.]

## Connected Security Distributed Services (CSDS) Architecture

- **CSDS Architecture (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The Connected Security Distributed Services (CSDS) Architecture delivers a scalable, distributed security architecture design that fully decouples the forwarding and security services layers. In this design, MX Series routers serve as intelligent forwarding engines for load balancing while SRX Series Firewalls help expand your data centers securely. The solution supports carrier-grade NAT (CGNAT), IPsec VPN, and stateful firewall security services.

  The architecture ensures redundancy in forwarding and services layers. It uses ECMP-based consistent hashing for the routers, and Multinode High Availability for the physical and virtual firewalls.

  You can manage nodes with Junos Node Unifier (JNU) and orchestrate vSRX Virtual Firewalls with Junos Device Manager (JDM).

  [See Connected Security Distributed Services Architecture Deployment Guide, and Release Notes: Connected Security Distributed Services Architecture.]

- **Junos Node Unifier support in CSDS for unified CLI management (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—We support centralized management of devices in the Connected Security Distributed Services (CSDS) Architecture with the Junos Node Unifier (JNU) single-touchpoint solution. The JNU topology uses MX Series routers as JNU controllers, and SRX Series Firewalls and Junos Device Manager (JDM) as JNU satellites. From the controller, you can perform the following operations on the satellites:
  - Configure and manage the nodes using Junos OS configuration commands.
  - Run Junos OS operational mode commands.

[See Junos Node Unifier for CSDS, request jnu satellite sync, show chassis jnu satellite, and jnu-management.]

## Content Security

- **Web proxy support for Content Security Sophos 2.0 antivirus and reputation-based file blocking (cSRX, SRX Series Firewall, and vSRX)**—Content Security Sophos 2.0 antivirus now supports web proxy. In addition, we introduce the following file reputation groups to control traffic and provide more control over security:

  - Malware
  - Potentially unwanted applications
  - Unknown
  - Known good or clean

  The Sophos antivirus blocks the traffic if the file reputation belongs to the malware group and permits the known good or clean group traffic. You can define the action for the potentially unwanted applications and unknown group traffic based on your requirements.

  [See Sophos Antivirus Protection Overview, server (Security Sophos Engine Antivirus), sophos-engine, notification-options (Security Antivirus), show security utm anti-virus status, and show security utm anti-virus statistics.]

## Device Security

- **Maintain flow session stability during policy configuration changes (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—You can maintain flow session stability during security policy configuration commits. Changes such as policy match condition modifications, policy addition or deletion, policy swap, or policy order alteration can disrupt flow sessions. These disruptions can affect Packet Forwarding Engine configuration data, potentially impacting ongoing policy searches and leading to incorrect or default policy selection.

  To prevent this disruption and to maintain flow session stability, use the `set security policies lookup-intact-on-commit` command.

  [See Configuring Security Policies.]

- **Enhanced policy configuration synchronization (SRX Series Firewalls and vSRX Virtual Firewall)**—Use file serialization to propagate policy configuration changes to the data plane. This method serializes policy configurations into files, ensuring that the Packet Forwarding Engine applies them reliably.

  Enabled by default, file serialization minimizes security policy mismatches and boosts system reliability.

  [See Configuring Security Policies and file-serialization.]

## Intrusion Detection and Prevention

- **Support logging for exempt rule matching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Use exempt rule logging in the IDP system to monitor and analyze traffic patterns, detect potential security threats, and troubleshoot network issues. Administrators can examine logs to gain insights into traffic exempt from IDP rules and make informed network policy decisions. Enable logging functionality for exempt rules at the rule level for fine-grained monitoring and analysis of security events, enhancing system visibility.

  [See Support logging for exempt rule matching.]

- **IDP signature package server-side improvements (cSRX, SRX Series Firewalls, and vSRX3.0)**—The IDP system now reports installation status to the signature server. The signature server uses information from multiple devices to decide if a signature package fails the integrity check globally. If a signature package does not pass integrity checks globally, it becomes unavailable for future downloads.

  [See IDP signature package server-side improvements.]

- **IDP intelligent offload per protocol (cSRX, SRX Series Firewalls, and vSRX 3.0)**—The protocol-specific Intelligent-Offload Configuration feature in IDP enables administrators to set inspection depth limits for different protocols. Administrators can use this capability to enable or disable offloading on a per-protocol basis and to configure specific offload limits for protocols such as SSH and FTP. This flexibility optimizes resource usage and ensures efficient session inspections.

  Use the options in the `set security idp sensor-configuration global intelligent-offload-tunable` CLI command to modify the offload settings, specify the protocol, and adjust the offload limit.

  [See Intrusion Detection and Prevention Overview.]

## Network Address Translation (NAT)

- **Monitor subscriber port utilization (cSRX, MX240, MX480, MX960, SRX1500, SRX1600, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX3.0)**–You can monitor and manage port utilization when deploying Carrier Grade Network Address Translation (CGNAT).

  Configure threshold limits to receive notifications when port or port block usage exceeds the configured thresholds.

  - If a pool is configured as Port Block Allocation (PBA) and a subscriber uses more port blocks than the threshold, a notification is generated.
  - For Deterministic NAT (DETNAT) pools, if a subscriber uses more ports than the threshold in the allocated block, a notification is generated.

  The system log messages are:

- RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_RAISE: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 90%, current: 100%`

- RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 50%, current: 25%`

- RT_SRC_NAT_SUBS_POOL_ALARM_RAISE

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING: Subscriber IP: 10.1.1.2, NAT pool: pool-name, threshold alarm [raise, clear] suppressed for 2 times in last 10 seconds`

[See jnxJsSrcNatSubThresholdStatus, jnxJsNAT, Monitor Subscriber Port Utilization Using Carrier Grade NAT, subscriber-pool-utilization-alarm, and pool-utilization-alarm (Security Source NAT Pool).]

- **PMI support for DS-Lite tunnel (cSRX, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Enhance DS-Lite tunnel performance by reducing instruction cache misses and optimizing the packet processing path. Use Packet Management Interface (PMI) for DS-Lite tunnel processing, which includes: encapsulate IPv4 packets within an IPv6 header using Vector Packet Processing (VPP), decapsulate by stripping the IPv6 header to process the inner IPv4 packet, and handling post-fragmentation of DS-Lite encapsulated traffic if it exceeds the tunnel's Maximum Transmission Unit (MTU).

  [See IPv6 Dual-Stack Lite]

- **Support for DS-Lite fragmentation (SRX Series Firewall)**—Configure the pre-fragmentation and post-fragmentation MTU options on Dual-Stack Lite (DS-Lite) tunnels.

  - Pre-fragmentation–Enable or disable pre-fragmentation or clear the df bit in the IP packet.
  - Post-fragmentation–Enable or disable post-fragmentation to fragment the IPv6 packet. By default, post-fragmentation is off. When enabled, the IPv6 packet fragments; otherwise, if the MTU exceeds, an ICMP error message is sent to the originator.

  [See softwire-name.]

- **NAT IPv6 with DS-Lite in SOF (SRX4600, SRX5400, SRX5600, and SRX5800 firewalls with IOC3 card)**—Use NAT IPv6 with Dual-Stack Lite (DS-Lite) service offload to encapsulate IPv4 packets with IPv6 headers to enable traversal through IPv6 networks. This feature offloads DS-Lite packet processing to the Network Processing Unit (NPU), optimizing performance and reducing CPU load on the Services Processing Unit (SPU). Enable service offload for a DS-Lite softwire concentrator (SC) using the `set security softwires softwire-name service-offload` command. Disable it with the `set security softwires softwire-name service-offload off` command. New sessions will not be offloaded, but existing ones remain unchanged.

  [See IPv6 Dual-Stack Lite]

## Platform and Infrastructure

- **Improvements to infrastructure and optimization of the software architecture for Junos OS (SRX300, SRX320, SRX340, SRX345, SRX380)**—We've improved the infrastructure and continued our work in optimizing the software architecture further for these devices so that they align with the other SRX Series Firewalls. These improvements impact system infrastructure and booting, system snapshot and recovery, and software installation, upgrade, and downgrade procedures.

  **System infrastructure and booting:**

  - Because upgrading or downgrading now restructures the file system, you may lose the log files and configuration. Therefore, save the configuration and important log files before you upgrade or downgrade.
  - The system is now divided between two volumes, the **/junos** volume and the **/oam** volume. The **/junos** volume is the main drive and contains all the software and files needed for the day-to-day running of the device, including configuration information and logs. The **/junos** volume also contains non-recovery snapshots, which are new with Junos OS Release 24.4R1. You cannot use the non-recovery snapshots to recover a failed system. The **/oam** volume contains the recovery snapshot, which provides the ability to boot from the **/oam** volume when a failure occurs.
  - The boot partition now has read-write permissions.
  - The software no longer supports the Network File System (NFS) `mount` shell mode command.

  **System snapshot and recovery:**

  - This release includes changes to the `request system snapshot` and `request system reboot` commands and adds a new `request system recover` command.
  - We have deprecated the `request system autorecovery` command. Instead, use the `request system snapshot` command.
  - We have deprecated the `request system software delete-backup` command. Instead, use the `request system snapshot delete` *`snapshot-name`* command.
  - See *KB 85650* for information on how to recover the device when the device does not boot properly.

  **Software installation, upgrade, and downgrade:**

  - In Junos OS Release 24.4R1, there are several installation packages instead of one. These packages include one for each installation method:

**Table 10: New Package Prefixes**

| Installation Method | Package prefix |
|---|---|
| CLI | `junos-install-srxsme-mips-64*` |
| Network install with tftp using the loader | `junos-install-media-net-srxsme-mips-64*` |
| Install from the USB driver | `junos-install-media-usb-srxsme-mips-64*` |

The firmware is delivered in a separate package, and the prefix for that package is `jfirmware-srxsme-mips-64*`.

- For Trivial File Transfer Protocol (TFTP) or USB installation, you must first upgrade the U-Boot software to version 3.15 or later before upgrading to Junos OS Release 24.4R1. You must also upgrade the loader to a build from the year 2023 or later. During the boot process, the loader reveals the build date. For example, this loader was built on May 23, 2023:

```
FreeBSD/mips U-Boot loader, Revision 2.0
(2023-05-23 22:48:57 builder@host)
```

  Once you install Junos OS Release 23.4R2-S3 or Release 24.2R2, the Junos OS image contains the latest boot loader binaries in these paths: **/boot/uboot** and **/boot/veloader**. You can upgrade the U-Boot software and veloader software as follows:

  - From the CLI prompt, enter the `start shell` command.
  - From the shell prompt, update the U-Boot software with the `bootupgrade -u /boot/uboot` command.
  - From the shell prompt, update the veloader with the `bootupgrade -l /boot/veloader -x` command.
  - Reboot the device. Once the device is back up, you can use a USB drive or TFTP to upgrade to Junos OS Release 24.4R1.

- Before upgrading to Junos OS Release 24.4R1, you must first upgrade to either Release 23.4R2-S3 or to Release 24.2R2. To upgrade to either of these releases, use either of the following commands depending on the device type:

  - `request system software add` *`package-name`* `partition no-copy no-validate reboot` for the SRX300, SRX320, SRX340, and SRX345 firewalls.

- `request system software add package-name no-copy no-validate reboot` for the SRX380 firewall.

  To upgrade from either of these releases to Release 24.4R1, you must use the `request system software add package-name no-copy no-validate reboot` command. To downgrade from Junos OS Release 24.4R1, you must first downgrade to either Junos OS Release 23.4R2-S3 or to Release 24.2R2 before downgrading to any other release. To downgrade the software, you must use the `request system software add package-name no-validate` command.

  If you have chassis clusters, you cannot use the In-Band Cluster Upgrade (ICU) method for this particular upgrade or downgrade. Because of the infrastructure changes, you cannot use the ICU method to upgrade from or downgrade to either Junos OS Release 23.4R2-S3 or to Release 24.2R2. You can use either the procedure outlined in *KB 85650* or the minimal downtime procedure documented in KB17947 (Minimal_Downtime_Upgrade_Branch_Mid PDF file). Once you have upgraded to Junos OS Release 24.4R1, you can use the ICU method to upgrade to any later releases or downgrade from one of those later releases to Junos OS Release 24.4R1 or later.

- Because of the disk re-partitioning that occurs when you upgrade to or downgrade from Junos OS Release 24.4R1, you must be mindful of the following:

  - You cannot use the `request system rollback` command to roll back from Junos OS Release 24.4R1 to either Junos OS Release 23.4R2-S3 or to Release 24.2R2. Instead, you must treat the rollback as a downgrade, and use the `request system software add package-name no-validate reboot` command.

  - When upgrading to or downgrading from Junos OS Release 24.4R1 on your device using TFTP or USB to install the software, after the device reboots, it comes up in Amnesiac state. Therefore, before you install, make sure you have saved the configuration file so that you can more easily reconfigure the device from the console port.

  [See Recovering Junos OS on a Device Running Junos OS with Upgraded FreeBSD, How to Recover Junos OS with Upgraded FreeBSD, Autorecovery of Configuration, Licenses, and Disk Information on SRX Series Firewalls, Installing Software on SRX Series Firewalls, Junos OS Installation Package Names, request system reboot (Junos OS with Upgraded FreeBSD), request system snapshot (Junos OS with Upgraded FreeBSD), show system snapshot (Junos OS with Upgraded FreeBSD), and request system recover.]

## 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.]

## Software Installation and Upgrade

- **LTS22 Support (SRX1500, SRX4100, and SRX4200)**—We are transitioning from WRL6 to Wind River Linux LTS22 (LTS22), upgrading the kernel to version 5.15.106. This change unifies the VMHOST kernel across SRX Series Firewall Routing Engine cards while keeping the same feature set as WRL6. The upgrade process remains seamless, allowing all current features and modules to function as expected.

## VPNs

- **Passive mode tunneling support (SRX4600)**—Enable this feature using the configuration statement `set security ipsec vpn vpn-name passive-mode-tunneling`. The feature allows you to perform IPsec tunneling of malformed packets bypassing the usual active IP checks, TTL checks, and fragmentation.

  See [passive-mode-tunneling (security), show security ipsec security-associations, and show security ipsec inactive-tunnels.]

- **Enhanced QoS using DSCP per SA in IPsec VPN with iked process (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—We provide traffic classification support with Differentiated Services Code Point (DSCP) per security association (SA) in IPsec VPNs using the iked process. This feature is available when you run the IPsec VPN service without the PowerMode IPsec (PMI) mode configuration. It allows your VPN gateways to negotiate separate child SA for each CoS type.

  [See CoS-Based IPsec VPNs, show security ipsec security-associations, and show security ipsec statistics.]

- **Juniper® Secure Connect integration with JIMS (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The SRX Series Firewalls can send Juniper Secure Connect's remote access VPN connection state events to Juniper® Identity Management Service (JIMS) using the push to identity management (PTIM) solution. By default, Junos OS enables this feature when you use `identity-management` at the `[edit services user-identification]` hierarchy level.

  You can use the following options to configure this feature:

  - `no-push-to-identity-management` at the `[edit security ike gateway gateway-name aaa]` hierarchy level to disable the iked process communication with JIMS.

  - `user-domain` at the `[edit security remote-access profile realm-name options]` hierarchy level to optionally configure the domain alias name.

  See [Juniper Secure Connect Integration with JIMS, identity-management, and profile (Juniper Secure Connect).]

- **Migration of policy-based VPNs to route-based VPNs (cSRX, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Migrate

policy-based VPNs to route-based VPNs when you run the IPsec VPN service with the iked process. You must configure multiple VPN objects on a shared point-to-point `st0` logical interface to perform the migration.

[See Shared Point to Point st0 Interface and Migrate Policy-Based VPNs to Route-Based VPNs.]

- **SAML-based user authentication in Juniper® Secure Connect (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Juniper Secure Connect remote access VPN supports user authentication using Security Assertion Markup Language (SAML) version 2. To perform the remote user authentication using SAML, run the VPN service using the iked process on your firewall and ensure you have the SAML-supported Juniper Secure Connect application.

  Configure SAML service provider and identity provider settings at the `[edit access saml]` hierarchy level. Enable SAML settings in the access profile configuration using the `set access profile` *`profile-name`* `authentication-order saml` command.

  See [SAML Authentication in Juniper Secure Connect, saml, authentication-order (access-profile), saml (Access Profile), saml-options, show network-access aaa saml assertion-cache, show network-access aaa statistics, request network-access aaa saml load-idp-metadata, request network-access aaa saml export-sp-metadata, clear network-access aaa saml assertion-cache, clear network-access aaa saml idp-metadata, and clear network-access aaa statistics.]

- **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.

- **Supported transceivers, optical interfaces, and DAC cables (SRX Series)**—Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach

copper (DAC) cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.

- **Enhanced Address Detection for Reliable Connectivity (ACX5448-M, MX10008, MX10016, SRX5800, and QFX10008)**—We've improved our network address detection process to deliver more reliable connectivity and uninterrupted performance. This update prevents disruptions caused by duplicate address detection (DAD) failures under rare network conditions. By integrating advanced algorithms and unique identifiers, we reduce false detections and ensure smooth data flow, keeping your network running seamlessly.

## What's Changed

IN THIS SECTION



Learn about what changed in this release for SRX Series.

## Content Security

- **Juniper NextGen Web filtering license warning enhancement (SRX Series and vSRX)**—Starting in Junos OS Release 24.4R1, if you configure the Web Filtering type as `juniper-enhanced` or `ng-juniper` without a corresponding valid license, the system does not generate a warning message. You can confirm whether the Web Filtering is down due to a missing license using the `show security utm web-filtering status` comamnd.

  Earlier to this release, if you configure Web Filtering type as `juniper-enhanced` or `ng-juniper` without a valid license, the system generated a warning message.

[See show security utm web-filtering status and Juniper NextGen Web Filtering Overview.]

## Interfaces and Chassis

- **Autonegotiation in xe ports (SRX380)**—Starting in Junos Release 24.2R2, autonegotiation is disabled by default on all the four xe ports of SRX380 Firewalls. It is recommended to disable the autonegotiation at the remote end devices. To change the autonegotiation default recommended behavior, use the `set interfaces xe-x/y/z gigether-options auto-negotiation` command.

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## Network Management and Monitoring

- **DES deprecation for SNMPv3 (Junos)**—The Data Encryption Standard (DES) privacy protocol for SNMPv3 is deprecated due to weak security and vulnerability to cryptographic attacks. For enhanced security, configure the triple Data Encryption Standard (3DES) or the Advanced Encryption Standard (CFB128-AES-128 Privacy Protocol) as the encryption algorithm for SNMPv3 users.

  [See privacy-3des and privacy-aes128.]

## PKI

- **Enhancement to fix output with Junos PyEz for duplicate keys in PKI (MX Series, SRX Series, EX Series)**—In earlier releases, though the CLI output displayed all the duplicate keys for the corresponding hash algorithms in PKI using `show security pki local-certificate detail | display json`

command, for the same requested data, Junos PyEz displayed the last key only. Starting this release, the CLI output and the PyEz displays all the duplicate keys with the enhanced tags.

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the `Hostname` field first instead of last. The `show version` command output includes the `Family` field. The `Family` field identifies the device family under which the device is categorized, for example, `junos`, `junos-es`, `junos-ex`, or `junos-qfx`.

  [See show system information and show version.]

## VPN

- **Compliance check is added for Juniper Secure Connect (SRX Series, and vSRX 3.0)**—In Junos OS, we have added a compliance check to enforce that only Juniper Secure Connect clients can establish remote access VPN connections, and to reject connection requests from non-compliant remote access clients. You'll notice this behavior for the VPN connection using the remote access profile attached to the IPsec VPN object.

- **Changes to syslog messages for IPsec VPN service (SRX Series, and vSRX 3.0)**—We've made changes to the syslog messages for the IPsec VPN service. You'll notice that: Tunnel-id field is added to the KMD_PM_SA_ESTABLISHED syslog messages when running IPsec VPN service using the kmd process. - New syslog message IKE_VPN_SA_ESTABLISHED is added for an IPsec rekey event when running IPsec VPN service using the iked process.

- **Changes to the lifetime-kilobytes option in IPsec VPN Security Association (SRX Series Firewalls, and vSRX 3.0)**—The minimum allowed IPsec proposal lifetime-kilobytes value is changed from 64KB to 64000KB for IPsec VPN Security Association.

  [See proposal (Security IPsec).]

- **Changes to syslog messages for IPsec VPN service (SRX Series, and vSRX 3.0)**—We've made changes to the syslog messages for the IPsec VPN service. You'll notice that: - Tunnel-id field is added to the KMD_PM_SA_ESTABLISHED syslog messages when running IPsec VPN service using the kmd process. New syslog message IKE_VPN_SA_ESTABLISHED is added for an IPsec rekey event when running IPsec VPN service using the iked process.

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the `ipados` option at the `[edit security remote-access compliance pre-logon` *`name`* `term` *`name`* `match platform]` hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

## Known Limitations

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 command 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. PR1830053

### 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, SRX5000 line of devices, BFD ICL will flap. PR1789245

## Flow-Based and Packet-Based Processing

- On Junos OS SRX Series Firewall running as L3 VNI gateway in EVPN-VXLAN scenario, traffic drops will be observed if traffic passes through two VXLAN tunnels and traffic fails to cross the two VXLAN tunnels when the Packet Forwarding Engine is processing the packet having same remote IPs for two VXLAN tunnels. PR1847419

## General Routing

- Additional logging has been added to the primary 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
- On all Junos and Junos Evolved platforms, repd core observed during ISSU.PR1797189
- On SRX4100 and SRX4200 devices, starting and stopping the monitor traffic interface, causes the VPN tunnel or tagged traffic to be dropped. However, keeping the monitor traffic interface running, ensures that traffic will function properly. Issue occurs when monitor interface command on an interface is performed on devices that has vlan-tagging configured. PR1808353
- On SRX5600 and vSRX3.0, while upgrading from Junos OS release to 22.4R3-S1 or 22.4R3-S2, the upgrade process can fail as the rpd process stops as part of validation process. This is seen if the router configuration has Multicast or IGMP or BBE configuration. PR1810817
- MACSec is supported in routing mode but not in transparent mode. PR1812427
- On SRX1500 device, large IP packets of size 1470 bytes or larger might be dropped when using ethernet-switching and trunk ports.PR1813536
- On vSRX3.0 platforms using SWRSS L2HA configured, traffic loss for RTO traffic might be observed and on secondary node sessions not getting cleared and sessions reaching maximum limit of 12M. The issue happens when RTO traffic not evenly distributed to all flow threads over the fabric interface. PR1819911
- Use the -O option on remote host while initiating scp file transfer or enable sftp-server. PR1827152
- If the IDP security-package is installed multiple times, it will cause sigpack installation failure as the AppID memory allocation got failed. PR1832094
- On SRX300 line of devices configured with custom applications and a signature package already installed, installing a new sigpack might result in the failure to recompile the custom applications, causing detection failures. During Layer 4 to Layer 7 traffic processing, custom applications might be incorrectly marked as INCONCLUSIVE, impacting application detection. PR1833667
- Link aggregation on SRX1600 does come up with flexible vlan tagging enabled on aggregated port. PR1838033
- In the MIPS and FIPS mode, kernel panics while switching floating point state, reboots and generates a vmcore file. PR1838923
- On SRX1600, with MVRP enabled vlan learning and assignment not happening. PR1839275

- A core file is generated due to memory corruption when sigpack install is pushed from Routing Engine to Packet Forwarding Engine. PR1841520
- When upgrading to Junos OS release 23.4R1 and above, unnecessary trace log files related to licenses are generated. PR1845079
- Added missing syslog messages for SCEP and CMPv2 certificate enrollment failure. PR1845573
- On SRX380 device in packet mode, when VLAN -VPLS encapsulation is configured on an ingress interface of the PE device, the incoming packet is dropped because these packets are identified as L2 unknown unicast packets. PR1845997
- On SRX300 line of devices configured with native-vlan-id, after upgrading the device to Junos OS release 23.4R1 or higher the native-vlan-id option is missing under the interface hierarchy. This leads to a syntax error, stopping users from setting the native-vlan-id. PR1847366

## Network Address Translation (NAT)

- New RSI CLI command request support information security-components nat. PR1825372

## Platform and Infrastructure

- On SRX5000 line of devices, if vmcore is initiated for XLP PIC vmcore process stops. PR1811765
- On SRX300 line of devices, when TACACS accounting is configured, after an upgrade to Junos OS release 23.4R2-S2.1, the DHCP-relay might not work anymore and the shm-rtsdbd process might generate core files. PR1843935
- An authentication bypass by spoofing vulnerability in the RADIUS protocol allows an on-path attacker between a RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. PR1850776

## Services Applications

- On SRX5000 line of devices with HA cluster in FIPS mode, repeated manual failovers of redundancy groups can result in SPC3 or IOC4 or both the cards going offline.PR1797468

## User Interface and Configuration

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

## VPNs

- MNHA Conn State and ICL are down after 48+ hours of device being up with background traffic due to BFD flaps at regular intervals.PR1822662
- With Primary node reboot and back to back failovers after, the VPN sequence number synchronizes RTO packets between the primary node and secondary node stops for few mins after the secondary node moves to secondary state from secondary-hold state. If any failover occurs during this period, traffic loss occurs until the IPSEC sequence number on the newer primary node catches up the sequence number sent by the previous primary node.PR1842874
- FIPS using the VPN traffic-selector in an SRX Series Firewalls HA cluster, when a VPN traffic-selector configuration is committed in the backup HA cluster node, the VPN might not be present in the Packet Forwarding Engine after the configuration. This issue will prevent VPN to initiate an IKE negotiation if the VPN is triggered on-traffic locally, and the RG1+ is active at the other HA node than that of the RG0. PR1846168

## 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 flowd process might stop on HA and MNHA mode with H.323 ALG configured. PR1804025

## Chassis Clustering

- Junos OS: SRX5000 Series: Receipt of a specific malformed packet will cause a flowd crash (CVE-2024-47504). PR1821452
- MNHA configured SRX Series Firewall becomes unresponsive post manual reboot. PR1830654

## Content Security

- Memory corruption resulting in srxpfe process stops. PR1816280
- Packet Forwarding Engine process continuously cores after enabling Sophos Antivirus and large sizes from 10 MB and above are processed. PR1841398

## Flow-Based and Packet-Based Processing

- The flowd process might stop in cluster HA mode when there is a route change. PR1785993
- On SRX5000 line of devices and SRX4600, the setting apply-to-half-close-state for TCP sessions is not taking effect. PR1807505
- On SRX Series Firewall, when using IPv6 Multi-path BGP with MX configured with EVPN, transit SFW traffic experiences packet drops during IPv6 Neighbor discovery refresh. PR1817211
- On SRX4300 with 200 tenant system configured only 50 tenant system traffic is working. PR1820258
- Junos OS: SRX4600 and SRX5000 Series: Sequence of specific PIM packets causes a flowd crash (CVE-2024-47503). PR1820291
- Deleting L3 VPN vrf-group configuration causes unrelated bgp neighbor session termination. PR1821325
- AppQoS rate limit in PMI mode on SRX5000 line of devices and SRX4600 might drop packets unexpectedly. PR1828819

## General Routing

- A few line cards will be stuck in the present state and later go offline. PR1631579
- Tail drops on high priority queue or egress traffic less than maximum capacity when congestion. PR1712964
- Traffic drops are observed for incorrect destination MAC address learned in the hardware. PR1746684
- SNMP jnxLicenseAboutToExpire trap is sent every minute when an alarm license for feature name is about to expire is raised. PR1777649
- AppID failure observed post reboot of a node in redundancy group. PR1800966
- The cl interface goes down when the dl interface is disabled for link failover. PR1803966
- MVRP registration for dynamically created VLAN is not seen. PR1804268
- SRX4600 with SOF is observed to continue sending IPv6 traffic out a downed member link. PR1807541
- Traffic drop is seen when monitor traffic interface command is issued for an interface. PR1808353

- CPU utilization of the rpd process is high. PR1808463
- NSD file handles incrementing consistently in database file causing a rare condition of ssh access failure. PR1810310
- When the same virtual mac is used on multiple interfaces, a packet destined to the virtual mac will be dropped PR1810428
- The LLDP neighborship does not recover on aex. PR1811545
- Monitored status keeps up after CTL link down. PR1811858
- Batch commit might not working in HA. PR1813367
- ISSU functionality breaks in cluster and security logs configuration setup. PR1813435
- Junos OS: SRX1500,SRX4100,SRX4200: Execution of low-privileged CLI command results in chassisd crash (CVE-2025-21596). PR1814404
- False SNMP traps for PSU failure generated on Junos SRX1500 Series Firewall. PR1815083
- Junos OS: SRX Series: Low privileged user able to access sensitive information about file system (CVE-2024-39527). PR1815751
- IIC access error during commit operation cause false positive alarms in devices. PR1816912
- Routes for secure tunnel interface not installed on forwarding table. PR1817807
- Configurations commit fails due to mustd process stops. PR1818692
- The ~root/.ssh directory contents is deleted on every reboot. PR1819054
- On SRX4700, the LLMD support is enhanced. PR1819096
- The 1 G interface might be down after upgradation on SRX4600. PR1819376
- DAC interface does not send fault signal to a peer device when the DAC interface is admin disabled. PR1821368
- Device might boot in amnesiac mode and configuration commit might fail with error: Check-out failed for CASB process. PR1823224
- Unable to define NAT policy address names containing dots or slashes in J-Web. PR1823264
- High CPU utilization by the nsd process observed due to DNS common cache and multiple update handlers. PR1823978
- Juniper Secure Connect will not get connected if loopback is configured as external interface. PR1825573

- Traffic outages due to memory shortage and core files. PR1826129
- Packet Forwarding Engine might generate core files during ISSU. PR1827283
- IPsec session will flap if assigned IP for config payload request is given in full IPv6 format. PR1827426
- Flowd process might generate core files when security metadata streaming enabled and then enabling AAMW traceoptions. PR1828721
- The Packet Forwarding Engine might stop on dynamic-filter configuration. PR1830246
- Log messages related to gencfg no msg handlers' will be seen on SRX4600. PR1830290
- SSH getting timed out over IRB Global Mode switching interface. PR1833746
- The jexec process might not respond to ICMPv6 request to all nodes multicast IP. PR1834135
- The h2c upgrade header is removed even though SRX Series Firewall configured with disables upgrade strip. PR1835733
- SRX Series Firewalls default named.conf file is created with non dns-proxy related configuration changes. PR1836235
- Device alarm implementation for secondary disk boot on SRX2300, SRX4300, and SRX4700 Series Firewall. PR1838746
- The offline download of the IDP signature fails. PR1838853
- Traffic loss due to tunnel establishment failure in HA setup. PR1839090
- After performing ISSU on SRX4600, the SPM is no longer operational. PR1839346
- The srxpfe process might stop when the BFD interval is configured to less than 2 seconds in the MNHA. PR1840872
- The xe interfaces link down when IP address is assigned. PR1841080
- AAMW or flow based antivirus does not generate ACTION_LOG message when the malware is detected by URI cache. PR1841999
- The split-brain condition might be seen in SRX4600 Series Firewall configured in chassis cluster under certain conditions. PR1843413
- SRX1500 might not show jnxOperatingTemp and jnxFruTemp temperature reading for PSU temperature. PR1845407
- Packet Forwarding Engine might stop when source identity is enabled. PR1845506

- Core file might be generated for some processes while using license feature. PR1848160
- Local or peer device interface reflects down after SRX380 reboot. PR1848557

## Interfaces and Chassis

- 40 G interfaces on Junos SRX5000 line of devices cluster will go down after cluster failover. PR1809220

## Intrusion Detection and Prevention (IDP)

- The srxpfe process might stop during heavy traffic processing by IDP. PR1825279
- Memory leak might be observed when IDP is configured. PR1826377

## J-Web

- Display issue is observed when range option is used to configure destination and source port range in custom application. PR1810991
- Reload or refresh the J-Web page showing the Empty reply from server error. PR1832731
- J-Web application cannot be removed from application-set. PR1834748
- Junos OS image upload through J-Web might fail. PR1837925
- Unable to load J-Web after upgrading when time zone is set to GMT+x or GMT-x. PR1851362

## Network Management and Monitoring

- In MNHA, node configuration on primary might differ from backup due to configuration synchronization failure at the time of commit. PR1819656

## Platform and Infrastructure

- Multiple Products: RADIUS protocol susceptible to forgery attacks (Blast-RADIUS) (CVE-2024-3596). PR1802329

## Routing Policy and Firewall Filters

- Traffic might be dropped when AppID DB is not installed. PR1821890
- FQDN based security policies will not work as expected when DNS server responds with a non-positive error code or refuse responses. PR1844191
- The mgd process might stop during large amount of configurations. PR1847877

## User Interface and Configuration

- The commit fails error can be seen when configuration is modified after commit prepare. PR1799215
- The system scripts refresh might fail when using load CLI option. PR1821845

## VPNs

- High CPU on SPU might lead to FPC reboot and VPN traffic impact by not failing over to the backup node. PR1794895
- Traffic loss for VPN going down due to inconsistency between the VPN configuration in the iked and the SRG database. PR1804965
- MNHA: Stale IPsec tunnel in backup node. PR1805690
- IS-IS packets over 1500 bytes sent to L2 VPN over MPLS are not being processed. PR1807853
- Memory leak in ikemd process when deleting VPN tunnel. PR1815800
- IPsec VPN traffic disruption after a change of authentication protocol is seen on platforms running kmd process. PR1817228
- The srxpfe process might stop due to memory buffer corruption if the outgoing interface of the IPsec VPN peer goes down and the default route points to st0. PR1818197

- The show security ipsec tunnel-events-statistics displays wrong message. PR1820654
- On rare circumstances, the kmd or iked process might stop on using the third-party library API. PR1833072
- SRX Series Firewall might becomes unresponsive when SNMP requests are sent through the fxp0 interface immediately after a reboot. PR1834204
- The kmd process might stop on random number generation by the third-party library API. PR1841364

## 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**Table 11: 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

IN THIS SECTION



Learn about new features introduced in this release for vSRX.

## Application Identification (AppID)

- **Application signature package enhancements (SRX Series Firewalls)**—We've enhanced the application signature package feature to:
  - Facilitate two types of downloads—major version (IDP signatures, IDP detector, and application identification protobundle) and minor version (regular signature updates).
  - Enable the application signature engine to communicate the status back to the signature package server for installation success or failure (update failures or package errors). The engine stops the installation when errors occur, reverts to the previous version, and reports the status to the server. If multiple devices report a faulty application signature package, the server analyzes the data, marks the package as invalid, and prevents future downloads.

  See [ Predefined Application Signatures for Application Identification].

- **Enhancements to application identification (SRX Series Firewalls and vSRX Virtual Firewall)** —We've introduced the following enhancements to application identification:
  - Offline installation of an application signature package from a local TAR file
  - CLI command or system log message that generates a list of deprecated application groups
  - Improvements in the policy lookup process for micro-applications.

  See [Predefined Application Signatures for Application Identification.]

## Connected Security Distributed Services (CSDS) Architecture

- **CSDS Architecture (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The Connected Security Distributed Services (CSDS) Architecture delivers a scalable, distributed security architecture design that fully decouples the forwarding and security services layers. In this design, MX Series routers serve as intelligent forwarding engines for load balancing while SRX Series Firewalls help expand your data centers securely. The solution supports carrier-grade NAT (CGNAT), IPsec VPN, and stateful firewall security services.

  The architecture ensures redundancy in forwarding and services layers. It uses ECMP-based consistent hashing for the routers, and Multinode High Availability for the physical and virtual firewalls.

  You can manage nodes with Junos Node Unifier (JNU) and orchestrate vSRX Virtual Firewalls with Junos Device Manager (JDM).

  [See Connected Security Distributed Services Architecture Deployment Guide, and Release Notes: Connected Security Distributed Services Architecture.]

- **Junos Device Manager support in CSDS for vSRX orchestration (vSRX 3.0)**—Use Junos Device Manager (JDM) to orchestrate vSRX Virtual Firewalls in the Connected Security Distributed Services (CSDS) services plane. JDM is a Linux container that offers a Junos OS-like CLI environment for the virtual machine (VM) life-cycle management. You can use JDM to deploy and manage vSRX Virtual Firewalls on Intel or AMD baremetal servers with Ubuntu OS.

  You must use the MX Series Junos Node Unifier (JNU) controller to centrally manage JDM and vSRX Virtual Firewalls that serve as the JNU satellites.

  [See Junos Device Manager for CSDS, csds, request csds add-vsrx, request csds authenticate-host, request csds delete-vsrx, request csds extract-vsrx-keys, request csds jdm, and request csds sync-controller.]

- **Junos Node Unifier support in CSDS for unified CLI management (MX240, MX304, MX480, MX960, MX10004, MX10008, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—We support centralized management of devices in the Connected Security Distributed Services (CSDS) Architecture with the Junos Node Unifier (JNU) single-touchpoint solution. The JNU topology uses MX Series routers as JNU controllers, and SRX Series Firewalls and Junos Device Manager (JDM) as JNU satellites. From the controller, you can perform the following operations on the satellites:

  - Configure and manage the nodes using Junos OS configuration commands.
  - Run Junos OS operational mode commands.

  [See Junos Node Unifier for CSDS, request jnu satellite sync, show chassis jnu satellite, and jnu-management.]

## Content Security

- **Web proxy support for Content Security Sophos 2.0 antivirus and reputation-based file blocking (cSRX, SRX Series Firewall, and vSRX)**—Content Security Sophos 2.0 antivirus now supports web proxy. In addition, we introduce the following file reputation groups to control traffic and provide more control over security:

  - Malware
  - Potentially unwanted applications
  - Unknown
  - Known good or clean

  The Sophos antivirus blocks the traffic if the file reputation belongs to the malware group and permits the known good or clean group traffic. You can define the action for the potentially unwanted applications and unknown group traffic based on your requirements.

[See Sophos Antivirus Protection Overview, server (Security Sophos Engine Antivirus), sophos-engine, notification-options (Security Antivirus), show security utm anti-virus status, and show security utm anti-virus statistics.]

## Device Security

- **Enhanced policy configuration synchronization (SRX Series Firewalls and vSRX Virtual Firewall)**—Use file serialization to propagate policy configuration changes to the data plane. This method serializes policy configurations into files, ensuring that the Packet Forwarding Engine applies them reliably.

  Enabled by default, file serialization minimizes security policy mismatches and boosts system reliability.

  [See Configuring Security Policies and file-serialization.]

## High Availability

- **Multinode High Availability features in private clouds (vSRX Virtual Firewall)**—vSRX Virtual Firewalls deployed in private clouds (KVM and VMware ESXi) support following features:

  - ICL encryption—Uses IPsec protocols to secure synchronization messages between high-availability nodes, ensuring data privacy.
  - Flexible datapath failure detection—Offers path monitoring with granular control through weighted features, supporting IP, BFD, and interface monitoring.

  You can configure these features on vSRX instances using the same method as for physical SRX Series firewalls.

  See [Multinode High Availability Support for vSRX Virtual Firewall Instances.]

- **MNHA support for Google Cloud Platform (vSRX Virtual Firewalls)**—You can configure a pair of vSRX instances on the Google Cloud Platform (GCP) Marketplace for an active/backup Multinode High Availability setup. This configuration enhances reliability and efficiency of high availability operations on GCP, ensuring uninterrupted services for users.
  [See Multinode High Availability in Google Cloud Platform.]

- **IPsec VPN tunnels support for Multinode High Availability on AWS and Azure Cloud (vSRX3.0)**—IPsec VPN support is available for active/backup Multinode High Availability in AWS and Azure Cloud deployments.

  IPsec VPN tunnels are secure, encrypted connection between different networks or endpoints. In the Multinode High Availability setup, the system establishes secure tunnels between the nodes in high availability setup and VPN peer devices.

  [See IPsec VPN Support in Multinode High Availability.]

## Intrusion Detection and Prevention

- **Support logging for exempt rule matching (cSRX, SRX Series Firewalls, and vSRX 3.0)**—Use exempt rule logging in the IDP system to monitor and analyze traffic patterns, detect potential security threats, and troubleshoot network issues. Administrators can examine logs to gain insights into traffic exempt from IDP rules and make informed network policy decisions. Enable logging functionality for exempt rules at the rule level for fine-grained monitoring and analysis of security events, enhancing system visibility.

  [See Support logging for exempt rule matching.]

- **IDP signature package server-side improvements (cSRX, SRX Series Firewalls, and vSRX3.0)**—The IDP system now reports installation status to the signature server. The signature server uses information from multiple devices to decide if a signature package fails the integrity check globally. If a signature package does not pass integrity checks globally, it becomes unavailable for future downloads.

  [See IDP signature package server-side improvements.]

- **IDP intelligent offload per protocol (cSRX, SRX Series Firewalls, and vSRX 3.0)**—The protocol-specific Intelligent-Offload Configuration feature in IDP enables administrators to set inspection depth limits for different protocols. Administrators can use this capability to enable or disable offloading on a per-protocol basis and to configure specific offload limits for protocols such as SSH and FTP. This flexibility optimizes resource usage and ensures efficient session inspections.

  Use the options in the `set security idp sensor-configuration global intelligent-offload-tunable` CLI command to modify the offload settings, specify the protocol, and adjust the offload limit.

  [See Intrusion Detection and Prevention Overview.]

## Network Address Translation (NAT)

- **Monitor subscriber port utilization (cSRX, MX240, MX480, MX960, SRX1500, SRX1600, SRX2300, SRX4200, SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX3.0)**–You can monitor and manage port utilization when deploying Carrier Grade Network Address Translation (CGNAT).

  Configure threshold limits to receive notifications when port or port block usage exceeds the configured thresholds.

  - If a pool is configured as Port Block Allocation (PBA) and a subscriber uses more port blocks than the threshold, a notification is generated.
  - For Deterministic NAT (DETNAT) pools, if a subscriber uses more ports than the threshold in the allocated block, a notification is generated.

  The system log messages are:

- RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_RAISE: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 90%, current: 100%`

- RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_CLEAR: Subscriber ip: 10.0.0.1, Source NAT pool: pool-name, Pool type: PBA, threshold: 50%, current: 25%`

- RT_SRC_NAT_SUBS_POOL_ALARM_RAISE

  `RT_NAT: RT_SRC_NAT_SUBS_POOL_ALARM_DAMPENING: Subscriber IP: 10.1.1.2, NAT pool: pool-name, threshold alarm [raise, clear] suppressed for 2 times in last 10 seconds`

[See jnxJsSrcNatSubThresholdStatus, jnxJsNAT, Monitor Subscriber Port Utilization Using Carrier Grade NAT, subscriber-pool-utilization-alarm, and pool-utilization-alarm (Security Source NAT Pool).]

- **Support for DS-Lite fragmentation (SRX Series Firewall)**—Configure the pre-fragmentation and post-fragmentation MTU options on Dual-Stack Lite (DS-Lite) tunnels.

  - Pre-fragmentation–Enable or disable pre-fragmentation or clear the df bit in the IP packet.
  - Post-fragmentation–Enable or disable post-fragmentation to fragment the IPv6 packet. By default, post-fragmentation is off. When enabled, the IPv6 packet fragments; otherwise, if the MTU exceeds, an ICMP error message is sent to the originator.

  [See softwire-name.]

## Platform and Infrastructure

- **Distributed mode for fast BFD and Dedicated Offload CPU (vSRX 3.0)**—Distributed mode for fast Bidirectional Forwarding Detection (BFD) offers a quicker failure detection time of 900 milliseconds. You can use this feature in both stand-alone and L3-HA mode. To activate distributed mode, set the BFD failure detection time to 500 milliseconds. Additionally, vSRX 3.0 includes a dedicated offload CPU feature. This feature reallocates a flow thread and employs the Data Plane Development Kit (DPDK) flow filters on the network interface card (NIC) to shift high-priority packets onto the dedicated flow thread.

  To enable the dedicated offload CPU on vSRX 3.0, run the `set security forwarding-options dedicated-offload-cpu` command.

  To view the current dedicated offload CPU status use the `show security forward-options dedicated-offload-cpu` command.

  [See Understanding How BFD Detects Network Failures, Configuring BFD, and detection-time (BFD Liveness Detection).]

## VPNs

- **Enhanced QoS using DSCP per SA in IPsec VPN with iked process (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—We provide traffic classification support with Differentiated Services Code Point (DSCP) per security association (SA) in IPsec VPNs using the iked process. This feature is available when you run the IPsec VPN service without the PowerMode IPsec (PMI) mode configuration. It allows your VPN gateways to negotiate separate child SA for each CoS type.

  [See CoS-Based IPsec VPNs, show security ipsec security-associations, and show security ipsec statistics.]

- **Juniper® Secure Connect integration with JIMS (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—The SRX Series Firewalls can send Juniper Secure Connect's remote access VPN connection state events to Juniper® Identity Management Service (JIMS) using the push to identity management (PTIM) solution. By default, Junos OS enables this feature when you use `identity-management` at the `[edit services user-identification]` hierarchy level.

  You can use the following options to configure this feature:

  - `no-push-to-identity-management` at the `[edit security ike gateway` *`gateway-name`* `aaa]` hierarchy level to disable the iked process communication with JIMS.

  - `user-domain` at the `[edit security remote-access profile` *`realm-name`* `options]` hierarchy level to optionally configure the domain alias name.

  See [Juniper Secure Connect Integration with JIMS, identity-management, and profile (Juniper Secure Connect).]

- **Migration of policy-based VPNs to route-based VPNs (cSRX, SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Migrate policy-based VPNs to route-based VPNs when you run the IPsec VPN service with the iked process. You must configure multiple VPN objects on a shared point-to-point `st0` logical interface to perform the migration.

  [See Shared Point to Point st0 Interface and Migrate Policy-Based VPNs to Route-Based VPNs.]

- **SAML-based user authentication in Juniper® Secure Connect (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Juniper Secure Connect remote access VPN supports user authentication using Security Assertion Markup Language (SAML) version 2. To perform the remote user authentication using SAML, run the VPN service using the iked process on your firewall and ensure you have the SAML-supported Juniper Secure Connect application.

Configure SAML service provider and identity provider settings at the `[edit access saml]` hierarchy level. Enable SAML settings in the access profile configuration using the `set access profile` *`profile-name`* `authentication-order saml` command.

See [SAML Authentication in Juniper Secure Connect, saml, authentication-order (access-profile), saml (Access Profile), saml-options, show network-access aaa saml assertion-cache, show network-access aaa statistics, request network-access aaa saml load-idp-metadata, request network-access aaa saml export-sp-metadata, clear network-access aaa saml assertion-cache, clear network-access aaa saml idp-metadata, and clear network-access aaa statistics.]

- **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).]

## What's Changed

**IN THIS SECTION**



Learn about what changed in this release for vSRX.

## Content Security

- **Juniper NextGen Web filtering license warning enhancement (SRX Series and vSRX)**—Starting in Junos OS Release 24.4R1, if you configure the Web Filtering type as `juniper-enhanced` or `ng-juniper` without a corresponding valid license, the system does not generate a warning message. You can confirm whether the Web Filtering is down due to a missing license using the `show security utm web-filtering status` comamnd.

  Earlier to this release, if you configure Web Filtering type as `juniper-enhanced` or `ng-juniper` without a valid license, the system generated a warning message.

  [See show security utm web-filtering status and Juniper NextGen Web Filtering Overview.]

## Junos XML API and Scripting

- **Commit script input to identify software upgrades during boot time (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `junos-context` node-set includes the `sw-upgrade-in-progress` tag. Commit scripts can test the `sw-upgrade-in-progress` tag value to determine if the commit is taking place during boot time and a software upgrade is in progress. The tag value is `yes` if the commit takes place during the first reboot after a software upgrade, software downgrade, or rollback. The tag value is `no` if the device is booting normally.

  [See Global Parameters and Variables in Junos OS Automation Scripts.]

## User Interface and Configuration

- **Compact format deprecated for JSON-formatted state data (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've removed the `compact` option at the `[edit system export-format state-data json]` hierarchy level because Junos devices no longer support emitting JSON-formatted state data in compact format.

- **Access privileges for request support information command (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series Firewalls, and vSRX Virtual Firewall)**—The `request support information` command is designed to generate system information for troubleshooting and debugging purposes. Users with the specific access privileges `maintenance`, `view`, and `view-configuration` can execute request support information command.

- **Changes to the `show system information` and `show version` command output (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The `show system information` command output lists the

Hostname field first instead of last. The show version command output includes the Family field. The Family field identifies the device family under which the device is categorized, for example, junos, junos-es, junos-ex, or junos-qfx.

[See show system information and show version.]

## VPN

- **Compliance check is added for Juniper Secure Connect (SRX Series, and vSRX 3.0)**—In Junos OS, we have added a compliance check to enforce that only Juniper Secure Connect clients can establish remote access VPN connections, and to reject connection requests from non-compliant remote access clients. You'll notice this behavior for the VPN connection using the remote access profile attached to the IPsec VPN object.

- **Changes to syslog messages for IPsec VPN service (SRX Series, and vSRX 3.0)**—We've made changes to the syslog messages for the IPsec VPN service. You'll notice that: Tunnel-id field is added to the KMD_PM_SA_ESTABLISHED syslog messages when running IPsec VPN service using the kmd process. - New syslog message IKE_VPN_SA_ESTABLISHED is added for an IPsec rekey event when running IPsec VPN service using the iked process.

- **Changes to the lifetime-kilobytes option in IPsec VPN Security Association (SRX Series Firewalls, and vSRX 3.0)**—The minimum allowed IPsec proposal lifetime-kilobytes value is changed from 64KB to 64000KB for IPsec VPN Security Association.

  [See proposal (Security IPsec).]

- **Changes to syslog messages for IPsec VPN service (SRX Series, and vSRX 3.0)**—We've made changes to the syslog messages for the IPsec VPN service. You'll notice that: - Tunnel-id field is added to the KMD_PM_SA_ESTABLISHED syslog messages when running IPsec VPN service using the kmd process. New syslog message IKE_VPN_SA_ESTABLISHED is added for an IPsec rekey event when running IPsec VPN service using the iked process.

- **Support for iPadOS for prelogon compliance checks in Juniper Secure Connect (SRX Series, and vSRX3.0)**—You can configure prelogon compliance checks on your firewall to allow or reject endpoints running iPadOS. Use the ipados option at the [edit security remote-access compliance pre-logon *name* term *name* match platform] hierarchy level to enforce these checks. This ensures that only compliant iPadOS devices are permitted access, enhancing the security of your network.

  [See compliance (Juniper Secure Connect).]

## 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.

### Platform and Infrastructure

- 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. PR1827152

### 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.

### Infrastructure

- mlx5 VFs stop forwarding traffic after a little while on vSRX 3.0 with Junos OS version 24.2R1 PR1819356

### Intrusion Detection and Prevention (IDP)

- Not able to update IDP signature DB when using Proxy server PR1822319
- Memory leak will be observed on all SRX platforms when IDP is configured PR1826377

### J-Web

- [JWeb] application cannot be removed from application-set PR1834748

### Platform and Infrastructure

- 24.2DCB:vSRX3.0:USERFW:ca-certificate config shouldn't be there form 24.3 release PR1787581
- The srpfe crash during SAV longevity testing PR1814271
- Intermittent jsqlsyncd crash on all SRX platforms PR1815820
- License-service subsystem crash is observed when license keys are modified PR1820329
- Junos SRX Series device might boot in amnesiac mode and configuration commit might fail with 'error: Check-out failed for CASB process' PR1823224

- Juniper Secure Connect will not get connected if loopback is configured as external interface PR1825573
- Traffic outages due to memory shortage and core dumps PR1826129
- The offline download of the SRX IDP signature fails PR1838853

### Routing Policy and Firewall Filters

- On Junos SRX Series platforms traffic will be dropped when AppID DB is not installed PR1821890

### Unified Threat Management (UTM)

- On devices with no EWF filtering license installed on configuring Web Filtering type as juniper-enhanced or ng-juniper syslog will be generated PR1805875
- Memory corruption resulting in srxpfe crash on SRX platforms PR1816280

## 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 example, you can upgrade from 21.2 to the next three releases – 21.3, 21.4 and 22.1 or downgrade to the previous three releases – 21.1, 20.4 and 20.3.

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. For example, 21.2 is an EEOL release. Hence, you can upgrade from 21.2 to the next two EEOL releases – 21.4 and 22.2 or downgrade to the previous two EEOL releases – 20.4 and 20.2.

**Table 12: 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

> **NOTE**: To obtain information about the components that are supported on the devices and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **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

10 July 2025—Revision 18, Junos OS Release 24.4R1.

25 June 2025—Revision 17, Junos OS Release 24.4R1.

23 June 2025—Revision 16, Junos OS Release 24.4R1.

29 May 2025—Revision 15, Junos OS Release 24.4R1.

22 May 2025—Revision 14, Junos OS Release 24.4R1.

2 May 2025—Revision 13, Junos OS Release 24.4R1.

28 April 2025—Revision 12, Junos OS Release 24.4R1.

22 April 2025—Revision 11, Junos OS Release 24.4R1.

18 April 2025—Revision 10, Junos OS Release 24.4R1.

1 April 2025—Revision 9, Junos OS Release 24.4R1.

27 March 2025—Revision 8, Junos OS Release 24.4R1.

7 March 2025—Revision 7, Junos OS Release 24.4R1.

20 February 2025—Revision 6, Junos OS Release 24.4R1.

18 February 2025—Revision 5, Junos OS Release 24.4R1.

06 February 2025—Revision 4, Junos OS Release 24.4R1.

31 January 2025—Revision 3, Junos OS Release 24.4R1.

10 January 2025—Revision 2, Junos OS Release 24.4R1.

27 December 2024—Revision 1, Junos OS Release 24.4R1.