# Release Notes

Published
2023-06-12

## Junos OS Release 22.4R2®

## Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 22.4R2. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

# Table of Contents

# Junos OS Release Notes for ACX Series

IN THIS SECTION



## What's New

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

## What's Changed

IN THIS SECTION



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

## EVPN

- **Specify the UDP source port in a ping overlay or traceroute overlay operation** — In Junos OS releases prior to 22.4R1, you could not configure the udp source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other hash-* options that may be used to determine the source port value.

## General Routing

- **Label-switched interface (LSI) delay during reboot (ACX Series)** —Rebooting ACX Series routers running Junos OS Evolved with a class-of-service routing-instance configuration might encounter errors due to a delay with the label-switched interface (LSI). LSI state information has been added to the output of the `show route instance` command to assist in the analysis of such errors.

  [See show route instance.]

## Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## Platform and Infrastructure

- **The `ping host | display xml` command produces CLI output without errors (ACX Series, PTX Series, and QFX Series)** — In Junos OS release 22.4R2, the `ping host | display xml` command now produces CLI output formatted in XML.

  [See ping.]

## Known Limitations

There are no known limitations in hardware or software 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.

## 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 WRL8 based VMHost platform (ACX6360), there is no log rotation for resild log and temperature sensor information is incorrectly written into resild log, which could result in continuous logs in resild log file. The disk usage might keep increasing due to this issue. The disk usage could be eventually full which could cause system to hang and reboot. PR1480217
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. Due to high risk KBP SDK upgrade planned for 21.1. PR1533513
- Service MIC does not work on ACX500 running Junos 20.4 or higher. PR1569103
- On all ACX platforms, the hosts will not receive multicast traffic when snooping is configured in a EVPN-MPLS (Ethernet Virtual Private Network - Multiprotocol Label Switching) enabled broadcast domain.PR1613462

- Vulnerability in class-of-service (CoS) queue management. The Junos OS on the ACX2000 Series devices allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). PR1637615
- When TCP Main and TCP remaining attached together on IFD its observed that Improper Scheduler MAP is getting configured on HQoS IFD while scheduled params modification and bind performed on same commit. This is a sequence issue from CoSD(RE) which not guaranteed at Packet Forwarding Engine side. And this is applicable for all platforms. PR1664785
- In VPLS MH cases, the standby UNI ifl in backup router will be programmed in disable state, by adding the UNI interface to invalid VPN ID in HW. During switch over the UNI ifl will be deleted and will be added under the VPLS instance VPN ID. In issue case, UNI interface added under invalid VPN ID in backup router tried to delete by passing the VPLS instance VPN ID, causing the issue. This issue is applicable only for ACX5000 Series.PR1665178
- Reserved buffers might be shown as 0, but internally reserved buffers do get used to queue and transmit traffic on the queue. This seems to be a day one issue and will be fixed in future releases. PR1689183
- The aggregate Ethernet statistics might show 0 bps for output traffic. It is a CLI output display issue. It will be fixed in the future releases. It does not impact the traffic output.PR1689185
- dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. PR1692400
- After restart chassis-control or restart routing, sometimes the error message mentioned in the PR description are seen. PR1694997
- Convergance time can be more than 60ms for OSPF TILFA Node protection testing.PR1695292

## Interfaces and Chassis

- In case of EVPN routing-instance, there will be an implicit bridge-domain created for VPLS route table. This BD index will be used by daemon DCD in successive commits. When igmp-snooping is enabled, mcsnoopd daemon publishes update on INET route table with BD index value 0, which is mismatching with the DCD. As a result, this might cause to flap IFLS which are part of this routing-instance on successive commits.PR1712800

# 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

- Delegated BFD sessions configured on routing-instance might fail to come up. PR1633395
- SSH non-default port configuration causes FPC offline after an upgrade to 21.4. PR1660446
- Na-grpcd process core observed in telemetry services. PR1665516
- New BFD sessions will not come up on ACX5448 or ACX710 due to continuous flaps. PR1670684
- ACX-5448: pps values seen on interface even when it is in disabled state. PR1685344
- Traffic is silently dropped during l2circuit pseudowire redundancy neighbor switchover. PR1686260
- The subscriber-management-helper is thrashing, not restarted, messages seen on ACX5448. PR1688107
- The jdchpd core seen with dhcp-snooping persistent configuration. PR1688644
- The LACP would get stuck in a continuous update loop in the MC-LAG scenario. PR1688958
- Integration of RCP binary into the LTS19 code for Vmhost Platforms. PR1689100
- EVPN packets might go to incorrect queues due to the wrong classification and might lead to packet drop during congestion. PR1689604
- PCS errors and framing errors on 100GE interfaces on certain Junos platforms. PR1692063

- [interface] [acx_ifd] ACX7100-48L :: 400g-ZR-M link is not up between storm-01 and wolverine-01 due to **Optics Over Temperature Shutdown**. PR1698342
- On ACX5448 devices, an interface with SFP-T optic set to 100m and auto-negotiation disabled will remain down after reboot or on chassis-control restart. PR1702239
- ACX5448 ingress PE is pushing Label 0 instead of Leaf label. PR1702615
- CoS rewrite rules will not work in L3VPN scenario. PR1703840
- [dhcp] [DHCP_RELAY] ACX7100-48L :: Getting commit error for the dhcp configuraiton commit and then it is coring with the bt jtimer_start_oneshot. PR1707690
- Transit traffic drop is observed for the BGP-LU route prefixes with ECMP forwarding path on Junos ACX5448 and ACX710 platforms. PR1712564
- The member interface will not be added to the aggregate Ethernet bundle if the link-speed of the aggregate Ethernet interface does not match that of the member. PR1713699
- The traffic through the aggregate Ethernet member link will be dropped. PR1714111
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- The multicast packets could hit the CPU/RE on ACX5448 and ACX710 platforms. PR1722277

## Interfaces and Chassis

- Incompatible and unsupported configuration is not getting validated correctly during ISSU and normal upgrade causing the traffic loss. PR1692404

## Routing Protocols

- Wrong SRTE secondary path weight makes the secondary path active in forwarding table. PR1696598

# 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, 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**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 |
|---|---|---|---|---|
| Standard 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 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 cSRX

IN THIS SECTION



## What's New

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

## What's Changed

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

## Known Limitations

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

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

## Open Issues

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

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

## Resolved Issues

There are no resolved issues in this release for cSRX.

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

# Junos OS Release Notes for EX Series

IN THIS SECTION

## What's New

There are no new features or enhancements to existing features in this release for EX Series switches.

## What's Changed

**IN THIS SECTION**



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

## EVPN

- **Specify the UDP source port in a ping overlay or traceroute overlay operation**—In Junos OS releases prior to 22.4R1, you could not configure the `udp source port` in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other hash options that may be used to determine the source port value.

## Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## Platform and Infrastructure

- **The `ping host | display xml validate` command validates XML without error (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, and vMX)**—In the earlier releases of Junos OS and Junos OS Evolved release 22.4R2, the `ping host | display xml validate` command results in CRITICAL ERROR: Root tag name mismatch. Expected 'ping-results', got 'run-command'. The command now validates the XML successfully without error.

  [See ping.]

## 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

- EVPN-VXLAN: After Routing Engine switchover, you will see a momentary traffic loss with EVPN VXLAN on the EX4400 switches. PR1659315

## General Routing

- On all Junos trinity-based platforms such as EX Series and MX Series, global port mirroring will not work for RSPAN scenario (port-mirror output as VLAN or bridge-domain). Port-mirror instance configuration `set forwarding-options port-mirroring instance` will work for RSPAN scenario. PR1668900
- MVRP on P-VLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

## Virtual Chassis

- EX4400 supports multiple uplink modules. Some supports Virtual Chassis port (VCP) conversion and some doesn't. Therefore, the recommended procedure is to convert VCP to NW port first and then make sure uplink module is made offline using `request chassis pic fpc` command before removal. PR1665242

## Open Issues

**IN THIS SECTION**

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

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

## EVPN

- After Routing Engine switchover, a momentary traffic loss may be observed with EVPN VxLAN on EX4400 switches. PR1659315

## General Routing

- Runt, fragment and jabber counters are not incrementing on EX4300-MPs. PR1492605
- When launching a guest virtual machine to run a third party application on the Junos OS 15.1R1 and above, the guest virtual machine might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596
- Pause frame counters do not increment when pause frames are sent on the EX2300, EX3400, EX4300-48MP, and EX4300 line of switches. PR1580560
- In an interoperable scenario, when using 1G SFP optic on PIC-2, you must disable auto-negotiation on the peer. PR1657766
- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle or software reboot, all ports are initialized and links are up when you enable auto-negotiation. Few ports are up and traffic flows whereas few ports are up but no traffic flow through them.PR1672583
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch. If there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)======(et-0/0/1 and et-0/0/2)R2. And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs (MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200 (correspnding to MSTI-2). This potentially can cause a problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2, genuine member of vlan-200 goes into BLK state for MSTI-2. When traffic is received in vlan-200 it will be sent out of et-0/0/1, an it will be dropped.PR1686596

- On Junos OS QFX5000 Series line of switches, configuration-change/protocol flapping/port flapping in EVPN Virtual Extensible LAN (VXLAN) can cause traffic loss (changes related to the underlay network). PR1688323
- When you enable port beacon LED for the port, `show chassis led` statement output shows incorrect port LED status for the interfaces as lit up instead of off. PR1697678
- On changing the speed from or to 10m, some of the port might not ping. PR1712495
- Booting the device having LLDP PDs connected with perpetual PoE configuration enabled will take time to update the negotiated value in the configuration statement (show poe interface).PR1713545
- EX4100MP might allocate the power 0.1w less than the one PD requested. For example, when PD requests the power 19.4W in LLDP, EX4100 will allocate 19.3W to PD.PR1716261
- PoE firmware upgrade might fail or might get stuck if the PoE firmware download procedure got interrupted. PR1717869

## Layer 2 Features

- The memory might leak because of the eswd daemon on the EX Series platforms. A message like the following is displayed in the system log: eswd[1330]: JTASK_OS_MEMHIGH: Using 212353 KB of memory, 158 percent of available /kernel: KERNEL_MEMORY_CRITICAL: System low on free memory, notifying init (#2). /kernel: Process (1254,eswd) has exceeded 85% of RLIMIT_DATA: used 114700 KB Max 131072 KB. PR1262563

## Layer 2 Ethernet Services

- When an EX3400 Virtual Chassis members are zeroized or if it powered on for the first time after halt, `set chassis auto-image-upgrade` configuration is removed during the process of VC formation. Absence of this configuration will not allow user to download configuration and images via ZTP. PR1694952

## Platform and Infrastructure

- On EX4300 platform, if you configure `encapsulation ethernet-bridge` statement, the interface is getting programmed as trunk instead of access in VLAN membership. This leads to untagged traffic drop. PR1665785

- On EX4300-24T, EX4300-48P, EX4300-VC, EX430024P, EX430032F and EX430048T platforms, when a VSTP (VLAN Spanning Tree Protocol) BPDU (Bridge Protocol Data Unit) arrives with a VLAN ID that is not configured in the switch, but that matches with an HW Token of any other configured VLAN, the VLAN ID of the BPDU will be changed to the VLAN ID corresponding to the matched HW Token and flooded. This disrupts STP convergence on the configured VLAN because some ports can incorrectly go into blocking state. PR1673000

## Virtual Chassis

- On Junos EX4600 Virtual Chassis (VC), the primary Routing Engine reboot and all-members reboot lead to the Packet Forwarding Engine manager hogging logs when SFP-T pluggable is installed in. The Packet Forwarding Engine manager hogging logs has no functionality impact. PR1685067
- On EX4600-VC, when you execute the `request system reboot all members` statement, post-reboot one of the Virtual Chassis member or Flexible PIC Concentrator (FPC) might disconnect and join the Virtual Chassis back due to Packet Forwarding Engine restart. Traffic loss is seen when FPC disconnects. PR1700133

## 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.

## Forwarding and Sampling

- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073

## General Routing

- DHCP packets get looped in EVPN-VXLAN setup. PR1657597
- EX4100 MACsec interface statistics of encrypted/decrypted bytes do not increment further after reaching a 40-bit limit (1099511627775). PR1658584
- EX4100 and EX4100-F series: On-device reboot in scaled PoE scenario with perpetual PoE configured, the correct status for LLDP enabled ports reflects after sometime. PR1671311
- On EX2300 and EX3400 devices, `set system ports console log-out-on-disconnect` does not allow the user to log-in via console. PR1680408
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- EX4300-48MP factory reset or mode button cannot toggle status mode LED (SPD, DX, EN, and PoE). PR1687407
- CPU will not reset automatically and will have abnormal behaviour when CAT error is observed. PR1687790
- EX4400 SNMP : FRU removal or insertion trap might not be generated when Fan try or PIC is removed and inserted. PR1687848
- The FPC crashes when you apply the same CoS configuration with wildcard for all the physical interfaces and aggregated Ethernet. PR1688455
- jdchpd core seen with `dhcp-snooping persistent` configuration. PR1688644
- A self-ping silently drops along with fmpc process crash in a rare scenario causing traffic loss. PR1692365
- Few uplink ports of EX2300-48MP are not coming up. PR1692579
- The dot1x reauthentication will not work for a port with VoIP VLAN. PR1693640
- DHCP binding fails after dot1x authentication in EVPN-VXLAN network. PR1693967

- Packet Forwarding Engine crashes on all Junos OS QFX5000 and EX4600 platforms with L2PT configuration. PR1694076
- On P-VLAN with DAI ARP packets will be forwarded between isolated ports. PR1694800
- The l2cpd telemetry might crash when the LLDP NETCONF notification from external controllers along with NETCONF services configuration is present on the device. PR1695057
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- Traffic forwarding fails when deleting all L2 related configurations. PR1695847
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- Transceiver not detected after it's unplugged and plugged in again. PR1696444
- The dot1x authentication will not be enabled on interfaces with specific configuration combination. PR1696906
- Network port status LED will go off in duplex mode. PR1696940
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- TCAM space might exhaust when learning DHCP snooping entries on a trusted port. PR1699777
- The BFD session will remain in init or down state in the Virtual Chassis scenario. PR1701546
- The PXE BIOS recovery fails on EX9204, EX9208, and EX9214 Virtual Chassis setup. PR1704457
- Traffic drops with hierarchal overlay ECMP configuration. PR1704470
- Traffic silently drops and discarded in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- Alarms do not generate as expected when the management interface link is down. PR1706116
- Layer 3 forwarding issues for IRB. PR1706845
- The PoE firmware upgrade fails on EX4400 platforms. PR1706952
- In a VC scenario, sometimes the alarms raised on the line-card or secndary Routing Engine may not show on the primary Routing Engine. PR1707798

- QSFPs displays as UKNOWN after the upgrade. PR1708123
- When 100G transceiver is used on VCP port, the VCP port will either not come up or come up as 40G. PR1711407
- The dot1xd crashes on the Junos OS EX2300 platforms. PR1711422
- The multiple supplicant scenario for dot1x does not work with MAC based tagging in case of group based policies. PR1713982
- On EX4650, jnxOperatingDescr.1.1.0.0 is populated with blank. PR1714056
- EX4400 link or activity LED is not lit when it transits to the factory default configuration by pressing the Factory Reset/Mode button. PR1714116
- BIOS upgrade is not getting successful via CLI when the system is booted with secondary partition [HDD00.6]. PR1715258
- The interface phy of PIC 0 comes up causing traffic loss while the device reboots. PR1715680
- The link remains down on connecting the transceiver 10GBASE-T with the serial number starting with "2P1". PR1716703
- `set forwarding-options evpn-vxlan shared-tunnels` command will not be available for EX9200 and MX Series platforms. PR1716881
- DHCP Security ARP statistics are not as expected after DHCP binding. PR1718286

## Interfaces and Chassis

- The unicast traffic is dropped on QFX5100/EX4600-VC platforms. PR1695663

## Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when you reconfigure `forward-only` under the routing instance. PR1689005

## Platform and Infrastructure

- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- dhcp offer packet fails to send back to the client leaf from server leaf in ERB int-vrf model. PR1698833

## Routing Protocols

- The mcsnoopd process might crash when the VLAN name for `igmp-snooping` statement has certain characters. PR1711153

## Virtual Chassis

- Instability after mastership switchover on members with SFP-T pluggable installed on the EX4600-VC device. PR1689946

## 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**Table 2: EOL and EEOL Releases**

| Release Type | End of Engineering (EOE) | End of Support (EOS) | Upgrade/ Downgrade to subsequent 3 releases | Upgrade/ Downgrade to subsequent 2 EEOL releases |
|---|---|---|---|---|
| Standard End of Life (EOL) | 24 months | End of Engineering + 6 months | Yes | No |
| Extended End of Life (EEOL) | 36 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**Table 3: EOL and EEOL Releases**

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

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

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

# Junos OS Release Notes for Juniper Secure Connect

**IN THIS SECTION**

## What's New

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

## What's Changed

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

## Known Limitations

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

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

## Open Issues

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

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

## Resolved Issues

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

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

# Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION



## What's New

There are no new features or enhancements to existing features in this release for Junos fusion for enterprise.

## What's Changed

There are no changes in behavior and syntax in this release for Junos Fusion for enterprise.

## Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for enterprise.

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 Junos Fusion for enterprise.

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

## Resolved Issues

**IN THIS SECTION**



Learn about the issues fixed in this release for Junos Fusion for enterprise.

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

## Junos Fusion Satellite Software

- The Junos Fusion Satellite device will be stuck in the SyncWait state. PR1682680

# Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION



This section contains the procedure to upgrade or downgrade Junos OS and satellite software for a Junos fusion for enterprise. Upgrading or downgrading Junos OS and satellite software might take several hours, depending on the size and configuration of the Junos fusion for enterprise topology.

## Basic Procedure for Upgrading Junos OS on an Aggregation Device

When upgrading or downgrading Junos OS for an aggregation device, always use the `junos-install` 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 `junos-install` package and details of the installation process, see the Installation and Upgrade Guide.

**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. See the Junos OS Administration Library.

To download and install Junos OS:

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

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

2. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.

4. Select the release number (the number of the software version that you want to download) from the Version drop-down list on the right of the page.

5. Select the **Software** tab.

6. Select the software package for the release.

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 `junos-install` package on the aggregation 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 commands, where *n* is the spin number.

    ```
    user@host> request system software add validate reboot source/package-name.n.tgz
    ```

    All other customers, use the following commands, where *n* is the spin number.

    ```
    user@host> request system software add validate reboot source/package-name.n-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*** (available only for Canada and U.S. version)

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.

Adding the `reboot` command reboots 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.

## Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to minimize disrupting network operations as follows:

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*.

## Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion for enterprise. See Configuring or Expanding a Junos fusion for enterprise.

For satellite device hardware and software requirements, see Understanding Junos fusion for enterprise Software and Hardware Requirements.

Use the following command to install Junos OS on a switch before converting it into a satellite device:

```
user@host> request system software add validate reboot source/package-name
```

**NOTE**: The following conditions must be met before a Junos switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch running Junos OS can be converted only to SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

When the interim installation has completed and the switch is running a version of Junos OS that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device using the console port.
2. Clear the device:

```
[edit]
user@satellite-device# request system zeroize
```

**NOTE**: The device reboots to complete the procedure for resetting the device.

If you are not logged in to the device using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

If you lose connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
```

For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, or preconfiguration. See Configuring or Expanding a Junos fusion for enterprise for detailed configuration steps for each method.

## Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos fusion topology. For more information, see Converting a Satellite Device to a Standalone Device.

## Upgrade and Downgrade Support Policy for Junos OS 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.

**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 |
|---|---|---|---|---|
| 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.

## Downgrading Junos OS

Junos fusion for enterprise is first supported in Junos OS Release 16.1, although you can downgrade a standalone EX9200 switch to earlier Junos OS releases.

> **NOTE**: You cannot downgrade more than three releases.
> For more information, see the Installation and Upgrade Guide.

To downgrade a Junos fusion for enterprise, follow the procedure for upgrading, but replace the `junos-install` package with one that corresponds to the appropriate release.

# Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION



## What's New

There are no new features or enhancements to existing features in this release for Junos Fusion for Provider Edge.

## What's Changed

There are no changes in behavior and syntax in this release for Junos Fusion for provider edge.

## Known Limitations

There are no known limitations in hardware or software in this release for Junos fusion for provider edge.

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 Junos Fusion for provider edge.

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

## Junos Fusion Provider Edge

- On all Junos Fusion platforms, SDPD (Satellite Discovery and Provisioning Daemon) crash will be observed on the aggregation device (AD) while sending discovery packets for satellite device(SD) provision. Satellite provisioning will not be completed due to this issue and the SD cannot be managed from the AD. PR1624219

## Resolved Issues

There are no resolved issues in this release for Junos Fusion for provider edge.

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 procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos fusion for provider edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

## Basic Procedure for Upgrading an Aggregation Device

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.

**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. See the Installation and Upgrade Guide.

The download and installation process for Junos OS Release 22.4R2 is different from that for earlier Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:

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

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.
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 page.
5. Select the **Software** tab.
6. Select the software package for the release.
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 aggregation 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 commands.

- For 64-bit software:

> **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-22.4R2.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.4R2.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

  **NOTE**: We recommend that you use 64-bit Junos OS software when implementing Junos fusion for provider edge.

```
user@host> request system software add validate reboot source/jinstall64-22.4R2.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.4R2.SPIN-export-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*** (available only for the Canada and U.S. version)

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

Adding the `reboot` command reboots 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 22.4R2 `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.

## Upgrading an Aggregation Device with Redundant Routing Engines

If the aggregation device has two Routing Engines, perform a Junos OS installation on each Routing Engine separately as follows to minimize disrupting network operations:

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*.

## Preparing the Switch for Satellite Device Conversion

Satellite devices in a Junos fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. For satellite device hardware and software requirements, see Understanding Junos fusion Software and Hardware Requirements

**NOTE**: The following conditions must be met before a standalone switch that is running Junos OS Release 14.1X53-D43 can be converted to a satellite device when the action is initiated from the aggregation device:

- The switch can be converted to only SNOS 3.1 and later.
- Either the switch must be set to factory-default configuration by using the `request system zeroize` command, or the following command must be included in the configuration: `set chassis auto-satellite-conversion`.

Customers with EX4300 switches, use the following command:

```
user@host> request system software add validate reboot source/jinstall-ex-4300-14.1X53-D43.3-domestic-signed.tgz
```

Customers with QFX5100 switches, use the following command:

```
user@host> request system software add reboot source/jinstall-qfx-5-14.1X53-D43.3-domestic-signed.tgz
```

When the interim installation has completed and the switch is running a version of Junos and OS on one line that is compatible with satellite device conversion, perform the following steps:

1. Log in to the device by using the console port.
2. Clear the device:

   ```
   [edit]
   user@satellite-device# request system zeroize
   ```

   **NOTE**: The device reboots to complete the procedure for resetting the device.

   If you are not logged in to the device by using the console port connection, your connection to the device is lost after you enter the **request system zeroize** command.

   If you lose your connection to the device, log in using the console port.

3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

   ```
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
   ```

   For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

   ```
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 0
   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 1
   ```

```
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 2
user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port 3
```

This step is required for the 40-Gbps QSFP+ interfaces that will be used as uplink interfaces in a Junos fusion topology. Built-in 40-Gbps QSFP+ interfaces on EX4300 switches are configured into VCPs by default, and the default settings are restored after the device is reset.

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration. See Configuring Junos fusion for provider edge for detailed configuration steps for each method.

## Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos fusion topology.

**NOTE**: If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is software that includes *pxe* in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D43 is named install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz . If the satellite device is an EX4300 switch, you install a standard jinstall-ex-4300 version of Junos OS.

The following steps explain how to download software, remove the satellite device from Junos fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

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

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

2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.

3. Select **By Technology > Junos Platform > Junos fusion** from the drop-down list and select the switch platform series and model for your satellite device.

4. Select the Junos OS Release 14.1X53-D30 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

7. Copy the software to the routing platform or to your internal software distribution site.

8. Remove the satellite device from the automatic satellite conversion configuration.

   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite member-number
   ```

   For example, to remove member number 101 from Junos fusion:

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite 101
   ```

   You can check the automatic satellite conversion configuration by entering the `show` command at the `[edit chassis satellite-management auto-satellite-conversion]` hierarchy level.

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

   Otherwise, commit the configuration to a single Routing Engine:

   ```
   [edit]
   user@aggregation-device# commit
   ```

10. Install the Junos OS software on the satellite device to convert the device to a standalone device.

    ```
    [edit]
    user@aggregation-device> request chassis satellite install URL-to-software-package fpc-slot
    member-number
    ```

For example, to install a PXE software package stored in the **/var/tmp** directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/install-media-pxe-qfx-5-14.1X53-D43.3-signed.tgz fpc-slot 101
```

For example, to install a software package stored in the **var/tmp** directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz fpc-slot 101
```

The satellite device stops participating in the Junos fusion topology after the software installation starts. The software upgrade starts after this command is entered.

11. Wait for the reboot that accompanies the software installation to complete.
12. When you are prompted to log back into your device, uncable the device from the Junos fusion topology. See Removing a Transceiver from a QFX Series Device or Remove a Transceiver, as needed. Your device has been removed from Junos fusion.

> **NOTE**: The device uses a factory-default configuration after the Junos OS installation is complete.

## Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 22.4R2, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

## Upgrade and Downgrade Support Policy for Junos OS 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.

**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 |
|---|---|---|---|---|
| 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.

## Downgrading from Junos OS Release 22.4

To downgrade from Release 22.4 to another supported release, follow the procedure for upgrading, but replace the 22.4 `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 MX Series

IN THIS SECTION



## What's New

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

## What's Changed

IN THIS SECTION

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

## Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## 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

- In a scaled setup with LDP over RSVP configuration and maximum-ecmp as 32 or 64, line card CPU usage can remain high for extended duration on link flap operation. In this duration, LACP might take 5+ minutes to converge and the AE bundle to be active. PR1624219

- On all Junos platforms, agentd process crash will be seen in telemetry streaming longevity test.PR1647568
- If proper gap is given between channelisation and dechannelisation the issue is not seen. Proper gap means allowing the system to complete the previous config before we load the new configuration. The recommendation is to if we give channelisation configuration commit wait for the links to come up or atleast the IFDs get created on both EVO and RE side and then only revert the config to dechannlisation and vice versa. PR1665625
- VM host snapshot recovery is not enabled for RE-S-X6-128G-K. PR1674091
- Even though GRES is enabled, the `show system filesystem encryption status` command display information about the specific Routing Engine only.PR1674373
- For IPv6 traffic that is ingressing into an Abstract Fabric (AF) interface via MPC11e card, and also sampled, the OutputIntf in the flow records might not be captured if nexthop-learning statement is not enabled. PR1680873
- MVRP on PVLAN promiscuous port is not supported. If MVRP is configured on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. PR1693345

## MPLS

- With local reversion ON, there is a possibility of transit router not informing headend of RSVP disabled link when link is flapped more than once. As a workaround, remove local-reversion configuration. PR1576979

## Platform and Infrastructure

- On MX and EX9200 serial platforms, under Ethernet VPN (EVPN) environment, packets routed using IRB interface could not be fragmented due to media maximum transmission unit (MTU) problem. PR1522896
- When the `deactivate services rpm` and `deactivate routing-options rpm-tracking` commands are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps. 1. deactivate routing-options rpm-tracking 2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service needs to be deactivated, 3. deactivate services rpm 4. commit. PR1597190

- On Mx platforms, VPLS flood traffic loss is observed if flood composite next-hops are out-of-sync on ingress and egress FPCs during transport path revertion.PR1656216

## Routing Protocols

- When "routing-options transport-class fallback none" is not configured, do not configure more than 10 transport-classes. Or advertise more than 10 distinct colors in SR-TE or FlexAlgo. PR1648490

## Services Applications

- In Junos OS Release 17.4 and forward, subscriber sessions on the LNS that send an ICRQ that includes RFC5515 AVPs might fail to establish a session. The client will receive a CDN error `receive-icrq-avp-missing-random-vector` in response. PR1493289

## 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.

## Class of Service (CoS)

- While Traffic control profile is having only scheduler map associated with it and if its attached to IFL , commit error to be thrown. PR1688790

## EVPN

- On all platforms, MAC-IP route deletion and addition are triggered when re-ARP (Address Resolution Protocol) on MH (Multihoming) device fails in the EVPN-MPLS multihoming scenario resulting in traffic drop. PR1691132
- On all Junos and Junos OS Evolved platforms with IGMP-snooping (Internet Group Management Protocol) enabled under instance type EVPN (Ethernet Virtual Private Network) with vlan-id=none or unspecified vlan-id there will be a spike in the mcsnoopd process CPU utilization. This will lead to the mcsnoopd process crash and there will be disruptions in the traffic. PR1713508

## General Routing

- AFEB crashing with PTP thread hog on the device. PR1068306
- When there is an input failure on one of the AC PEMs (low or high) it's incorrectly categorized as a "Mix of AC PEMs". Thus, instead of "PEM input failure" an alarm "Mix of AC PEMs" might be raised.PR1315577

- "TALUS(number) PCIe(number) DMA RX interrupt received. Queue stuck status 0xeeeeee0" are spurious messages which are triggered in system logs due to queue-back pressure or FPGA drops. PR1465888

- On WRL8 based VMHost platforms (i.e., ACX6360/PTX10001/MX150/NFX150/NFX250/NFX350), there is no log rotation for resild log and temperature sensor info is incorrectly written into resild log which could result in continuous logs in resild log file. The disk usage might keep increasing due to this issue. The disk usage could be eventually full which could cause system to hang and reboot. PR1480217

- When there are HW link errors occurred on all 32 links on an FPC 11. Because of these link errors, all FPCs reported destination errors towards FPC 11 and FPC 11 was taken offline with reason "offlined due to unreachable destinations". PR1483529

- Runt, fragment and jabber counters are not incrementing. PR1492605

- After backup Routing Engine halt, CB1 goes offline and comes back online; this leads to the backup Routing Engine booting up, and it shows the reboot reason as "0x1:power cycle/failure." This issue is only for the Routing Engine reboot reason, and there is no other functional impact of this. PR1497592

- In the platform using INH (indirect next hop, such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines (PFEs). When the version-id of session-id of INH is above 256, the PFE might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in PFE. It might lead PFE to have a different view of Unilist against load-balance selectors. Then either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- PR1463859 introduces a software defect that causes a 10GE interface to flap continuously when configuring with the WAN-PHY framing with the default "hold-down" timer (0). Once upgrading a router to an affected software release, the interface may flap continuously. This is not applicable to an interface with the default framing - LAN-PHY. PR1508794

- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS Release 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596

- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue, Due to high risk KBP SDK upgrade planned for Junos OS Release 21.1. PR1533513

- USF-SPC3 : With ipsec PMI/fat-core enabled, "show services sessions utilization" CLI not displaying right CPU utilization. PR1557751

- 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
- VE and CE mesh groups are default mesh groups created for a given Routing instance. On vlan/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. Trinity based CE boxes have unlimited capacity of tokens, so this would not be a major issue. PR1560588
- When the active slave interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in 'show ptp lock-status' output for few seconds before BMCA chooses the next best slave interface. This is the day-1 behavior and there is no functional impact. PR1585529
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version prior to 21.3R1. PR1597276
- During RE switchover, if there is a burst of ICMP/BFD/SSH/FTP/TELNET/RSVP packets (~18K pps) you might see new backup RE restarting. PR1604299
- On MX-VC (Virtual Chassis) platforms with MS-MPC or SPC3 service cards and Aggregated Multi-Service (AMS), traffic on the line card in the backup chassis might not be load-balanced properly due to timing conditions. This works well on the line card in the master chassis. There might be traffic loss when interfaces are not properly balanced. PR1605284
- The output of show network agent command should be null, which shows statistic per component after GRES. PR1610325
- When user tries to disable AMS IFD using configuration knob, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. PR1613432
- On all Junos platforms the MAC address of the 17th ae interface might be changed after the upgrade from 18.4+ to 20.4+ releases. It will lead to mac based service interruption.PR1629050
- For a topology with VSTP and VRRP configured and IPV6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams. PR1629345
- The fabric statistics counters are not displayed in the output of "show snmp mib walk ascii jnxFabricMib". PR1634372
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143

- The mspmand daemon running on MS-MPC/MS-MIC cards can occasionally crash when the service card (fpc/pic) is turned offline and then online at regular intervals when the number of service-set configured is moderately high and when extensive hardware crypto operations are being performed. Exact issue is yet to be isolated. PR1641107
- Source MAC should nt be configured on the underlying static interface on the UP for PPPoE login to work correctly. PR1641495
- vMX: "input fifo errors" drops reported under pfe shell "show ifd" but not seen in "show interface extensive" output. PR1642426
- bb device has to be manually enabled in configuration for DHCP and PPP access models for BNG CUPS. Configuration to enable bb device is as follows:: `user@router #set system subscriber-management mode force-broadband-device`. PR1645075
- On Junos platform, PTP does not lock when port speed is not configured under PIC hierarchy or port speed for some additional random ports are configured under the PIC hierarchy or perform PIC deactivate/activate. PR1645562
- Currently User can install images older that the minimum supported image on RE-S-X6-128G-K. System comes up in Linux prompt in such cases.PR1655935
- Core files reported intermittently where random grpc stack crash is observed. The license service will auto restart and recover. PR1656975
- On Junos platforms, in the VPLS environment with `routing-options resolution preserve-nexthop-hierarchy` configured results in the packet dropped at egress PE for multiple MPLS stack labels. PR1658406
- The OpenSSL project has published security advisories for multiple vulnerabilities resolved in OpenSSL. Please Refer to https://kb.juniper.net/JSA70186 for more information.PR1661450
- Not all MAC addresses are learnt for some VPLS instances after "clear vpls mac-table" command is executed. PR1664694
- With following configuration changes subscribers are coming up. Configuration changes: `set forwarding-options dhcp-relay overrides allow-snooped-clients set forwarding-options dhcp-relay group DHCP-FO overrides allow-snooped-clients set forwarding-options dhcp-relay group DHCP-FO overrides user-defined-option-82 100.112.77.66 deactivate forwarding-options dhcp-relay group DHCP-FO interface ae31.0 overrides`PR1665499
- UDP Telemetry might not work when subscribes to /junos/system/linecard/intf-exp/ sensor. PR1666714
- User should not modify the locator attributes, instead locator, SIDs should be deleted and configured back. Otherwise it will lead to generating core files.PR1667320

- On MX platforms with MIC-MACSEC-20GE, Forwarding Engine Board (FEB) might go down while activating/deactivating GRES(G?raceful Routing Engine Switchover) configuration.PR1668983
- Sometimes core files are reported on backup Routing Engine during init after a reboot etc. When the backup Routing Engine initialization is being done and system is busy, some commands executed in context of spmbpfe are taking more time to complete due to the initial heavy lifting by the kernel, In this stage, in case the commands from spmbpfe process do not complete for >2.5 seconds, then there are chances of spmbpfe core files. This is a temporary issue seen on backup Routing Engine during init time only. This might not be impacting because if in case spmbpfe process crashes due to this, it would restart by itself and continue to init and run once the initial high CPU condition has passed. It should not cause any functionality or performance impact; especially since it is reported only on backup RE.PR1675268
- On LC480 MX line-card with 1G interface 1PPS time error does not meet class B requirement (maximum absolute time error is 70 ns). PR1677471
- 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
- The issue here is that we see ?MQSS(0): DRD: Error: WAN reorder ID timeout error? once per PFE during bootup of FPC. This happens because during the FPC bootup some control packet from vmhost comes before the PFE init is fully complete. Because of this the EA Asic is not able to process the packet and throwing the error. The fix involves complex changes in the bootup sequence of ASICS and will result in other major issues. The original issue has no functionality impact. It is just one error per PFE seen during the FPC reload case only. At that time the traffic is not started yet and once the system is up no other impact is seen due to the Error. Hence the issue will not be fixed. Any "WAN reorder ID timeout error" during the bootup of FPC can be safely ignored. PR1681763
- When the hostname configuration is changed, the change is not reflected in the RIFT output. Also when changes are made to the REDIS configuration, they are not applied until rift is restarted via "restart rift-proxyd". PR1686233
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch. PR1686596
- With Sharding enabled, BGP flags like the following are not displayed on Active route in "show route extensive" output:"Accepted Multipath MultipathContrib MultiNexthop" Per shard view, using "show route extensive prefix rib-sharding shard-name" will show these flags.PR1693207
- It is recommended to use IGP shortcut with strict SPF SIDs in SR-TE path. if Strict SPF SIDs are used then this issue would not occur. This issue will occur only if regular IS-IS SIDs are used in SR-TE path and IGP shortcut is enabled. with this, if customer perform multiple times deactivate/activate for SR-TE telemetry.PR1697880
- On Junos platforms, Kernel crashes can happen in Virtual Private LAN Service (VPLS) scenario. This issue is seen when the VPLS has IRB (Integrated Routing and Bridging) interface and the next-hop of

IRB is RLT (Redundant Logical Tunnel) interface. This issue is triggered when there is an ARP request sent from the IRB interface. There can be a service impact because of this issue as the device can reboot.PR1698781

- During BGP MP route 9.0.0.2 re-resolution window, a corner case was hit, such that rpd will assert and restart. This error case is observed during Multi-Feature-Test with BGP-MP, L3VPN/L2VPN, over RSVP/LDP transport, as well as colored SRTE, and SRv6 tunnel transport along with BGP CT. This issue will get resolved in next Junos OS 22.4R1 services releases.PR1699773
- When packets of size bigger than 1518 Bytes are received/transmitted, pps counter value does not show correct value. PR1700309
- On MX platforms, traffic egressing on the IRB (Integrated Routing and Bridging) interface with the underlying L2 (layer2) access port has VLAN tags imposed incorrectly.PR1700321
- The optic configuration mismatch alarm was always enabled, but was not reported by the RE during 'show chassis alarms'. This alarm will now be correctly reported by the FPC and displayed in the RE. There is no behavior change other than the alarm being reported correctly now.PR1700606
- When subscribing to sensor paths "/junos/system/linecard/packet/usage/", "/junos/services/label-switched-path/usage/" or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command "show network-agent statistics gnmi detail" output. The collector output might also contain missing sequence numbers. For example, the sequence number output might be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418
- The line card abruptly rebooted with a process crash when ISSU (In-Service Software Upgrade) is performed without properly disabling Jflow.PR1703910
- In Chassisd, Jvision thread takes more time in streaming of jvision packets because of volume of data and number of sensors involved with this daemon. Jvision thread engaged for more time to process streaming events caused Chassisd master thread to lose receive/send keepalive messages to/from other Routing Engine, which eventually was causing automatic Routing Engine switchover in most of the cases. To avoid this, fix done for exporting small payload jvision packets (formation of which takes less time) and deferring jvision thread more in an interval, to allow chassisd master thread to process high-priority hello/keep-alive messages. This means now, more number of packets is sent in one reporting interval and with larger spread (earlier same amount of data was sent with 2 or 3 packets of higher payload size, and 100ms of deferring time for jvision thread. This behaviour is increasing KPI-2 but lowering KPI-1 (payload size). It is not possible to back out changes done to solve keep-alive message loss issue. Hence we will have to keep Chassisd as an exception, when we measure/report KPI-2 values. Jvision in Chassisd has to give more priority/time to process keep-alive messages than sending of jvision packets. Hence delay between jvision packets are more. PR1706300
- For DHCP access-model and IFL-SETs, when the load-balancing group is not configured with the same port name for each user-plane, during IFL-SET weigh-based load-balancing, the last IFL-SET

over the max-weight could be incorrectly placed on both user-planes at the same time. This is because the load-balancing logic takes into account IFL-SET affinity by comparing the IFL-SET names on each UP in the load-balancing group to see if the same IFL-SET is already installed, and if it is installed already, to place the subscriber on an existent IFL-SET. However, the IFL-SET affinity check fails if the IFL-SET name is formed using different port names. This is documented in the Functional Spec of the RLI.So when this issue is seen, the IFL-SET names are different for each UP: UP xda, port up:xda:xe-2/0/0:0 UP xda1, port up:xda1:xe-0/1/0:2 which results in the creation of: IFL-SET: on UP "xda" IFL-SET = xe-2/0/0:0-101 AND on UP "xda1" IFL-SET:= xe-0/1/0:2-101 Then the names are different and the load-balancing logic cannot distinguish between the 2. PR1710447

- Second IFL macsec interface stats not working. PR1710867
- On all Junos platforms, Master and Backup Routing-Engine synchronization issues will be seen when chassisd (Chassis process) is restarted. The ksyncd (Kernel Synchronization) process crash will be observed on the backup RE and traffic would be impacted. PR1712352
- On MX platforms with MPC10/MPC11 line cards, when the Logical Tunnel (LT) interface is configured with family Virtual Private LAN Service (VPLS) and VLAN, unknown unicast traffic on this line card forwards the traffic instead of discarding it. Hence the services configured on the LT interface which will use unicast traffic are affected. PR1713523
- On Junos MX2010 and MX2020 platforms, when Junos Node Slicing is configured containing a sliced MPC11E line card (sub line card or SLC), a software upgrade or downgrade activity on the Guest Network Functions (GNF) containing the SLC can lead to a crash on the SLC. Traffic through the affected SLC will be impacted as it crashes and fails to come online.PR1715603
- The fast-lookup-filter is not working on the router's loopback interface with AlfaRomeo line cards in the routers. PR1718893
- With no-reduced-srh configured, MX304 removes the last SID value from the SRH. Expectation is Last SID should be retained in SRH when "no-reduced-srh" is configured. There is no impact to the traffic. Traffic flow fine, since the "SEGMENT-LIST" and "LAST ENTRY" are encoded properly in the packet. PR1721404
- In some srv6 scenarios, with no-reduced-srh configured, next header in SRH is not set and packets may be dropped as invalid hop option. PR1721429
- On the MX10008 platform, the low-priority stream might be marked as a destination error and as a result, the low-priority stream is stuck and all traffic might get dropped. Complete traffic blackhole is observed from one PFE to another. PR1724007
- Issue: Convert the VNI model in GW from "Global-to-Translated" excluded vlan range from trigger having traffic loss Trigger: Convert the VNI model in GW from "Global-to-Translated" Impact: Experiencing traffic loss in other vlan ranges. PR1725496

- On MX platforms supporting packet-triggered subscribers and policy control (PTSP) feature, a high percentage of packet triggered subscribers are getting stuck in 'Configured' state due to an authentication failure. PR1726136
- On Junos MX304 device , Enabling disk smart-check utility on the routing-engine with Innodisk SSD raises a false positive smart error, which is visible in 'show chassis alarms'. PR1726252
- On Junos EX92xx, MX304 and MX series platforms with MPC10, MPC11 and LC9600, traffic drop will happen with the attachment of family filter configured with percent policer (bandwidth-percent) via input-list/output-list. PR1726733
- On MPC1/2/3/4/5/6/7/8/9 line cards, route churn (add or deletes) when the ASIC usage crosses a threshold (ASIC usage is high) which leads to a FPC crash. PR1727427
- On all MX platforms with SPC3 cards and PCP (Port Control Protocol) with DS-Lite (Dual Stack -lite) configured , PCP client should renew the mapping before its expiry time to keep the PCP mapping always active. issue seen if the traffic from outside network (public network) toward B4 (softwire initiator) was suspended for sometime . when traffic started again toward B4 from outside network , it will be dropped and service will be impacted. PR1729801

## High Availability (HA) and Resiliency

- When GRES is performed with the interface em0 (or fxp0) disabled on the primary Routing Engine, then enable the interface on the new backup Routing Engine, it isn't able to access network.PR1372087

## Infrastructure

- A use after free vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). Refer to https://kb.juniper.net/JSA70198 for more information. PR1636063
- Earlier implementation of kvmclock with vDSO (virtual Dynamic Shared Object) which helps avoid the system call overhead for user space applications had problem of time drift, the latest set of changes takes care of initializing the clock after all auxiliary processors are launched so that the clock initialization is accurate. PR1691036

## Interfaces and Chassis

- MediaType value in SNMP/Jvision is not correct at the beginning after the switch comes up only for the DOWN interfaces where copper mediaType is connected till the link is not UP. This value is correct always in CLI output. Below are the recovery ways 1. Bring the link up (Connect the other side) 2. Restart dcd daemon. PR1671706
- IFL packet counters are not implemented for AMS interface. It is a new change. PR1673337
- This issue is specific to MX Series Virtual Chassis only and the issue is not seen during manual execution of the test case. The issue is seen only with the test script that too rarely and hence the exact trigger of the issue is not clear. PR1686425
- On Junos MX platforms, when Virtual Router Redundancy Protocol (VRRP) packets come from the LAG interface with delegate-processing enabled, it should be processed on anchor PFE. If it comes from non-anchor PFE - it goes to anchor PFE through the fabric. In that case, TTL is decremented. If a FW filter on the loopback interface is applied for VRRP with a ttl=255 condition, the VRRP won't work - there will be a service impact. PR1701874
- In case of evpn routing-instance, there will be an implicit bridge-domain created for VPLS route table. This BD index will be used by daemon DCD in successive commits. When igmp-snooping is enabled, mcsnoopd daemon publishes update on INET route table with BD index value 0, which is mismatching with the DCD. As a result, this might cause to flap ifls which are part of this routing-instance on successive commits. PR1712800

## Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20--50 ms traffic drop on the existing logical interface. PR1367488

## Layer 2 Ethernet Services

- If a client sends a DHCP request packet, and option 55 includes PAD option (0), a DHCP ACK will not be sent back to the client. PR1201413
- In the CBNG (XDA CUPS) environment, DHCPv6 subscribers fail to login over PPP over L2tp Tunneled. This setup has XDA CP and UP for both LAC and LNS. DHCPv6 subscriber is stacked over PPP from the Client side. While the PPP(v4 and v6) session gets established successfully, DHCPv6 subscriber traffic is being dropped at the LNS UP. Though this is the Release notes for 22.4R1

Release, issue is not seen in 23.1 based Dev Common Branch. Adding the release notes for 22.4R1 scope only.PR1683955

## MPLS

- Ingress will retry after lsp stay down for extended period of time or customer can clear lsp to speed up the retry. PR1631774
- The packets that have MTU size greater than the inet MTU size get dropped. PR1723145

## Network Management and Monitoring

- When maximum-password-length is configured and user tries to configure password whose length exceeds configured maximum-password-length, error is thrown, along with error 'ok/' tag is also emitted. (Ideally 'ok/' tag should not be emitted in an error scenario.) The configuration does not get committed.PR1585855
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. PR1614358

## Platform and Infrastructure

- With given multi dimensional scale, if configuration is removed and restored continuously for more than 24 times, MX Trio based FPC might crash and restart. During the reboot, there can be traffic impact if backup paths are not configured. PR1636758
- On Junos MX platforms with specific line cards, when PFE (Packet Forwarding Engine) is disabled, scenarios like multicast receiver join/leave that result in allocation and de-allocation of memory on disabled PFE can cause a memory leak. This is because memory is allocated on the disabled PFE, but not freed. PR1686068
- PVSTP protocol packets is getting duplicated when it tunnelled through Layer2 tunnelling protocol. Other protocol data units PDUs ( STP,VTP,CDP ) are not impacted. PR1686331
- On all Junos platforms, in a rare scenario, GRES (Graceful Routing Engine switchover) may result in LACP (Link Aggregation Control Protocol) on the new master being down which may cause an FPC crash. PR1720591

- On Junos MX and EX92XX with specific line cards, VLAN rewrites will not happen for traffic egressing from IRB(Integrated Routing and Bridging) interface over an L2 AE (Aggregated Ethernet) IFL (Interface Logical), if the L2 AE IFL is configured to perform VLAN rewrites on the frames. This happens when the IRB is configured as a routing-interface on EVPN (Ethernet Virtual Private LAN) or VXLAN (Virtual Extensible LAN) routing instances and the traffic has to egress on IRB over an L2 AE IFL. As a result, the frames are forwarded with incorrect VLAN tag information. PR1720772

## Routing Policy and Firewall Filters

- Delete single prefix from prefix-list will cause all the prefixes to be deleted.PR1691218

## Routing Protocols

- Errors might be seen on ephemeral commit during unified ISSU.PR1679645
- BGP LU statistics does not report correct statistics when sharding is enabled. PR1684238
- Junos OS Release 22.3 onwards, isis yang is uplifted to 1.0.0 version which has major change in existing OC path that was supported earlier. Since OC path has change, same need to reflected in translation script which is not done. As part of D27 release for cloud, translation script will be modified with newer OC path. Till then supported older OC config is broken. eventually D27 code will come back to DCB and things will work fine after that.PR1686751
- This issue is seen with only evo and not seen Junos. Its seen in a combination of Rsvp and IS-IS. Stats is getting incremented. PR1700063
- On all Junos and Junos OS Evolved platforms with dual-RE, after back to back graceful routing engine switchover (GRES) is performed, the periodic packet management process (ppmd) crash will be seen.PR1702687
- Show route advertising-protocol bgp reporting NextHop self rather than IP in the configured policy-statement for next-hop. Behavior change observed after JUNOS upgrade from 18.4 to 20.4. #set policy-options policy-statement set-NH-MX term to-PP-All then next-hop 20.20.20.1 show route advertising-protocol bgp 10.10.10.10 test.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden) Prefix Nexthop MED Lclpref AS path * 10.0.0.0/31 Self 65000 I The CLI output for Nexthop reported Self rather than IP address 20.20.20.1. PR1712527
- On all Junos and Junos OS Evolved platforms unexpected behavior of bandwidth based metric in IS-IS is seen since actual bandwidth is falling back to 0 bps when one of the member interface of AE (Aggregated Ethernet) bundle (interface-group) goes down. PR1718734

- On all Junos and Junos Evolved platforms with PIM (Protocol Independent Multicast), MVPN (Multicast Virtual Private Network) configured and when the number of downstream interfaces is more than three thousand, slow convergence of PIM joins is seen to take up more of the time and CPU, causing traffic loss for some time. PR1720708

## Services Applications

- When a configured tunnel interface is changed to another one, flow-tap-lite functionality stops working that is, packets don't get mirrored to content destination. But, this problem isn't consistently seen.PR1660588

## Subscriber Access Management

- On MX platforms in a scaled subscriber scenario the session database and IP pool database can get out of sync on the backup RE if there is subscriber churn. After RE switchover this condition will lead to immediate termination of new subscriber sessions if the assigned IP address is still in use by existing subscriber. PR1723183

## VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server might be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290
- This happens only when MVPN protocol has separate route targets configured and then both the address families are disabled. rpd (Routing process daemon) infra parsing does not check if MVPN protocol is disabled and hence will create the auto policies for route-targets if configured. So if those policies are not marked as active in MVPN configuration flow, it does not get resolved and thereby the policy object might not be valid thus leading to the core files.PR1700345

# 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.

## Application Layer Gateways (ALGs)

- The PPTP connection is not stable and is lost in DS-Lite+ALG scenario. PR1715315

## Authentication and Access Control

- Connection fails are observed on Junos despite a valid auth entry. PR1692398

## Class of Service (CoS)

- The oid tree jnxCosQstatEntry returns nothing for some interfaces after restarting class-of-service. PR1693977
- The AE (Aggregated Ethernet) link flaps on MX platforms with MPC10, MPC11, and LC9600 when high or medium priorities are configured on the queue. PR1699714
- Control packets would be dropped when CoS configuration under AE wildcard IFLs gets applied to AE control IFLs as well. PR1702836

## EVPN

- PBB-EVPN PE cannot learn remote CE MAC address due to ARP suppression enabled. PR1529940
- In EVPN-MPLS Mutihoming scenario DF election will get stuck in the Preference based state. PR1662954
- Routing Protocol Daemon (RPD) core files is observed due to remote bgp routes being flashed as active routes. PR1692249
- Traffic loss is seen when IPv6 entries are not refreshed and age out under the EVPN-VXLAN scenario. PR1699509
- A configuration change caused a rpd core files for the EVPN migrated instance. PR1701632
- ARP/ND doesn't resolve when extended-vlan-list is configured for the specific VLAN. PR1702016
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- Ping overlay vxlan replies Overlay-segment present even the bridge-domain has been deactivated. PR1715343
- The rpd core is seen in the long-running devices with EVPN enabled. PR1723832

## Forwarding and Sampling

- Deactivating and activating the GRES causes churn in dfwd filter addition/deletion. PR1697959
- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073
- Firewall filter counters are not written to accounting file when interface-specific knob is used. PR1706085

## General Routing

- Continuous Deactivate/activate of security config can lead to process restart. PR1566044
- Error message seen in clksyncd logs with SyncE/PTP configurations "ESYNC-Error:ferrari_zl30362_reg_write: Error, EEC(0) not yet initialized". PR1583496
- On backup Routing Engine during GRES, you might see "RPD_KRT_KERNEL_BAD_ROUTE: krt unsolic client.128.0.0.5+62000: lost ifl 0 for route" warning messages. PR1612487
- Delegated BFD sessions configured on routing-instance might fail to come up. PR1633395
- Junos OS: The kernel will crash when certain USB devices are inserted (CVE-2023-28975). PR1638519
- SR-stats : Per-Interface egress and per-sid Egress sensor stats do not take MPLS label length into account in the output octet calculations. PR1646799
- NAT session reverse traffic fails due to NAT routes getting deleted from routing instance. PR1646822
- The system does not got to shell prompt and hangs before rebooting after pressing N during PXE installation. PR1647534
- .include directives are deprecated, and support for them will be removed in a future version> warning comes for all custom services. PR1647592
- The user-defined speed does not take effect on the AE interface in certain scenarios on Junos platforms. PR1649958
- MX960:: Syslog errors HALP-trinity_vbf_flow_unbind_handler:1107: vbf flow 624626: ifl 526 not found,fpc5 vbf_var_get_ifs:754: ifl not found,PFE_ERROR_NOT_FOUND seen frequently on MPC7E in 5.5K DCIP/10kPPPoE FTTB Stress Test. PR1650598

- DHCP packets getting looped in EVPN-VXLAN setup. PR1657597
- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. PR1657704
- SSH non-default port configuration causes FPC offline after an upgrade to Junos OS Release 21.4. PR1660446
- The family bridge disappeared on commit check when Network-services lan has been configured. PR1661057
- GNF : No streaming data received for /telemetry-system/subscriptions/dynamic-subscriptions/. PR1661106
- RE1 alarms persistent even after removed from slot. PR1664544
- Switch Fabric Board information for supporting PTP on MX10k8 with MX10K-LC2101 LC(s). PR1664569
- Na-grpcd process core observed in telemetry services. PR1665516
- Multibit ECC error causes the whole MX platform chassis to go down. PR1670137
- BIOS version REH_P_MTR1_00.30.07 PR1675016
- 40G-QSFP+ flapping on mx204 PR1676005
- Bgp peers status is not as expected. PR1677624
- Traffic drop can be seen for MPC7/8/9 during ISSU in a specific scenario. PR1678130
- 
- PTP servo is stuck in ACQUIRING state with high CF when configured with LAG on MX10k8 with JNP10K-LC480 Linecards. PR1679657
- Auto-negotiation is not getting reflected on the MPC7E-10GE line card. PR1682962
- Traffic loss is seen with port-mirroring is enabled on AE interface in multicast downstream. PR1683192
- SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- [MAP-E] PPE errors seen during deactivate/activate of partial reassembly - ZTCHIP_MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x227fa5) PR1683845
- License-check might generate core files on MX routers. PR1685433

- PICs on the GNF failed to come online after the chassisd restart. PR1685453
- 100GE interface on JNP-MIC1 TIC module may keep flapping for 1 ~ 45 minutes after a specific 3rd party peer device (NRU02 from Arista/Pluribus) is booting up. PR1686012
- New CLI commands addition to support RE and Chassis power-cycle. PR1686577
- Subscribers are not able to connect to the device after the device reboot. PR1686654
- The pre-installed optional packages and JSUs will be lost after a VMHost rollback. PR1686825
- The PIMv6 is not getting enabled for L2TP subscribers. PR1687138
- CoS memory errors are seen when "chassis traffic-manager enhanced-priority-mode" is configured. PR1687642
- The LLDP output packets are not transmitting on the em0 interface of Junos and Junos OS Evolved platforms. PR1688023
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and AE. PR1688455
- The LACP would get stuck in a continuous update loop in the MC-LAG scenario. PR1688958
- PFE wedge will be seen due to fast link flaps. PR1688972
- DCSPF LSPs remain down indefinitely after router-id of the ingress router is changed. PR1689067
- Integration of RCP binary into the LTS19 code for Vmhost Platforms. PR1689100
- A 1G port on a QSFPP-4x10G transceiver will be down sometimes after the FPC restart. PR1689644
- Use latest os-package when upgrading. PR1691209
- The process rpd crash will be observed with the SRTE tunnel delete. PR1691459
- PCS errors and framing errors on 100GE interfaces on certain Juniper platforms. PR1692063
- JNP10K-LC9600: G.8275.1: Synce to PTP and SyncE to 1PPS Transient Response not meeting G.8273.2 mask. PR1692202
- A self-ping blackhole is seen along with fmpc process crash in a rare scenario causing traffic loss. PR1692365
- ALG child session will not be transported through the DS-Lite tunnel which might lead to traffic failures in absence of a direct route to the host. PR1692525
- The fxpc core files is generated and an FPC restart results in traffic impact. PR1692993
- Traffic loss is observed when the ECMP path is IRB over AE (IPv4->MPLS). PR1693424

- PDT: ONDATRA: context deadline exceeded observed on while adding NH , IPv4. PR1693567
- The fabspoked-pfe process crashes when a FATAL ERROR occurs in the PFE. PR1693697
- Traffic loss will be seen when MACSEC is configured. PR1693730
- dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert(). PR1694129
- license-check warning reported on backup RE by commit or commit check. PR1694935
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- On Junos MX chassis with LC2101 upstream SyncE source interface stuck in abort state. PR1695156
- BMP EOR is sent with wrong peer address causing BMP failure. PR1695320
- The BUM packets are getting dropped on MX platforms during egress processing due to PFE mismatch. PR1695438
- MPC11E goes offline with "fpc-slice" configured. PR1695510
- Traffic loss is seen when a MAC moves from dot1x port to non-dot1x port. PR1695771
- The "[01;31m[KFPC3:NPU0[m[K" string is missing in Npu memory after jvision exports data. PR1696021
- An rpd crash is observed while creating indirect-next-hop in the BGP sharding environment with bgp.l3vpn.0 with next-shop as a color route. PR1696035
- Dynamic Tables stuck in KRT Queue. PR1696199
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428
- After a chassis power cycle the backup Routing Engine is in Present state and the "Loss of communication with Backup RE (Routing Engine)" alarm is seen. PR1696816
- License key is not installed after upgrade. PR1696879
- Time error spikes seen during switchover of upstream source clock. PR1696880
- The dot1x authentication will not be enabled on interfaces with specific configuration combination. PR1696906
- In the rare scenario, huge PTP Time errors are introduced and propagated to the downstream devices after the chassis reboot. PR1696957
- Time error observed on JNP10K-LC2101. PR1697167

- FPC crash will be observed when firewall filter is unconfigured and reconfigured with same index. PR1697404
- The agentd process crash might crash in a telemetry scenario. PR1697986
- EVO jkey path changed under protocol/isis. "isis/levels" is missing. PR1698192
- Junos OS and Junos OS Evolved: A BGP session will flap upon receipt of a specific, optional transitive attribute in version 22.3R1 (CVE-2022-22184). PR1698446
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- Transit tunnels fails and remains down on all Junos based MX and SRX platform with IKE-NAT-ALG enabled. PR1699115
- Output of "show chassis ethernet-switch statistics" includes 32 bit values which might overflow. PR1699136
- The rpd crash is observed when rib-sharding configured. PR1699557
- User plane subscriber management daemon process crash when distributed multicast service is activated on several hundred subscribers. PR1700571
- JDI-REG:MX10008 :: core-renault-bbe-fpc0-indus.elf-crashinfo.0 core seen during teardown. PR1700909
- How to identify and report fabric link errors caused due to connector related issues. PR1700983
- JNP10K-LC9600: G.8275.1: Multiple GRES operation resulting in huge time error. PR1701017
- FPC restart and core files generated in MPLS scaled scenario with "always-mark-connection-protection-tlv" configured. PR1701147
- Traffic loss is seen due to interface flap when changing speed from 10G and 1G. PR1701183
- On Junos platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed. PR1701305
- CB2 not properly offlined upon Power Zone Failure. PR1701539
- Some PPPoE subscriber connection lost during RE switchover. PR1701739
- License will be deleted due to multiple FPC reboot or switchover on QFX/MX VC scenario. PR1703200
- The l2ld process will crash when an IFL is changed to trunk mode and a new VLAN is added. PR1703226

- RPF firewall filter errors during DHCP dual stack subscriber logout. PR1703270
- RE will crash when static route duplicates with an interface IP address. PR1703940
- The next-hop is shown as unicast instead of reject even when the IPv6 neighbor is unreachable. PR1704114
- Traffic is blocked on a queue when enhanced priority mode is configured. PR1704129
- Severity reclassification of queuing ASIC XQSS and memory parity error auto recovery. PR1706494
- RPD core@bgp_rt_terminate_job->bgp_process_rt_terminate->bgp_rt_terminate_subr->bgp_rto_adv_q_free () PR1704393
- A transit PTP packet is modified when passing through an MPC5E and MPC6G line card 100G ports part of PTP boundary/ordinary clock configuration. PR1704606
- Traffic blackhole in the event of a link failure (Rx LOS) for 1GE-SX/LX optics. PR1705461
- EAP authentication might not be successful with 802.1X server-fail configuration. PR1705490
- No network reachability when enabling the routing-service knob for PPPoE subscribers over AE. PR1706446
- The Inline Flow Monitoring is not working on Junos MX Series Virtual Chassis platforms. PR1708485
- The telemetry sensor will not be created for PCE initiated SR-TE. PR1709557
- Ports with QSA adapter are down. PR1709817
- ICCP connection establishment b/w Junos and EVO is not supported. PR1710448
- AIGP not distinguished with BGP-LU when rib-sharding is enabled. PR1710829
- The FPC will be offline after upgrading the system. PR1710855
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- FPC memory leak will cause FPC crash. PR1712076
- The traffic is dropped while passing through VCP link on MX Virtual Chassis with MPC10 line card. PR1712790
- The rpd process will crash when BMP is configured. PR1713444
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- IPv6 Fragmentation is not working on MS-MPC/MS-MIC in DS-Lite scenario. PR1713725

- The jnxOperatingDescr.1.1.0.0 is populated with blank. PR1714056
- Traffic loss is seen on telemetry streaming in BGP sharding environment. PR1714087
- Traffic loss is seen on telemetry streaming in BGP sharding environment. PR1714087
- Illinois: CP: Incorrect multicast adjustment shown with interface-set queuing. PR1714271
- PPPoE subscriber connection on dynamic VLAN can fail on Junos MX platforms. PR1714778
- JDI-REG: [MX480][MX2010]: IPSEC:: IPsec Tunnels are not coming up after configuring IPSEC under Service-sets. PR1715071
- The bbe-smgd process is seen to crash if a large scale PWHT configuration is present. PR1715410
- J-flow sends wrong IP in sampling records when NAT is configured for traffic along with input sampling. PR1716707
- A 10G port on a MPC2E or MPC3E 4x10G MIC can randomly flap constantly every few seconds. PR1716766
- The `set forwarding-options evpn-vxlan shared-tunnels` command will not be available for EX92XX and MX series platforms. PR1716881
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. PR1717105
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- In a DHCP ALQ subscriber scenario delete-binding-on-renegotiation statement does not work as expected due to a synchronization error between the primary and the backup routers. PR1718342
- MX2010::DVAITA-SUBLC: Fabric plane on few PFEs assigned to SLC shows as unused. PR1718834
- The PPTP connection itself won't work when trying to establish PPTP connection along with DSLITE. PR1718840
- The rpd process crash will be observed while creating PCEP tunnel. PR1720031
- The dcpfe process crash will be observed in the EVPN-VXLAN multihoming scenario. PR1721322
- Observed re0:rpdagent:20852:TRACE_ERR Rtsock_ERROR_MSG Function = "rpd_rtsock_dispatch", error = 7, msg = "rttable after device reboot. PR1690105
- RPD core is seen after the switchover. PR1694773
- BFD session failed when configured on the loopback sub interface. PR1721714

## High Availability (HA) and Resiliency

- Traffic will be impacted if GR-ISSU fails. PR1694669
- The rpd crash will be observed when any commit is performed. PR1701146

## Interfaces and Chassis

- Management interface speed is incorrectly reported as 10G instead of 1G. PR1636668
- The dcd core might be seen on the backup Routing Engine after GRES is disabled if targeted distributed configuration is used. PR1650676
- The PFE I/O chip setup failed for some interfaces and causes those interfaces missing in PFE after backup chassis upgraded via Sequential Upgrade. PR1670345
- Node Slicing: In a rare scenario, the FPC/SLC will get stuck in the ready state after a restart. PR1682271
- Subscribers will fail to negotiate the PPP session and be unable to login post-software upgrade. PR1686940
- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. PR1692404
- VRRP Master session on AE ifl having child links on Satellite Device stops transmission post GRES. PR1697394
- MX Series Virtual Chassis: The backup VC router could become master after the system reboot. PR1697630
- The cstm4 interface on MIC-3D-8CHOC3-4CHOC12 cannot be partitioned to more than 10 E3 interfaces. PR1701875
- FPC offline can be seen on MX-VC during the sequential upgrade. PR1706268
- Not getting the expected values while verifying ['linktrace_egress_mac_address', 'linktrace_flags', 'linktrace_ingress_mac_address', 'reply_ttl'] On devices. PR1707126
- The firmware upgradation will fail for MPC7E line card in MX-VC scenario. PR1713502
- Issue in VRRP inline adjacency whenever a master router uplink goes down on MX platforms. PR1720943

## J-Web

- Junos OS: Multiple vulnerabilities in J-Web(CVE-2023-28962). PR1698072
- Junos OS: Multiple vulnerabilities in J-Web (CVE-2023-28963). PR1698075

## Layer 2 Features

- The rpd process crash will be observed during VPLS to EVPN migration. PR1729052

## Layer 2 Ethernet Services

- MX240:Verify VRRP stats is failed after Deactivate the Access interface. PR1666943
- IPv4 ALQ is not working with authentication. PR1688272
- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance. PR1689005
- A dcd process crash is observed continuously when the dhcp-service is restarted. PR1698798
- DHCPv6 client options missing in solicit messages if TLV's (Type Length value) exceed a certain length. PR1702831
- On all Junos MX/PTX platforms multiple LACP timeouts causes traffic loss due to PPMAN resource starvation. PR1706224
- A jdhcpd process crash is observed on all Junos platforms. PR1713619
- The DHCPv4 relay will send two option-82 to the server and the DHCP session will not be established. PR1714260

## MPLS

- LDP IPv6 session fails to come up in dual transport scenario. PR1683410
- Traffic is not load-balanced when one of the next-hop LSP is down. PR1690110
- The rpd crash will be observed during the MPLS label block allocation. PR1694648

- Restarting FPC or router reboot might causes some CCC interfaces to go down due to a 'Remote CCC down'. PR1694777
- The rpd core generated and routing daemon gets restarted. PR1696017
- [MX]L2VPN ping is failing when UHP rsvp LSP is used. PR1697982
- The rpd core files and traffic loss is observed on Junos and Junos Evolved platforms. PR1701420
- Memory leak issue in TED. PR1701800
- LDP flaps will be observed with LT interface with VLAN and LDP running between the logical-system instance and global instance. PR1702220
- When LDP dual transport is enabled, LDP V4 connection id changes from dual transport v4 id to router-id when rouer-id changes. PR1706064
- PathErr with RoutingProblem error code generated unexpectedly during dual failure local repair. PR1713392

## Platform and Infrastructure

- The MPC hosting an AE member interface with a shared bandwidth policer configured at the AE could crash upon encountering an HMC fatal error. PR1666966
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. PR1678506
- The traffic loss duration increases during the LSP switchover. PR1681250
- BGP session flap with error BGP_IO_ERROR_CLOSE_SESSION. PR1685113
- PFE will be disabled whenever XQ_TOE CM error is being detected. PR1692256
- Packets received from type-5 tunnel are not sent out to local CE in EVPN-VxLAN scenario. PR1696106
- The egress rewrite-rule might not work as expected for traffic entering the AE interface. PR1700860
- Severity reclassification of queuing ASIC XQSS and memory parity error auto recovery. PR1706494

## Routing Policy and Firewall Filters

- Commit error will not be seen after deactivating routing-instance applied under firewall filter. PR1720389

## Routing Protocols

- JDI-RCT : PPMD crashed at ppm_destroy_distrib_proto_stats_group_entry ( ). PR1660299
- SSH access is possible without ssh setting. PR1664512
- Traffic loss observed due to multicast routes exceeding the scale for OISM feature. PR1671901
- More than expected traffic loss is seen with ECMP FRR enabled during link down scenario. PR1687887
- BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway". PR1689904
- BMP will not send EOR message. PR1690213
- The rpd process crashes on a system running with IGP shortcuts. PR1690231
- The rpd crash is seen when using a BGP neighbor telemetry subscription in a sharding environment. PR1692255
- Deletion and addition of BGP transport-class caused the rpd crash. PR1692320
- Configuration check-out failed when applying "irb with inet and inet6" and "inet6.0 static route". PR1692484
- When Lsys is configured with 'family route-target', there is a certain corner case scenario where Lsys shutdown does not complete. PR1695050
- Silent drop in traffic is observed when removing the BGP routes take a long time to get removed from RIB. PR1695062
- Commit error when trying to configure rib-group under BGP in no-forward (default) RI. PR1696576
- Incorrect SR-TE secondary path weight makes the secondary path active in forwarding table. PR1696598
- The BGP Auto-discovered neighborship is not formed after a reboot. PR1699233

- The BGP graceful-shutdown community is not advertised on Junos/Junos Evolved platforms. PR1699633
- OSPF stuck in InitStrictBFD state for the neighbor which doesn't send LLS header. PR1700966
- Junos prefers SRMS advertised label over IS-IS/OSPF SID label advertised via opaque-AS Extended-Prefix. PR1702456
- Anycast PIM doesn't work when the peer has an authentication key configured for MSDP. PR1703707
- OSPF routes are not getting installed after the interface is flapped. PR1705975
- The BFD session would flap when the GRES is triggered with single-hop BFD over AE interfaces configured. PR1706018
- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. PR1711153
- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406
- Multipath route is not getting compute and skip the multipath eligibility check. PR1716153
- BGP connection doesn't establish when it is configured with rfc8950-compliant under logical-systems on all Junos and Junos OS Evolved platforms. PR1716946
- RPD crash observed when TI-LFA is configured and same flex-algorithm-locator is configured on multiple nodes(anycast flex-algorithm locator). PR1719033
- Multiple flaps of the interface will cause the BFD session to be down. PR1725971

## Services Applications

- A stale nat-long-route entry is present in the device causing incoming packets to be dropped. PR1719216

## Subscriber Access Management

- The interim-rate under radius-options feature is not working post implementing BBE statistics performance and scale improvements. PR1695956

- A few subscriber sessions will not be up post RE switchover. PR1697392
- Externally assigned IP address subscriber sessions logout after GRES. PR1709574
- High CPU utilization is seen on Junos MX series platforms. PR1710145
- IPv4 and IPv6 address allocation will be impacted due to changes in address pool configuration. PR1715490

## User Interface and Configuration

- gNMI GET request fails when OpenConfig is present. PR1697869

## VPNs

- 19.2TH:VPN:SRX5600: While verifying "show security ipsec next-hop-tunnels" output in device the IPsec SA and NHTB entry is not getting cleared after configuring firewall filter. PR1432925
- Routes flapping when configuration changes are applied to custom routing instance. PR1654516
- ike cookies didn't change in rekey lifetime expire cases after manual failover. PR1690921
- Two-digit numbered interfaces cannot be used as protect-interfaces. PR1695075
- VMX :: JDI-REG:Virtual:MVPN tunnel is not synced to back up router. MPVN tunnel interface is missed in show multicast route inet instance BLACK group 225.1.1.1 source-prefix 1.1.1.1 output. PR1710323
- The iked process will crash when VPN tunnels parameters are not matching. PR1716092

## Migration, Upgrade, and Downgrade Instructions

**IN THIS SECTION**

This section contains the upgrade and downgrade support policy for Junos OS for MX 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 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**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) | 36 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 NFX Series

IN THIS SECTION



## What's New

There are no new features or enhancements to existing features in Junos OS Release 22.4R2 for NFX.

## What's Changed

IN THIS SECTION



Learn about what changed in this release for NFX Series devices.

## Software Installation and Upgrade

- **Two-step Downgrade (NFX150, NFX250 NextGen, and NFX350)**—You cannot downgrade Junos OS Release 23.1R1 directly to certain releases (listed in the **Target Release** column in Table 7 on page 77). As a workaround, you can perform downgrade as a two-step activity, in which you downgrade

Junos OS Release 23.1R1 first to a corresponding intermediate release (listed in Table 7 on page 77), and then to the target release.

**Table 7: Release Compatibility for Downgrading Junos OS 23.1R1 on NFX Series Devices**

| Target Release | Intermediate Release |
|---|---|
| Any 22.4x release earlier than 22.4R2 | 22.4R2 |
| Any 22.3x release earlier than 22.3R2. | 22.3R2 |
| • Any 22.2x release earlier than 22.2R3.<br>• Any 22.1x release or earlier releases. | 22.2R3 |

PR1694074

## 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.

## Interfaces

- On the NFX250, the LACP subsystem does not start automatically when the dc-pfe process is restarted.

  Workaround—Deactivate and then activate the aggregated Ethernet interface.

  PR1583054

## Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interfaces (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. PR1512331

## 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.

## Interfaces

- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface` command displays the Front panel LED status as `up`, the front panel LED is not ON

  PR1702799

- When issuing request support information, there was a syntax error when looking at the nfx-back-plane (was nfx-backplane, instead of nfx-back-plane)

  PR1720228

## VPNs

- IPSec tunnel is down if IKE external-interface is configured with IPv4 and IPv6 address. As a workaround, specify the local-address inside the ike gateway object if the configured external-interface contains both IPv4 and IPv6 address hosted on it.

  PR1716697

## 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 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**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) | 36 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 PTX Series

IN THIS SECTION

## What's New

There are no new features or enhancements to existing features in this release for the PTX Series.

## What's Changed

IN THIS SECTION



Learn about what changed in this release for the PTX Series.

## EVPN

- **Specify the UDP source port in a ping overlay or traceroute overlay operation**—In Junos OS releases prior to 22.4R1, you could not configure the udp source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash`will override any other hash-* options that may be used to determine the source port value.

## Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## Platform and Infrastructure

- **The `ping host | display xml` command produces CLI output without errors (ACX Series, PTX Series, and QFX Series)** — In Junos OS release 22.4R2, the `ping host | display xml` command now produces CLI output formatted in XML.

  [See ping.]

## Known Limitations

IN THIS SECTION



Learn about known limitations in this release for the PTX 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

- On all Junos OS platforms, agentd process crash will be seen in telemetry streaming longevity test. PR1647568

- On PTX10002, all odd ports have a WAN re-timer connected to it , which might introduce more time during fault recovery, such as LocalFault clear. Therefore, sometimes even if the fault is of the order of milliseconds, the port might still get hold-time expired and flap when the configured `hold-time down` less than 3s. The behavior is confirmed as hardware limitation.PR1687092

## Routing Protocols

- The rpd process crashes and generates a core file if 100 transport-classes are configured. PR1648490

## Open Issues

**IN THIS SECTION**



Learn about open issues in this release for the PTX 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

- In the platform using indirect next hop (INH), such as unilist as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines. When the version-id of session-id of INH is above 256, the Packet Forwarding Engine might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in Packet Forwarding Engine. It might lead Packet Forwarding Engine to have a different view of unilist against load-balance selectors. Then, either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- When subscribing to sensor paths **/junos/system/linecard/packet/usage/**, **/junos/services/label-switched-path/usage/** or other line card (Packet Forwarding Engines) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command `show network-agent statistics gnmi detail` output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. PR1703418
- In Chassisd, Junos Telemetry interface thread takes more time in streaming Junos Telemetry interface packets because of the volume of data and number of sensors involved with this daemon. Junos Telemetry interface thread engaged for more time to process streaming events cause chassisd master thread to lose receive or send keepalive messages to and from other Routing Engine, which eventually cause automatic Routing Engine switchover in most of the cases. PR1706300
- On QFX10000 and PTX Series platforms, traffic going over unilist is dropped when unilist member goes from next-hop hold state to unicast and aggregate state.PR1713279

## Multicast

- On Junos OS PTX Series platforms, the traffic might silently drop or discard. This is because of the next-hop installation failure for multicast Resource Reservation Protocol (RSVP) Point to Multipoint (P2MP) traffic. This issue might only be encountered in a scaled RSVP P2MP environment after a network event which might cause reconvergence. PR1653920

## Routing Protocols

- On all Junos OS and Junos OS Evolved platforms unexpected behavior of bandwidth-based metric in IS-IS is seen since actual bandwidth is falling back to 0 bps when one of the member interface of aggregated Ethernet bundle (interface-group) goes down. PR1718734

## Resolved Issues

**IN THIS SECTION**

Learn about the issues fixed in this release for PTX 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

- Junos OS: The kernel will crash when certain USB devices are inserted (CVE-2023-28975). PR1638519
- The user-defined speed does not take effect on the aggregated Ethernet interface in certain scenarios on Junos OS platforms. PR1649958
- On PTX5000 platforms when a command is issued to power off an FPC, it gets stuck in the 'Announce Offline' state. PR1683562
- SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- Type elem not added for INTEGRATED_CIRCUIT. PR1685676
- Currently no alarm is raised when onchip memory exhausts on the PTX10008 based FPCs. PR1690289
- On all Junos OS PTX3000 and PTX5000 devices, upgrading from older Junos OS to 20.2R1 or later release might trigger intermittent link flapping. PR1693367
- When using the proprietary subscribe RPC for telemetry, the "isis/levels" keyword is missing from the jkey output for leaf lists. PR1698192
- Traffic loss can be seen while switching between primary and fallback sessions in MACsec setup. PR1698687
- Ports with QSA adapter are down. PR1709817
- gNMI line card (PFE) sensor /junos/system/linecard/packet/usage/ may have packet drops (gNMI translator lookup failures). PR1711779
- FPC memory leak will cause FPC crash. PR1712076

- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Convergence delay is seen when FPC is offlined under heavy traffic and scaled scenario. PR1719956

## Routing Protocols

- Traffic loss is more than expected when ECMP FRR is enabled in link down scenario. PR1687887
- The rpd process crashes on a system running with IGP shortcuts. PR1690231

## VPNs

- The aggregated Ethernet interface will be down when you configure. `l2circuit-control-passthrough`. PR1699493

## 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 PTX Series. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

**NOTE**: Junos OS 22.4 is the last supported release on many PTX Series products. For more information on EOL dates, see : PTX Series Hardware Dates & Milestones.

## Basic Procedure for Upgrading to Release 22.4

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**: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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

**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 router, 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.

**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 22.4R1:

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

   https://support.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 by 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 routing platform or to your internal software distribution site.
10. Install the new jinstall package on the router.

> **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/junos-install-ptx-
x86-64-22.4R1.9.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/junos-install-ptx-
x86-64-22.4R1.9-limited.tgz
```

Replace the 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.

Adding the `reboot` command reboots 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-PTX-X8 Routing Engine. For upgrading the host OS on this router 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.

**NOTE**: After you install a Junos OS Release 22.4 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.

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

## Upgrading a Router with Redundant Routing Engines

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

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.

## 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**Table 9: EOL and EEOL Releases**

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

IN THIS SECTION



## What's New

There are no new features or enhancements to existing features in this release for QFX Series switches.

## What's Changed

IN THIS SECTION



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

## EVPN

- **Commit error if interconnect and local route distinguishers have the same value**-On EVPN data center interconnect (DCI) gateway devices, if you configure an interconnect RD at the [`edit routing-instances` *`name`* `protocols evpn interconnect`] hierarchy, the interconnect RD must be different from the local RD in the routing instance. If you try to configure the same value for the interconnect RD and the local RD in a routing instance, the device enforces this requirement by throwing a commit error. However, with DCI seamless stitching for EVPN Type 5 routes, you don't see the commit error prior to this release. Starting in this release, the device throws the commit error to enforce this condition for DCI stitching with Type 5 routes.

  [See route-distinguisher.]

## Network Management and Monitoring

- `operator` **login class is restricted from viewing NETCONF trace files that are** `no-world-readable` **(ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## Platform and Infrastructure

- **The** `ping host | display xml` **command produces CLI output without errors (ACX Series, PTX Series, and QFX Series)** — In Junos OS release 22.4R2, the `ping host | display xml` command now produces CLI output formatted in XML.

  [See ping.]

## 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.

## Platform and Infrastructure

- All QFX5000 platforms supports DF only at port level granularity (In other words, for all evpn instances hosted on an ESI, only one of the Multihomed QFX5000 nodes can be DF). Below config options are recommended Have df-granularity knob (with which QFX5k platforms seem to have been qualified). Here, few bytes from esi value itself, instead of vlan-id are used for MOD-based DF. PR1672383
- On QFX10008 devices, statistics for multicast packets is not as expected as the packets has the Layer 2 header stripped during replication in the Packet Forwarding Engine because of which it is not forwarded to the next hop. PR1678723
- All QFX10000 devices might use udp port 67 as the source port in the VXLAN udp header. PR1727072

## 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.

## Interfaces and Chassis

- The following two error messages gets generated brcm_rt_ip_mc_ipmc_install:2455 Failed (Invalid parameter:-4) This message is due to IPMC Group being used is not created, when RE tried to add this check indicates there is a parameter mis-match. brcm_rt_ip_mc_ipmc_install:2455 Failed (Internal error:-1) This message is due to Failure to read IPMC Table or any memory/register. PR1461339

## Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when a new logical interface is added and if there is already a logical interface on the physical interface, there is 20--50 ms traffic drop on the existing logical interface. PR1367488

## Layer 2 Ethernet Services

- On QFX5100 and QFX5110 devices, vendor-id format maybe incorrect for network ports. This does not impact the ZTP functionality or service. The DHCP client config is coming from two places, i.e AIU script and vsdk sandbox. The DHCP client config coming from AIU script has the serial Id in vendor id where as the default configuration from sandbox does not have. PR1601504

## Platform and Infrastructure

- On the QFX5100 line of switches, inserting or removing optics on a port might cause a Packet Forwarding Engine Manager CPU spike and an eventual microcode failure. PR1372041
- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548
- In the platform using INH (indirect next hop, such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the session fast-reroute might be enabled in Packet Forwarding Engines (PFEs). When the version-id of session-id of INH is above 256, the PFE might not respond to session update, which might cause the session-id permanently to be stuck with the weight of 65535 in PFE. It might lead PFE to have a different view of Unilist against load-balance selectors. Then either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. PR1501817

- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. PR1529596
- On QFX5110 Virtual Chassis, FPC may gets disconnected with 24000 DHCPv6 relay scaling, after the traffic is stopped. "pfe_listener_disconnect" error messages may be seen. PR1594748
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VXLAN can use the version 21.3R1. PR1597276
- On all devices running Junos OS or Junos OS Evolved, where this is a high BGP scale with flapping route and the BGP Monitoring Protocol (BMP) collector/station is very slow, the rpd process might crash due to memory pressure. PR1635143
- When MACSEC and VRRP are enabled on QFX5120 VC, MACSEC sessions are flapping at random times. Without VRRP this issue is not seen. PR1640031
- On all QFX5100 Virtual Chassis platforms, after the reboot, Virtual Chassis port (VCP) ports might not establish a VCP connection and Cyclic Redundancy Check (CRC) errors are also observed. PR1646561
- On QFX platform, v6 ifl stats are being derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable. PR1653671
- 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. PR1665800
- On QFX5110 platforms with more than one l2circuit configured, deactivating and activating the l2circuit configurations successively might cause traffic drop on one or more Layer 2 circuits. PR1666260
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. PR1679919
- On QFX5000 series platforms, configuration-change/protocol flapping/port flapping in Ethernet Virtual private network (EVPN) Virtual Extensible LAN (VXLAN) can cause traffic loss (changes related to the underlay network). PR1688323
- On QFX5100 Virtual Chassis (VC) and Virtual Chassis Fabric (VCF) platforms on upgrading Virtual Chassis Fabric (VCF) and toggling the interface, when FPC (Flexible PIC Concentrators) is disabled and rebooted, the member fails to join the virtual chassis and the interface remains disabled even after been enabled. PR1689499
- The `show chassis hardware` command indicates duplicate entries for PSU and FAN tray after USB clean install or zeroize. PR1704106

- as list_get_head function is called in multiple places in pfe we needed previous 3 functions on the stack which had called list_get_head so we could debug why 'list_get_head list has bad magic ' this error has occured. PR1705853
- On QFX10000 devices, traffic going over unilist is dropped when unilist member goes from next-hop hold state to unicast or aggregate state. PR1713279
- On QFX5000 devices, the output of the `show forwarding-options enhanced-hash-key` command does not indicate weather the `ECMP Resilient Hashing` is enabled or disabled. PR1725916

## Routing Protocols

- On all QFX platforms unexpected behavior of bandwidth based metric in IS-IS is seen since actual bandwidth is falling back to 0 bps when one of the member interface of AE (Aggregated Ethernet) bundle (interface-group) goes down. PR1718734

## Virtual Chassis

- On QFX5100 platforms running QFX-5e images in Virtual Chassis setup, when Virtual Chassis Port (VCP) links are connected between PHY and PHYLESS ports, CRC alignment errors will be seen. As a result, there can be traffic loss on these links. PR1692102

## 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.

## EVPN

- In EVPN-MPLS Mutihoming scenario DF election will get stuck in the Preference based state. PR1662954
- Traffic drop would be observed due to the VTEP tunnels not being established in the EVPN-VXLAN scenario. PR1700196
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. PR1709007
- The generation of the VXLAN table appears to be lost after loading configuration. PR1712805

## Forwarding and Sampling

- The device is using the MAC address of the IRB interface even after configuring static MAC for a default gateway. PR1700073

## Interfaces and Chassis

- Management interface speed is incorrectly reported as 10G instead of 1G. PR1636668
- The Unicast traffic is dropped on QFX5100 Virtual Chassis. PR1695663

## Platform and Infrastructure

- On QFX10008 device, while verifying em0 statistics interface Speed is displaying in Gbps instead of mbps. PR1589942
- Virtual Chassis members are reloading randomly. PR1671293

- QFX10000 series platforms generates error messages constantly and IPv6 routing is not performed when configured rpf-check and inet6 on VXLAN enabled interface and trying to resolve arp ndp. PR1677422
- The protocol MTU for the IRB interface is not rolled back when the MTU of the IRB or IFD interfaces is modified or deleted. PR1685406
- QFX5120 will drop ingress traffic on an l2circuit configured interface on continuous flaps. PR1687257
- CPU will not reset automatically and will have abnormal behaviour when CAT Error is observed. PR1687790
- The LLDP output packets are not transmitting on the em0 interface. PR1688023
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregated Ethernet interface. PR1688455
- Packet Loss seen on the EVPN-VXLAN spine router router. PR1691029
- Traffic loss is observed when the ECMP path is IRB over AE (IPv4->MPLS). PR1693424
- PFE crash is seen on all Junos QFX5000 platforms with L2PT configuration. PR1694076
- dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert(). PR1694129
- All members of the VCF will not reboot on QFX5000 platforms. PR1694996
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. PR1695057
- Intra VLAN communication breaks in SP style config using VXLAN. PR1695058
- BMP EOR is sent with wrong peer address causing BMP failure. PR1695320
- On QFX5110-VC-VCF platforms, traffic impact is seen when the firewall filter with DSCP action is enabled. PR1695820
- Traffic forwarding fails when deleting all L2 related configurations. PR1695847
- On QFX5110-32Q Virtual Chassis, after loading "20.4R3-S5.3" dcpfe core is observed and device is unstable. PR1695943
- The BFD session might be stuck in "Init" state on certain QFX5000 platforms. PR1696113
- Traffic drop is observed for the VCP ports when there is traffic congestion in the egress queues. PR1696119
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. PR1696428

- VSTP will not work in the EVPN-VxLAN network. PR1696979
- Assigning VNI to VLAN will cause a small number of packets lost on other VLANs on the same interface. PR1697244
- Local multicast traffic forwarding issue can be seen on QFX5K in EVPN-VXLAN OISM setup. PR1697614
- Traffic drop is observed after deleting or deactivating the logical interface. PR1697827
- PE device changes an outer tag-id in a local return environment. PR1697835
- Dot1x authentication failure for EVPN VXLAN enabled port. PR1697995
- On QFX5K switch, VGA is not working when SP style config is mixed with EP style configuration. PR1698491
- Adaptive sampling will not work if the system clock is turned backward. PR1699585
- The BFD session remains in init/down state in the Virtual Chassis scenario. PR1701546
- License will be deleted due to multiple FPC reboot or switchover on QFX Virtula Chassis scenario. PR1703200
- The dcpfe process crashes which leads to FPC restart. PR1706515
- The FPC crash can be seen on QFX5000 platforms during simultaneous soft and hard OIR of SFP. PR1707094
- The spine does not reply to RS messages coming via the VXLAN tunnel in the CRB scenario. PR1707679
- Traffic drop is observed with the `vxlan encapsulate-inner-vlan` command on the QFX10000 platforms. PR1709605
- Ports with QSA adapter are down. PR1709817
- Virtual Chassis members are split when removing and inserting em0 cable. PR1709938
- The `fpc0 list_get_head, list has bad magic (0x0)` error message might be the output after the commit operation is complete. PR1710776
- The FPC will be offline after upgrading the system. PR1710855
- On QFX5110 devices, chassis alarm does not get generated when inserted PSU module which has a different airflow. PR1710952
- When a 100G transceiver is used as a VC port, the VC port will either not come up or come up as 40G. PR1711407

- Traffic drop is observed in the EVPN-VXLAN scenario with Type-2 ESI tunnel. PR1711889
- VXLAN traffic gets dropped after new Layer 3 VLANs are created. PR1712405
- On QFX5120-32C devices, the dcpfe process generates core file after restarting the l2-learning process. PR1713133
- The member interface will not be added to the AE bundle if the link-speed of the AE interface doesn't match that of the member. PR1713699
- The dcpfe process crashes on QFX5000 devices. PR1716996
- Traffic loop is seen due to incorrect root bridge ID. PR1717267
- Traffic egressing over the EVPN-VXLAN tunnel will drop which has AE interface as underlay. PR1718528
- ESI:FRR:L2ALD core at l2ald_vxlan_ifl_create_msg_build. PR1718534

## Routing Protocols

- The BGP Auto-discovered neighborship is not formed after a reboot. PR1699233
- The BGP graceful-shutdown community is not advertised. PR1699633
- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. PR1712406

## 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.

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 **20.3** 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 20.3 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-x86-64-22.4-R2.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 20.3 `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-x86-64-22.4R2.9.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-
x86-64-22.4R2.9.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 18.3R2.

**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-x86-64-20.4R2.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-x86-64-20.4R2.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-
x86-64-22.4R2.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-
x86-64-22.4R2.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-x86-64-22.4R2.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-x86-64-18.3R2.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R2.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 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**Table 10: 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) | 36 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 SRX Series

IN THIS SECTION



## What's New

There are no new features or enhancements to existing features in this release for SRX Series devices.

# What's Changed

Learn about what changed in this release for SRX Series.

### Network Management and Monitoring

- **Operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

### VPNs

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls:
  - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.
  - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.
  - In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
  - In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

# Known Limitations

IN THIS SECTION



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

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

## High Availability

- When you are upgrading an SRX Series device from Junos OS Release 22.3R1 to the next version of the Junos OS release, you may experience some disruption in traffic.PR1722689

## Network Address Translation (NAT)

- While port ranges are configured as part of NAT source pool, port affinity allocation can fail as when the affinity allocation is failed for a flow then the port random allocation is set. Random allocation can allocate any port and the allocation failure can grow. PR1678563

# Open Issues

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

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

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. PR1546430
- FTPS connection to the server will not be successful until the first attempt is aborted and a new connection to the server is made. PR1715918

### General Routing

- IPsec rekey fails when SRX is configured with kilobyte based lifetime in remote access solution. PR1527384
- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- All VPN traffic may internally drop during encryption / decryption processing in HW engine requiring PFE plane reset. PR1630981
- SRX550HM interfaces LED of ge-0/0/6-9 will auto turn off after device bootup some minutes.PR1634965
- Device does not drop session with server certificate chain more than 6.PR1663062
- FIPS mode is not supported in this release for SRXSME devices.PR1697999
- On SRX380, the Autonegotiation status on the 1G/10G ports may be incorrectly displayed as "Incomplete". This has no impact to traffic.PR1703002
- On SRX platforms, log streaming to the security director cloud fails on TLS(Transport Layer Security) when DNS(Domain Name System) re-query is performed.PR1708116
- On Junos SRX4600 platform running with an image with Glacis FPGA (Field Programmable Gate Array) v1.5d, ping is failing from a remote host to one of the SRX4600's WAN interface after updating to an image with Glacis FPGA v1.63.PR1712167

### Layer 2 Ethernet Services

- If a client sends a DHCP request packet, and option 55 includes PAD option (0), a DHCP ACK will not be sent back to the client. PR1201413

### User Interface and Configuration

- On all Junos and Junos Evolved platforms configured with persist-group-inheritance, which is enabled by default from 19.4R3 onwards, might lead to mustd process crash in highly scaled configuration.PR1638847

### VPNs

- First time when we add this command the existing active connections are not changed, only the new connection after this command will be taken into effect. PR1608715

## Resolved Issues

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

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)

- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed. PR1688986

### Chassis Clustering

- New secondary node to go into a disabled state after ISSU and failover RG0 because of fabric link failure. PR1678772
- Policy configured with condition route-active-on import is not working properly after RG0 failover. PR1686648
- The secure tunnel interface does not work properly in SRX standalone mode. PR1702763
- GTPv2 Message Filtering is not working. PR1704472

### Flow-Based and Packet-Based Processing

- Application traffic drop seen on all SRX platforms due to TCP window size issue. PR1699578
- Core dump will be seen when user is changing interface configuration PR1704623

- A flowd process crash is seen on SRX4100/4200/4600, vSRX, and SRX5K with SPC3 card when a route is changed frequently. PR1705996
- The IPv6 source-level fragmented SCTP packets passing through an IPSec tunnel will be dropped. PR1708876

### General Routing

- HA AP mode on-box logging in LSYS and Tenant: Security log verification is failing as the contents of binary log file in LSYS are not as expected. PR1587360
- SRX4600 - Packet drop or srxpfe coredump might be observed. PR1620773
- SRX5600/5800 - SNMP mib queries may result in occasional response timeouts. PR1631149
- 21.3R2:SRX_RIAD:srx1500,srx4200:SKYATP:IMAP/IMAPS Email permitted counter is not incremented in AAMW email statistics while testing whole email block. PR1646661
- No alarm under booting from backup partition. PR1646943
- show fwauth user details is not displaying group information. PR1659115
- SRX4600HA might not failover properly due to a hardware failure. PR1683213
- The user authentication page is not rendering on the client browser. PR1685116
- The chassis cluster will not respond to DNS queries when configured with DNS proxy service. PR1688481
- SRX1500 chassis cluster port ge-0/0/1 does not work in switching mode. PR1690621
- The process srxpfd/ flowd will crash on SRX devices. PR1694449
- TCP packet drops are seen when services-offload is enabled. PR1702138
- The flowd crash and core will be observed when TLS 1.3 session ticket is received on SSL-I. PR1705044
- TX would be stuck and no packet can be transferred by the SPC3 card. PR1706756
- Setting the security log profile without a category or stream will lead to srxpfe process crash. PR1708777
- The ECDSA certificate based websites are not accessible when the SSL proxy is enabled from 22.1R1 onwards. PR1709386
- SRX4600 doesn't support ae interfaces. PR1711467
- The 'targeted-broadcast' feature will not work on some SRX platforms. PR1711729

- Continuous vmcores observed on the secondary node when committing set system management-instance command. PR1712727
- Continuous vmcores observed on the secondary node when committing the "set system management-instance" command. PR1713759
- The firewall web-authentication feature will not work after enabling Juniper secure connect. PR1714845
- The SSL session drops because of the wrong SNI value. PR1716893
- The flowd process crash is observed when the web proxy packet reinjection fails. PR1719703

### Interfaces and Chassis

- SRX1500: Traffic fail seen on irb interface for network control forwarding class when verifying dscp classification based on single and multiple code-points. PR1611623
- Incompatible/unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. PR1692404

### Intrusion Detection and Prevention (IDP)

- Network outage caused during change in IDP policy. PR1705491

### J-Web

- [Jweb] "address-book address-book name attach zone" is unexpectedly removed when address-book entry is added or removed by Jweb. PR1712454

### Layer 2 Ethernet Services

- DHCPv6 client options missing in solicit messages if TLV's (Type Length value) exceed a certain length. PR1702831

### Network Address Translation (NAT)

- MNHA: Incorrectly a warning is thrown at commit check for Source NAT config when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0. PR1699407
- ICMP based traceroute is not showing any hops after SRX when SRX is configured with NAT64. PR1706541

### Network Management and Monitoring

- source-address on syslog at custom routing-instance not applied right after rebooting. PR1689661

### Platform and Infrastructure

- "%DAEMON-4: Set system alarm failed: Operation not supported by device" message is seen on high end SRX. PR1681701
- Fabric monitoring suspension and control link failure may cause HA cluster outage. PR1698797
- vmcores can be seen on SRX5k platforms when the fxp0 interface is configured under management-instance. PR1714002

### Routing Policy and Firewall Filters

- Packet drops are seen for SRX destined traffic with self-traffic-policy. PR1698021
- Security policies go out of sync during ISSU. PR1698508

### Routing Protocols

- The traffic drops are seen for the static route after VRRP failover when VRRP VIP is set as next-hop for that static route. PR1687884

### VPNs

- 19.2TH:VPN:SRX5600: While verifying "show security ipsec next-hop-tunnels" output in device the IPsec SA and NHTB entry is not getting cleared after configuring firewall filter. PR1432925
- Routes flapping when configuration changes are applied to custom routing instance. PR1654516
- The kmd crash is seen if the external-interface is empty in the IKE gateway configuration. PR1664910
- VPN traffic loss is seen after HA node reboot while using traffic selectors. PR1667223
- With Active-Active Multi SRGs, the address pools used by SRGs in the access profile must not overlap. PR1687654
- 22.4R1:SRX_RIAD:srx5600:MN_HA:ike cookies didn't change in rekey lifetime expire cases after manual failover. PR1690921
- IPSEC tunnel is not getting established back after the execution of 'clear security ike sa'. PR1694604

- IPsec VPNs will disconnect after ISSU. PR1696102
- Mismatch in configured and negotiated proxy-identity parameters can lead to KMD core. PR1699691
- From 20.4 onwards,St0.16000 to st0.16385 will not be allowed to be configured in HA and MNHA. mode PR1704670
- The iked process will crash when VPN tunnels parameters are not matching. PR1716092

## Migration, Upgrade, and Downgrade Instructions

**IN THIS SECTION**



This section contains the upgrade and downgrade support policy for Junos OS for SRX Series devices. 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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**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) | 36 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 vMX

IN THIS SECTION

## What's New

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

## What's Changed

IN THIS SECTION



Learn about what changed in this release for vMX.

## Network Management and Monitoring

- **`operator` login class is restricted from viewing NETCONF trace files that are `no-world-readable` (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

## Known Limitations

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

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 vMX.

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 input fifo errors drops reported under pfe shell show ifd but not seen in show interface extensive output. PR1642426

## Resolved Issues

IN THIS SECTION



Learn about the issues fixed in this release for vMX.

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

## General Routing

- VMX :: JDI-REG:Virtual:MVPN tunnel is not synced to back up router. MPVN tunnel interface is missed in show multicast route inet instance BLACK group 225.1.1.1 source-prefix 1.1.1.1 output. PR1710323

## Upgrade Instructions

You cannot upgrade Junos OS for the vMX router from earlier releases using the `request system software add` command.

You must deploy a new vMX instance using the downloaded software package.

Remember to prepare for upgrades with new license keys and/or deploying Agile License Manager.

# Junos OS Release Notes for vRR

IN THIS SECTION



## What's New

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

## What's Changed

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

## Known Limitations

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

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

To learn more about common BGP or routing known limitations in Junos OS 22.4R1, see "Known Limitations" on page 45 for MX Series routers.

## Open Issues

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

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 vRR.

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

### General Routing

- VRR should not advertise entropy-label-capability since it is a non-forwarding device. PR1695530
- The rpd crash is observed when rib-sharding configured. PR1699557
- AIGP not distinguished with BGP-LU when rib-sharding is enabled. PR1710829

# Junos OS Release Notes for vSRX

IN THIS SECTION



## What's New

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

## What's Changed

Learn about what changed in this release for vSRX.

### Network Management and Monitoring

- **Operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the `operator` login class do not have permissions to view the trace file.

### VPNs

- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls:

- ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.
- When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.
- In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
- In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.

## 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.

### Chassis Clustering

- Currently max BFD detection interval tested by RLI is 16s. If the detection interval is too large, no BFD down event will be posted by BFDD daemon to jsrpd and jsrpd cannot be aware that ICL once goes down since BFD is the single source of MNHA ICL link failure detection. We don't have other (or plan to add other) ways to detect ICL link going down as it introduces extra complexity. So currently this is a product-limitation.PR1671622

### VPNs

- In case of IKEv2, if the IKE and IPsec SA setup fails in the IKE-SA-AUTH exchange at the initiator end(due to authentication failure), it will lead to a situation where in the responder would have already brought up the IKE and IPsec SA and there would be no delete notification sent from initiator to the responder. To avoid such a scenario, it is recommended to enable dead-peer-detection (DPD)

on the responder end which will ensure that the IKE and IPsec SAs gets deleted on the responder. PR1680885

## Open Issues

IN THIS SECTION



Learn about open issues in this release for vSRX.

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

## General Routing

- With ssl-proxy configured along with web-proxy, the client session might not get closed on the device until session timeout, even though the proxy session ends gracefully.PR1580526
- Device does not drop session with server certificate chain more than 6.PR1663062
- When APBR profile is configured as a policy (and not attached to a security zone) and a failover occurs in between a long-lived ALG(FTP-DATA) session, then the APBR info won't be populated in the AppTrack session close log from the backup node. This issue will be seen only when the (FTP) control session and the ALG(FTP-DATA) session are not "Active" on the same node.PR1688021
- FIPS mode is not supported in this release for SRXSME devices.PR1697999
- On SRX platforms, log streaming to the security director cloud fails on TLS(Transport Layer Security) when DNS(Domain Name System) re-query is performed.PR1708116

## VPNs

- When using Group VPN, in certain cases, the PUSH ACK message from the group member to the group key server may be lost. The group member can still send rekey requests for the TEK SAs before the hard lifetime expiry. Only if the key server sends any new PUSH messages to the group members, those updates would not be received by the group member since the key server would have removed the member from registered members list. PR1608290

## 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.

### Application Layer Gateways (ALGs)

- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed. PR1688986

### Flow-Based and Packet-Based Processing

- APBR:MNHA: When PMI mode is enabled, Uplink-incoming-interface-name not updated properly though link switch is successful by APBR as well as symmetric routing maintained. PR1692062
- High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD. PR1692559
- TCP session timeout seen on GRE tunnel. PR1708646

### General Routing

- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. PR1657704
- EX/QFX SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. PR1683753
- GeoIP cloud feed update is failing. PR1698589
- VLAN tagging does not work for vSRX3.0 on HyperV Windows Server 2019 Datacenter. PR1711440

- The flowd process crash is observed when the web proxy packet reinjection fails. PR1719703

### Network Address Translation (NAT)

- MNHA: Incorrectly a warning is thrown at commit check for Source NAT config when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0. PR1699407

### Services Applications

- Flowd core is seen when type 5 EVPN is configured. PR1704061

## 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 22.4R1 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 22.4R1 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
        20.4K 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 22.4R1 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-x86-64-20.4-2020-10-12.0_RELEASE_20.4_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-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 20.4 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-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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-20.4-2020-10-12.0_RELEASE_20.4_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 22.4R1 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 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_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: 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
```

```
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_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 thirty six months after the first general availability date and customer support for an additional six more 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 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.

**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) | 36 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.

# 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/
- Create a service request online: https://myjuniper.juniper.net/

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

# Creating a Service Request with JTAC

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

- Visit https://myjuniper.juniper.net/
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

# Revision History

12 June 2023—Revision 4, Junos OS Release 22.4R2.

1 June 2023—Revision 3, Junos OS Release 22.4R2.

4 May 2023—Revision 2, Junos OS Release 22.4R2.

20 April 2023—Revision 1, Junos OS Release 22.4R2.