

# Release Notes

Published  
2023-08-09

## Junos® OS Release 22.1R2

---

### 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 22.1R2 for the ACX Series, cSRX Container Firewall (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, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

# Table of Contents

## Junos OS Release Notes for ACX Series

What's New | 1

What's Changed | 1

Known Limitations | 3

Open Issues | 3

Resolved Issues | 5

Migration, Upgrade, and Downgrade Instructions | 7

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 8

## Junos OS Release Notes for cSRX

What's New | 9

What's Changed | 9

Known Limitations | 9

Open Issues | 10

Resolved Issues | 10

## Junos OS Release Notes for EX Series

What's New | 11

What's Changed | 11

Known Limitations | 11

Open Issues | 12

Resolved Issues | 14

Documentation Updates | 16

Migration, Upgrade, and Downgrade Instructions | 16

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 16

#### Junos OS Release Notes for JRR Series

What's New | 18

What's Changed | 18

Known Limitations | 18

Open Issues | 18

Resolved Issues | 19

Migration, Upgrade, and Downgrade Instructions | 19

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 19

#### Junos OS Release Notes for Juniper Secure Connect

What's New | 21

What's Changed | 21

Known Limitations | 21

Open Issues | 21

Resolved Issues | 21

#### Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 22

What's Changed | 22

Known Limitations | 23

Open Issues | 23

Resolved Issues | 23

Migration, Upgrade, and Downgrade Instructions | 23

#### Junos OS Release Notes for Junos Fusion Provider Edge

What's New | 30

What's Changed | 30

Known Limitations | 30

Open Issues | 30

Resolved Issues | 31

Migration, Upgrade, and Downgrade Instructions | 31

#### Junos OS Release Notes for MX Series

What's New | 41

What's Changed | 42

Known Limitations | 43

Open Issues | 45

Resolved Issues | 57

Migration, Upgrade, and Downgrade Instructions | 80

#### Junos OS Release Notes for NFX Series

What's New | 86

What's Changed | 86

Known Limitations | 86

Open Issues | 87

Resolved Issues | 88

| Resolved Issues: 22.1R2 | 88

Migration, Upgrade, and Downgrade Instructions | 89

#### Junos OS Release Notes for PTX Series

What's New | 92

What's Changed | 92

Known Limitations | 93

Open Issues | 93

[Resolved Issues | 95](#)

[Migration, Upgrade, and Downgrade Instructions | 97](#)

#### **Junos OS Release Notes for QFX Series**

[What's New | 102](#)

[What's Changed | 103](#)

[Known Limitations | 104](#)

[Open Issues | 105](#)

[Resolved Issues | 110](#)

[Migration, Upgrade, and Downgrade Instructions | 114](#)

#### **Junos OS Release Notes for SRX Series**

[What's New | 116](#)

[What's Changed | 116](#)

[Known Limitations | 117](#)

[Open Issues | 118](#)

[Resolved Issues | 120](#)

[Migration, Upgrade, and Downgrade Instructions | 123](#)

[Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 124](#)

#### **Junos OS Release Notes for vMX**

[What's New | 126](#)

[What's Changed | 126](#)

[Known Limitations | 126](#)

[Open Issues | 126](#)

[Resolved Issues | 127](#)

[Upgrade Instructions | 127](#)

#### **Junos OS Release Notes for vRR**

**What's New | 128**

**What's Changed | 128**

**Known Limitations | 128**

**Open Issues | 129**

**Resolved Issues | 129**

## **Junos OS Release Notes for vSRX**

**What's New | 130**

**What's Changed | 130**

**Known Limitations | 131**

**Open Issues | 132**

**Resolved Issues | 133**

**Migration, Upgrade, and Downgrade Instructions | 135**

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 141

**Licensing | 142**

**Finding More Information | 143**

**Requesting Technical Support | 144**

**Revision History | 145**

# Junos OS Release Notes for ACX Series

## IN THIS SECTION

- What's New | 1
- What's Changed | 1
- Known Limitations | 3
- Open Issues | 3
- Resolved Issues | 5
- Migration, Upgrade, and Downgrade Instructions | 7

These release notes accompany Junos OS Release 22.1R2 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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

- Junos OS API and Scripting | 2
- Network Management and Monitoring | 2
- Routing Protocols | 3

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

## Junos OS API and Scripting

- **The `<request-system-zeroize>` RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the `<request-system-zeroize>` RPC successfully initiates the zeroize operation, the device emits the `<system-zeroize-status>zeroizing re0</system-zeroize-status>` response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the `<system-zeroize-status>` response tag.

## Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

[See [Understanding the NETCONF Perl Client and Sample Scripts.](#)]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
  - You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See [Enable and Configure Instances of the Ephemeral Configuration Database.](#)]

## Routing Protocols

- To achieve consistency among resource paths, the resource path `/mpls/signalling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter ip-addr='address'/state/countersname='name'/out-pkts/` is changed to `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter ip-addr='address'/state/countersname='name'/`. The leaf `out-pkts` is removed from the end of the path, and `signalling` is changed to `signaling` (with one "l").

## Known Limitations

### IN THIS SECTION

- [Infrastructure](#) | 3

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

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

## Infrastructure

- When upgrading from Junos OS 21.2 release and earlier to Junos OS 21.2 release and later, the validation and upgrade fails. You must use `no-validate` command to upgrade. [PR1568757](#)

## Open Issues

### IN THIS SECTION

- [General Routing](#) | 4

Learn about open issues in Junos OS Release 22.1R2 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

- Due to BRCM KBP issue, route lookup might fail. [PR1533513](#)
- On ACX platforms, traffic issue might occur with downstream devices when you configure the Precision Time Protocol (PTP) (G.8275.1 PTP profile) along with PHY timestamping and Multiprotocol Label Switching (MPLS) terminated on 10G interface. The transit PTP IPv4 packets gets updated with an incorrect Correction Factor(CF). Disable the PHY stamping to fix the issue but disabling might impact the PTP performance. [PR1612429](#)
- On ACX5448 devices with VM Host-based platforms, starting with Junos OS 21.4R1 release or later, ssh and root login are required during installation to copy the line card image from Junos VM to Linux host during installation. Use the `deny-password` command instead of the `deny` command as the default root-login option under the ssh configuration to allow internal trusted communication. [PR1629943](#)
- ACX5448 devices running any prior version of Junos OS release 22.2 does not support the Hierarchical-scheduler (HQOS) on MPLS (Core facing) interface . Enabling HQOS on MPLS Core facing interface causes unexpected traffic forwarding behavior. [PR1630086](#)
- ACX5048 and ACX5096 devices does not support interface speed 10m on 1G interface. [PR1633226](#)
- On ACX5448 and ACX710 devices, all types of delegated BFD sessions configured on routing-instance other than the default routing-instance might not come up.[PR1633395](#)
- Convergence time might be more than 60 seconds for the IS-IS TILFA Node protection testing. [PR1634033](#)
- On ACX5000 devices, in VPLS MH cases, the standby UNI ifl in the backup router gets programmed in the `Disable` state by adding the UNI interface to invalid the VPN ID in hardware. During switch over, the UNI ifl gets deleted and added under the VPLS instance VPN ID. In issue case, UNI interface added under the invalid VPN ID in the backup router tries to get deleted by passing the VPLS instance VPN ID, causing the issue. [PR1665178](#)
- On all Junos platforms, incorrect sensor base telemetry data gets collected when you configure multiple SR-TE tunnels with at least one uncolored, sharing the same single hop segment list.[PR1665943](#)

- On ACX710 and ACX5448 devices, when you configure the inline Bidirectional Forwarding Detection (BFD) session, the Packet Forwarding Engine (PFE) might crash and impact the service. [PR1667129](#)
- VMX crashes as result of riot out of memory condition, reporting Interrupted thread 30 TTP transmit. The memory leaks when checking the RSI for pool-0 values. [PR1669261](#)

## Resolved Issues

### IN THIS SECTION

- [General Routing | 5](#)
- [Network Management and Monitoring | 7](#)
- [Platform and Infrastructure | 7](#)
- [Routing Protocols | 7](#)

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

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

## General Routing

- The cfmd process might generate core files in the logs if you configure the CCM configuration from the aggregated Ethernet interface IFL to the physical IFL in a single commit. [PR1612212](#)
- Multicast traffic drop might be seen if you enable the IGMP snooping for VLAN. [PR1628600](#)
- Late drops are not at par with PN configured. [PR1630724](#)
- On ACX710 and ACX5448 devices, a PE device stops forwarding Layer 3 VPN traffic after core-facing link flaps. [PR1635801](#)
- The ARP request packets might be sent out from ACX device without the VLAN header. [PR1638421](#)
- KRT queue entries gets stuck during the Routing Engine switchover when the backup RPD is not ready. [PR1641297](#)

- On ACX5448 devices, high priority packets might be dropped. [PR1642187](#)
- On ACX5448 devices, attributes gets displayed as Unknown\_Attribute while verifying smartd parameters. [PR1643542](#)
- On ACX5448 devices, reboot reason is not as expected. [PR1643781](#)
- The copper ports on ACX5448 devices might go down if loaded with copper SFP. [PR1643989](#)
- Traffic might silently get discarded in the MPLS scenario with explicit-null. [PR1646097](#)
- The swap-pus or pop-swap VLAN map operations on VPLS IFL might not work. [PR1648182](#)
- While sending BGP notification messages for RFC 8538 HARD RESET, the data portion sometimes is not present. [PR1648479](#)
- If a firewall has a log action and it gets applied on the physical interface or lo0, the LDP cannot go up. [PR1648968](#)
- The BGP Sensor /bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/ are not available as a periodic sensor. [PR1649529](#)
- Due to the MAC learning limit being exceeded traffic drop might be observed in the MC-AE scenario. [PR1653926](#)
- The LDP sessions might flap in the VPLS scenario resulting in Packet Forwarding Engine errors. [PR1654172](#)
- The I2circuit backup might not get reverted to primary in rare condition. [PR1661802](#)
- On ACX5448 and ACX710 devices, the transit traffic drops for BGP-LU (Border Gateway Protocol-Labeled Unicast) prefix when the BGP-LU label routes has ECMP (Equal-Cost Multipath) forwarding path. [PR1663563](#)
- On ACX710 devices, the following log related to resources gets reported after you deactivate or activate EVPN RI multiple times : ACX\_BD\_ERR: dnx\_bd\_alloc\_l2\_svlan: System reached L3 IFL and BD limit(12286) [PR1670683](#)
- RIB and PFEs gets out of synchronization due to a memory leak caused by interface flaps or route churn. [PR1642172](#)
- Traffic might drop on the interfaces using copper SFP after reboot. [PR1645396](#)
- HTTP(S) file download becomes nonresponsive over EVPN-ETREE. [PR1653531](#)
- Shutting the CE interface and bringing back up causes traffic (going towards the core) to drop. [PR1667724](#)

- LLDP neighborship might fail if the chassis-id format of the LLDP packet is xx:xx:xx:88:8e:xx. [PR1669677](#)

## Network Management and Monitoring

- The snmpd process might generate core files with the filter-duplicates configuration. [PR1669510](#)

## Platform and Infrastructure

- The vmxt\_Inx process generates core files at topo\_get\_link jnh\_features\_get\_jnh jnh\_stream\_attach. [PR1638166](#)

## Routing Protocols

- IPv6 Inline BFD sessions goes down when neighbor does not get resolved. [PR1650677](#)
- Routing Process Daemon (rpd) crashes and restarts when a specific timing condition is hit with BGP configuration. [PR1659441](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 8](#)

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 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 | 9
- What's Changed | 9
- Known Limitations | 9
- Open Issues | 10
- Resolved Issues | 10

These release notes accompany Junos OS Release 22.1R2 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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 | 11](#)
- [What's Changed | 11](#)
- [Known Limitations | 11](#)
- [Open Issues | 12](#)
- [Resolved Issues | 14](#)
- [Documentation Updates | 16](#)
- [Migration, Upgrade, and Downgrade Instructions | 16](#)

These release notes accompany Junos OS Release 22.1R2 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

There are no changes in behavior and syntax in this release for EX Series Switches

## Known Limitations

### IN THIS SECTION

- [Platform and Infrastructure | 11](#)

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.

## Platform and Infrastructure

- In EVPN\_VXLAN deployment, BUM traffic replication over VTEP might send out more packets than expected. [PR1570689](#)
- On EX4600 and QFX5xx0 platforms, configure only one static arp with multicast-mac entry per IRB interface. If you configure more than one static arp with multicast Mac entry per IRB interface, then the packets with different destination IP having static multicast mac will always go out with any one of the multicast mac configured in the system. [PR1621901](#)
- On EX4300-MP platforms, when the you run the command `request system software rollback`, device might go down and dcpfe might generate core files.[PR1631640](#)
- Unified ISSU on QFX5120-48Y and EX4650 switches will not be supported if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in

the Cancun firmware leads to the chip reset and hence ISSU is impacted. The Cancun versions in the chipset SDKs should be the same between two JUNOS OS releases for ISSU to work. [PR1634695](#)

## Open Issues

### IN THIS SECTION

- [Forwarding and Sampling | 12](#)
- [Infrastructure | 12](#)
- [Layer 2 Features | 13](#)
- [Network Management and Monitoring | 13](#)
- [Platform and Infrastructure | 13](#)

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.

## Forwarding and Sampling

- When the fast-lookup-filter statement is configured with a match that is not supported in the FLT hardware, traffic might be lost. [PR1573350](#)

## Infrastructure

- USB AUX console is not working on EX4100 box. [PR1616315](#)
- Kernel might crash when the system is in the process of coming up after reboot (and observed only with multiple iterations of continuous reboot cycles). This is observed only during init sequence of mgmt driver and the impact is limited to increased system boot time. [PR1642287](#)

## Layer 2 Features

- When EX Series (applicable platforms: EX2200, EX3300, EX4200, EX4500, EX4550, EX6200, EX8200, and XRE200) is configured with STP and NSB (non-stop bridging), the interface flapping (link up/down events) might cause eswd memory leak. [PR1287184](#)

## Network Management and Monitoring

- A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are performed. [PR1602536](#)

## Platform and Infrastructure

- When the DHCP relay mode is configured as `no-snoop`, the offer might get dropped due to incorrect ASIC programming. This issue occurs only while running DHCP relay in an EVPN/VXLAN environment. [PR1530160](#)
- EX4400-48MP - VM generates core files and Virtual Chassis split might be observed with multicast scale scenario. [PR1614145](#)
- Firewall: End to End Traffic Validation Fails before applying filter on interface. [PR1634347](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- When running the `show pfe filter hw filter-name <filter name>` command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- During Routing Engine switchover, interface flap might be seen along with Scheduler slippage. [PR1541772](#)
- Pause frames counters are not getting incremented when pause frames are sent. [PR1580560](#)
- On EX4400 family of devices, sometimes login prompt is not shown after the login session ends. [PR1582754](#)
- After NSSU upgrade OSPF and OSPF3 adjacencies are flapped and stream outage is higher than the expected value. [PR1590434](#)

- Due to an Improper Initialization vulnerability in Juniper Networks Junos OS on EX4650 devices, packets received on the management interface (em0) but not destined to the device, might be improperly forwarded to an egress interface, instead of being discarded. Refer to <https://kb.juniper.net/JSA69494> for more information. [PR1628754](#)
- Interface might go flapping occasionally on EX4500 or EX4550 with SFP-T module without connecting a cable. [PR1659762](#)
- On Junos EX/NFX/QFX platforms, stale MAC addresses entry is not getting removed for RTG (Redundant trunk groups) interfaces. [PR1664955](#)

## Resolved Issues

### IN THIS SECTION

- [Interfaces and Chassis | 14](#)
- [Layer 2 Ethernet Services | 14](#)
- [Platform and Infrastructure | 15](#)

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.

## Interfaces and Chassis

- The vrrpd core might be observed after interface state change. [PR1646480](#)

## Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when forward-only is reconfigured under the routing instance. [PR1651768](#)

## Platform and Infrastructure

- Traffic is dropped after chassis-control restart when filter is attached and source and destination knob is enabled. [PR1615548](#)
- Traffic loss might be seen when the interface fails to verify the parameter "LOCAL-FAULT". [PR1623215](#)
- GARP reply doesn't update ARP entry though gratuitous-arp-reply option is configured. [PR1644616](#)
- Fabric Board reset with an error message might be observed on certain Junos platforms. [PR1648850](#)
- The dc-pfe might crash due to the VCCP flap. [PR1655530](#)
- EX4300 request system software add ftp fails with the message The /var/tmp filesystem on JUNOS is low on free disk space [PR1659460](#)
- The EX2300 might unexpectedly drop VOIP VLAN traffic after reboot. [PR1633883](#)
- The fxpc process crash might be triggered when a MAC is aging out. [PR1634433](#)
- DHCP snooping table might fail on all Junos platforms to populate MAC address after a VLAN change. [PR1637380](#)
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams. [PR1604283](#)
- The VMcore might be observed on EX platforms in rare scenario. [PR1641988](#)
- Traffic impact might be seen if you enable persistent-learning on an interface. [PR1643258](#)
- Traffic loop might occur due to STP ports not created in new master Routing Engine after switchover due to reboot of master Routing Engine on EX4300, EX3400, and EX2300 platforms in Virtual Chassis (VC). scenario [PR1647000](#)
- The Virtual Chassis port might not be formed automatically after Zeroize. [PR1649338](#)
- L2PT configuration on a transit switch in a Q-in-Q environment breaks L2PT. [PR1650416](#)
- L2PT might not work for AE interfaces in Q-in-Q environment. [PR1653260](#)
- Port mirroring traffic not being flooded on the expected interfaces. [PR1654812](#)
- EX4300-48MP does not generate ICMPv6 too big messages. [PR1655654](#)
- All Slaac-snooping entries learnt on an IFL are deleted when an IFBD is deleted such that IFL is member of more than 1 VLANs. [PR1655913](#)

- port/mac gbp tags might not be carried forward to the spine. [PR1659384](#)
- The fxc crash might be observed with rpf check enabled. [PR1662508](#)
- EX4300-48MP: Virtual Chassis: NSSU aborted with Backup Routing Engine might be in inconsistent state. [PR1665562](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release documentation for the EX Series documentation.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 16](#)

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 | 18](#)
- [What's Changed | 18](#)
- [Known Limitations | 18](#)

- Open Issues | 18
- Resolved Issues | 19
- Migration, Upgrade, and Downgrade Instructions | 19

These release notes accompany Junos OS Release 22.1R2 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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 Junos OS Release 22.1R2 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 and software in Junos OS Release 22.1R2 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 Junos OS Release 22.1R2 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

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 19](#)

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 | 21](#)
- [What's Changed | 21](#)
- [Known Limitations | 21](#)
- [Open Issues | 21](#)
- [Resolved Issues | 21](#)

These release notes accompany Junos OS Release 22.1R2 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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 | 22](#)
- [What's Changed | 22](#)
- [Known Limitations | 23](#)
- [Open Issues | 23](#)
- [Resolved Issues | 23](#)
- [Migration, Upgrade, and Downgrade Instructions | 23](#)

These release notes accompany Junos OS Release 22.1R2 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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 open issues in hardware and 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

There are no resolved issues in the Junos OS main and maintenance releases for Junos Fusion Enterprise.

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

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device](#) | 24
- [Upgrading an Aggregation Device with Redundant Routing Engines](#) | 26
- [Preparing the Switch for Satellite Device Conversion](#) | 26
- [Converting a Satellite Device to a Standalone Switch](#) | 28
- [Upgrade and Downgrade Support Policy for Junos OS Releases](#) | 28
- [Downgrading Junos OS](#) | 29

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

Table 4: EOL and EEOL Releases (*Continued*)

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/Downgrade to subsequent 3 releases	Upgrade/Downgrade to subsequent 2 EEOL releases
Extended End of Life (EEOL)	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 Provider Edge

## IN THIS SECTION

- [What's New | 30](#)
- [What's Changed | 30](#)

- [Known Limitations | 30](#)
- [Open Issues | 30](#)
- [Resolved Issues | 31](#)
- [Migration, Upgrade, and Downgrade Instructions | 31](#)

These release notes accompany Junos OS Release 22.1R2 for Junos Fusion provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

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

## Known Limitations

There are no known limitations in hardware or software in this release for Junos Fusion 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

There are no known issues in hardware and software in this release for Junos Fusion Provider Edge.

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

- [Junos Fusion Provider Edge | 31](#)

Learn about the issues fixed in this release for Junos Fusion 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

- [Configuring port mirroring firewall filter in a bridge domain with IRB might cause traffic loss over IRB. PR1607750](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 32](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 35](#)
- [Preparing the Switch for Satellite Device Conversion | 35](#)
- [Converting a Satellite Device to a Standalone Device | 37](#)
- [Upgrading an Aggregation Device | 39](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 39](#)

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 22.1R2 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/jinstall64-22.1R2.SPIN-  
domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.1R2.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/jinstall64-22.1R2.SPIN-
export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-22.1R2.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 22.1R2 *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, unplug 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 22.1R2, 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 22.1

To downgrade from Release 22.1 to another supported release, follow the procedure for upgrading, but replace the 22.1R2jinstall 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 | 41](#)
- [What's Changed | 42](#)
- [Known Limitations | 43](#)
- [Open Issues | 45](#)
- [Resolved Issues | 57](#)
- [Migration, Upgrade, and Downgrade Instructions | 80](#)

These release notes accompany Junos OS Release 22.1R2 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

### What's New

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

## What's Changed

### IN THIS SECTION

- [General Routing | 42](#)
- [User Interface and Configuration | 42](#)

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

## General Routing

- OpenConfig container names for Point-to-Multipoint per interface ingress and egress sensors are modified for consistency from "signalling" to "signaling".
- **Router advertisement module status on backup Routing Engine (MX Series)**---The router advertisement module does not function in the backup Routing Engine as the Routing Engine does not send an acknowledgment message after receiving the packets. Starting in this Junos OS Release, you can view the router advertisement module information using the `show ipv6 router-advertisement operational` command.

See [show ipv6 router-advertisement](#)).

## User Interface and Configuration

- When you configure `max-cli-sessions` at the `[edit system]` hierarchy level, it restricts the maximum number of CLI sessions that can coexist at any time. Once the `max-cli-sessions` number is reached, new CLI access is denied. The users who are configured to get the CLI upon login, are also denied new login.

## Known Limitations

### IN THIS SECTION

- [General Routing | 43](#)
- [Infrastructure | 44](#)
- [Network Management and Monitoring | 44](#)
- [Platform and Infrastructure | 44](#)
- [Routing Protocols | 45](#)
- [VPNs | 45](#)

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

- Currently, IP options are not supported for egress firewall attach points, relevant supporting doc attached: <https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/firewall-filter-match-conditions-for-ipv4-traffic.html>. The issue might occur IP-options router alert traffic not hitting the egress firewall filter. [PR1490967](#)
- BUM (Broadcast, Unknown Unicast, and Multicast) traffic replication over VTEP is sending out more packets than expected and there seems to be a loop. [PR1570689](#)
- On all MX Series platforms, changing configuration AMS 1:1 warm-standby to load-balance or deterministic NAT might result in vmcore and cause traffic loss. [PR1597386](#)
- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This typically occurs with the first session hitting such a filter. [PR1597864](#)
- We should configure only one static ARP with multicast-mac entry per IRB interface. If we configure more than one static ARP with multicast MAC entry per IRB interface, then the packets with different destination IP having static multicast MAC will always go out with any one of the multicast MAC configured in the system. [PR1621901](#)

- This is a product limitation for MX-SPC3 with new junos-ike architecture. The issue is seen when we have any-any TS configured and any-any TS negotiated (both in IPv4 and IPv6). As a workaround, do not configure any-any TS when it is sure that negotiated traffic selector for the IPsec tunnel will also be any-any. When there is no TS configured, the scenario might be treated as proxy-id case and bypasses the issue without having any impact on the described scenario. [PR1624381](#)
- Changing the root-authentication password in cpce does not bring down the existing session. The password change will be in effect for all new connections. [PR1630218](#)
- The available space check in case of: 1. Upgrade is 5 GB 2. Fresh Install is 120 GB. The scenario Upgrade/Fresh-Install is decided from within RPM spec that is if RPM finds any older version is already installed. Since RPM-DB is destroyed during LTS-19 (vm-host) upgrade, rpm install scripts deduce the upgrade as fresh-install and look for 120GB free space. The warning can be ignored, as it has no functional impact. [PR1639020](#)
- On MX operating as a SAEGW-U/UPF at high mobile session scale (around 1 Million sessions), show services mobile-edge sessions extensive will not work. Mobiled process will take exception and generates core files. [PR1639595](#)

## Infrastructure

- When you upgrade from Junos OS Release 21.2 to later releases, validation and upgrade will fail. The upgrading requires using of no-validate configuration statement. [PR1568757](#)

## Network Management and Monitoring

- Configuring the set system no-hidden-commands blocks NETCONF sessions. As a workaround, customer can disable the no-hidden-commands. [PR1590350](#)
- When an ephemeral instance is being edited, if show ephemeral-configuration merge command is run from another terminal, then the uncommitted changes in the ephemeral instance being edited will also appear in the output of show ephemeral-configuration merge command. [PR1629013](#)

## Platform and Infrastructure

- Deactivating services rpm/rpm-tracking does not remove the tracked route from the routing or forwarding tables. [PR1597190](#)

- After a switchover event, when pppd calls sendmsg system call to transmit the protocol packets, it gets blocked long enough that a few sendmsg calls cumulatively take up around 7 seconds to 8 seconds. This indirectly impacts the BFD session because the BFD session has a Routing Engine-based detect time of 7.5 seconds to expire. [PR1600684](#)

## Routing Protocols

- When we have high scale, the openconfig telemetry sensor /bgp-rib/ used in periodic streaming will cause high CPU usage by RPD. [PR1625396](#)

## VPNs

- In some scenario (for example, configuring firewall filter), routers might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)

## Open Issues

### IN THIS SECTION

- [Class of Service \(CoS\) | 46](#)
- [EVPN | 46](#)
- [Flow-based and Packet-based Processing | 47](#)
- [Forwarding and Sampling | 47](#)
- [Infrastructure | 47](#)
- [Interfaces and Chassis | 47](#)
- [Juniper Extension Toolkit \(JET\) | 48](#)
- [Layer 2 Features | 48](#)
- [MPLS | 48](#)
- [Network Management and Monitoring | 49](#)
- [Platform and Infrastructure | 50](#)
- [Routing Protocols | 56](#)

- Services Applications | 57
- User Interface and Configuration | 57
- VPNs | 57

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)

- Show Class-of-service Interface might not show the Classifier bind info on an IFL with only Inet/ Inet6 (without family mpls or not with any rewrite rules). Show issue, Classifier will be still present and functional. There is no impact to the traffic. [PR1652342](#)
- The AE interfaces in per-unit-scheduler mode and committing CoS configuration on AE IFLs in a single commit leads to race-conditions.[PR1666010](#)

## EVPN

- In PBB-EVPN (Provider Backbone Bridging - Ethernet VPN) environment, ARP suppression feature which is not supported by PBB might be enabled unexpectedly. This could cause MAC addresses of remote CEs not to be learned and hence traffic loss. [PR1529940](#)
- EVPN-MPLS multi-homing control MACs are missing after vlan-id removal and adding back on a trunk IFL of one of the multi-homing PEs. This is not a recommended way to modify vlan-id configuration. Both MH PEs need to be in symmetric always . [PR1596698](#)
- This problem happens only with translation VNI when mac moved one from DC1 to DC2. VM move across DC where there is not translate VNI configuration in the interconnect works as designed. [PR1610432](#)
- EVPN Local ESI Mac limit configuration might not get effective immediately when it has already learned remote MH Macs. Clear the Mac table from all MH PEs and configure the Mac limit over local ESI interfaces. [PR1619299](#)

- This is a case where interface is disabled and comes up as CE after a timeout. A manual intervention of `clear ce interface` command should restore this. As workaround, perform the following steps:
  - Clear `auto-evpn ce-interface interface-name`.
  - Configure `editactivate interface-name family inet inet6`.

[PR1630627](#)

## Flow-based and Packet-based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores \* 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. [PR1470637](#)

## Forwarding and Sampling

- When the `fast-lookup-filter` statement is configured with a match that is not supported in the FLT hardware, traffic might be lost. [PR1573350](#)

## Infrastructure

- The following IPC timeouts logs might be seen for statistics query to kernel (queried from CLI or daemons querying internally) when there is configuration churn, or large number of IPCs getting exchanged between kernel and pfe in the system. `if_pfe_msg_handler: pfe_peer_msg_handler error: error for msg type type, msg subtype subtype, opcode op and peer index index`Default IPC timeout value in kernel for IPC statistics request is 10s. [PR1629930](#)

## Interfaces and Chassis

- The memory usage of the `rpd` process on the backup routing engine might increase indefinitely due to leak in `krt_as_path_t`. [PR1614763](#)

- On EVO platforms during lacpd process restart, child IFD indexes from the port options IFD based data, which gets stored in kernel by lacpd, might not get reused due to old indexes not being freed. When this occurs, new indexes might be generated repeatedly, which might cause the port numbers exhaustion problem in Aggregated Ethernet (ae) interface bundle. [PR1647145](#)
- The transportd.core core file is seen with fabric configuration. [PR1649019](#)
- Due to the issue, there is an error log printed and DCD is restarted. But there is no functionality impact for BFD sessions. There may be a slight delay in the new configuration to take effect as DCD is restarted.

[PR1658016](#)

## Juniper Extension Toolkit (JET)

- In Junos OS Evolved, there are two different gRPC Python files for each JAPI file. The names of the files are \*pb2\_grpc.py and \*pb2.py. The stub creation functions are present in \*pb2\_grpc.py. [PR1580789](#)
- Until Junos OS Release 21.3 release mgd is 32-bit binary on EVO. libsi can only be linked with 64-bit binaries. To access data/WAN ports in EVO we need libsi to be linked with the binary. By default the shell on the EVO device includes libsi, but it's not available to CLI commands as CLI will make mgd invoke cscript to run a Python script via CLI. [PR1603437](#)

## 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](#)

## MPLS

- BFD session flaps during unified ISSU only in mpc7e card (BFD sessions from other cards of DUT to peer routers did not flap during ISSU). The issue is not seen frequently. [PR1453705](#)
- Single hop BFD sessions might sometimes flap after GRES in highly scaled setups which have RSVP link or link-node-protection bypass enabled. This happens because sometimes RSVP neighbor goes down after GRES if RSVP hellos are not received after GRES before neighbor timeout happens. As a

result of RSVP neighbor going down, RSVP installs a /32 route pointing to bypass tunnel which is required to signal backup LSPs. This route is removed when all LSPs stop using bypass after link comes back up. The presence of this /32 route causes BFD to flap. [PR1541814](#)

- In MVPN case, if the nexthop index of a group is not same between master and backup after a NSR switchover, we might see a packet loss of 250 to 400 ms. [PR1561287](#)
- The use-for-shortcut statement is meant to be used only in SR-TE tunnels which use SSPF (Strict SPF Algo 1) prefix SIDs. If set protocols isis traffic-engineering family inet-mpls shortcuts and set protocols isis traffic-engineering tunnel-source-protocol spring-te are configured on a device, and if any SR-TE tunnel using Algo 0 prefix SIDs is configured with use-for-shortcut statement, it could lead to routing loops or rpd core files. [PR1578994](#)
- When there is scaled RSVP sessions [~21K] and have enabled RSVP for all the interfaces, RPD process walks through all the interfaces, which results in high CPU usage for some time, which also results in LSP flap. [PR1595853](#)
- With the chained-composite statement enabled, the following statement does not have any effect if ingress and egress ports are on the same Packet Forwarding Engine instance on the line card (FPC). For example, the outer label TTL would not be set as 255. Instead, it would be set as (ip TTL-1). PS: This issue is not seen if ingress and egress ports are on different FPC slots or on difference Packet Forwarding Engine instances of the same FPC. set protocols mpls label-switched-path <lsp-name> no-decrement-ttl, chained-compositestatement, and set routing-options forwarding-table chained-composite-next-hop ingress l3vpn [PR1621943](#)
- Ingress will retry after lsp stay down for extended period of time, or customer can clear lsp to speed up the retry. [PR1631774](#)

## 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](#)
- A minor memory leak is seen in the event-daemon process when multiple GRES switchovers are performed. [PR1602536](#)
- mgd might crash when an invalid value is configured for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem happens with json and xml loads. [PR1615773](#)

- On all Junos and EVO platforms, the "snmpd" process might crash, if there is no response for the SNMP requests, and a timeout happens. [PR1666548](#)

## Platform and Infrastructure

- If a vmhost snapshot is taken on an alternate disk and there is no further vmhost software image upgrade, the expectation is that if the current vmhost image gets corrupted, the system boots with the alternate disk so the user can recover the primary disk to restore the state. However, the host root file system and the node boots with the previous vmhost software instead of the alternate disk. [PR1281554](#)
- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- On MX Series routers with MPC7E, MPC8E, or MPC9E installed, if optics QSFP-4X10GE-LR from Innolight vendor (subset of modules with part number 740-054050) is used, the link might flap. [PR1436275](#)
- With NAT/Stateful-firewall/TCP tickle (enable by default) configured on MS-MPC/MS-MIC, the vmcore crashes sometimes along with mspmand crash might happen if large-scale traffic flows (that is, million flows) are processed by it. [PR1482400](#)
- When there are hardware 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](#)
- When running the command `show pfe filter hw filter-name <filter name>`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- When an AMS ifd is configured for the first time or any member of the AMS bundle is removed or added, the PICs on which the members of AMS bundle are present go for a reboot. There is a timer running in the AMS kernel which is used as a delay for the PIC reboot to complete and once that timer expires AMS assumes that the PICs might have been rebooted and it moves into next step of AMS fsm. In scaled scenarios, this rebooting of the PIC is delayed due to DCD. This is because when a PIC goes down, DCD is supposed to delete the IFDs on that PIC and then the PIC reboot happens. But DCD is busy processing the scaled configuration and the IFD deletion is delayed. This delay is much greater than the timer running in AMS kernel. When the above timer expires, the FSM in AMS kernel incorrectly assumes the PIC reboot would be completed by then, but the reboot is still pending. By the time DCD deletes this IFD the AMS bundles are already UP. Because of this, there is a momentary flap of the bundles. [PR1521929](#)

- In Mac OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually. [PR1525889](#)
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. [PR1533513](#)
- The Flexible PIC Concentrator (FPC) might generate a core file (or dump file) if the flap-trap-monitor feature under set protocols oam ethernet cfm performance-monitoring sla-iterator-profiles is used and performance monitoring flap occurs. [PR1536417](#)
- In scaled MX2020 router, with vrf localisation enabled, 4 million nexthop scale, 800k route scale. FPCs might go offline on GRES. Post GRES, router continues to report many fabric related CM\_ALARMS. FPC might continue to reboot and not come online. Rebooting master and backup Routing Engine will help recover and get router back into stable state. [PR1539305](#)
- During Routing Engine switchover interface flap might be seen along with Scheduler slippage. [PR1541772](#)
- Unsupported configuration is being attempted by the script that then hits the maximum threshold for the given platform. [PR1555159](#)
- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interop works as expected. Also it is to be noted QFX10002-60C and ACX or Traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both QFX10002-60C and MX2010, which needs to be debugged with the help from HW and SI teams and resolved. [PR1555955](#)
- The SyncE to PTP transient response is a stringent mask to be met with two way time error. The SyncE to PTP transient response mask might not be met for MPC7E-1G and MPC7E-10G line cards. [PR1557999](#)
- VE and CE mesh groups are default mesh groups created for a given routing instance. On adding VLAN or bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group and flood-group. Ideally, VE mesh-group does not require a CE router where IGMP is enabled on CE interfaces. MX Series based CE boxes have unlimited capacity of tokens. So, this would not be a major issue. [PR1560588](#)
- Support switchover on routing-crash configuration statement during abnormal termination of rpd. [PR1561059](#)
- The session status becomes nonresponsive in the invalid state after the core-facing link fails in the primary PE devices. [PR1562387](#)
- Configure an interface hold time to avoid the additional interface flap. [PR1562857](#)
- On MX480 routers, traffic loss is observed with a scale of 4000 tunnels 800 VRF test. The problem is with Layer 1 node not reflecting correct bandwidth configured for tunnel services. When baseline

has 1G configuration on some FPC or PIC in groups global chassis and if we override with local chassis tunnel service in 10G bandwidth scaled scenario. Out of 10 Gbps bandwidth configured only 1 Gbps is allowed per 1G speed configured in baseline configuration. [PR1568414](#)

- When inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. [PR1569229](#)
- The following messages might be seen in the logs from MPC11E line-card: router-re0-fpc8 afd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9. There is no functional impact, these logs can be ignored. [PR1573972](#)
- When you commit the configuration /8 pool with block size as 1, the block creation utilizes more memory causing NAT pool memory shortage. This results in syslog RT\_NAT\_POOL\_MEMORY\_SHORTAGE. [PR1579627](#)
- Firewall programming fails due to scaled prefix configuration with more than 64800 entries. [PR1581767](#)
- When you configure interim logging for PBA, syslog messages are generated in regular intervals. Change in information of PBA interim syslog message, the message string change from "allocates port block" to "interim port block". [PR1582394](#)
- When the active secondary 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 secondary interface. There is no functional impact. [PR1585529](#)
- On all devices running Junos OS Release 19.1R3-S5-J3, when you delete Extensible Subscriber Services Manager (ESSM) the subscriber logical interface might get stuck. [PR1591603](#)
- Currently, SyncE configurations are allowed during unified ISSU but trigger a warning since SyncE state might not be maintained during unified ISSU. PTP configurations, however, need to be deactivated, else the unified ISSU will be aborted. [PR1592234](#)
- Pim VxLAN do not work on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. [PR1597276](#)
- On MX2010 and MX2020 devices, Junos OS does not support unified ISSU for software upgrades from Junos OS 21.2 release to Junos OS 21.3 and 21.4 releases due to a flag day change. [PR1597728](#)
- Rebooting JDM from inside JDM shell changes JDM's main PID as a result systemd's knowledge of JDM PID becomes stale. Due to this reason systemd fails to stop or start JDM. [PR1605060](#)
- Leaf difference w.r.t. memory-usage/heap in the output of Sensor (/junos/system/linecard/firewall) between MPC7E and MPC10E. [PR1606791](#)

- If RPD Agent sends INH deletion/additions out of order(Rarely occurs) to backup RPD, RPD might generate core files. RPD then restarts and works fine. [PR1607553](#)
- IS-IS adjacency remains down in backup Routing Engine during link flap test. [PR1608591](#)
- Dfwd generates core files when accessing ephemeral db files which is deleted through script. [PR1609201](#)
- When user tries to disable AMS ifd using configuration, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. [PR1613432](#)
- Changing aggregated AE mode (aggregated-ether-options link-protection) with subscribers logged in on that AE will cause undesirable subscriber management behavior. You will need to confirm there are no subscribers on the AE before changing the AE protection mode. [PR1614117](#)
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION\_CLOSE Syslog will be seen. [PR1614358](#)
- MAX AE interfaces software index was 128. Hence, a failure is seen when you configure with 218 interfaces. Therefore, we increase the max indexes to 255. [PR1618337](#)
- Memory Zone is not reflecting properly while doing Memory Tests through Vty command test usp service-sets memory-testing start. [PR1619499](#)
- On all MX series platforms with MPC10+, configuring syslog as a filter action might cause the FPC to restart. [PR1627986](#)
- For a topology with VSTP and VRRP configured and IPv6 traffic, if you change VSTP bridge priority a couple of times (to trigger toggling of root bridge), V6 traffic drop might be seen on some of the streams. [PR1629345](#)
- For MX204 and MX2008 "VM Host-based" platforms, starting with Junos OS Release 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use deny-password instead of deny as default root-login option under ssh configuration to allow internal trusted communication. Ref <https://kb.juniper.net/TSB18224> [PR1629943](#)
- On MX platform with enhanced subscriber management enabled, when you configure host-prefix-only on the underlying-interface for subscribers, it might not work in FPC. [PR1631646](#)
- The fabric statistics counters are not displayed in the output of show snmp mib walk ascii jnxFabricMib. [PR1634372](#)
- Ports speed is stuck and never changes for any port profile changes,if pic bounce is done fast not letting the previous configuration complete. [PR1637954](#)
- The USB device on MX304 can be accessed from host linux instead of junos (as is usually done on most other platofrms) MX304 is similar to PTX1000 in this respect. Regular procedure to access usb

in junos on most platforms : <https://kb.juniper.net/InfoCenter/index?page=content=KB12880>  
 Procedure to access usb in host linux (ptx1000, mx304) : <https://www.juniper.net/documentation/us/en/software/junos/junos-install-up-grade/topics/topic-map/storage-media-and-routing-engines.html#id-accessing-usb-storage-on-ptx1000-routers> [PR1639071](#)

- On all Junos and Junos Evolved platforms, there may be a high Control Processing Unit (CPU) utilization for the routing processor daemon (rpd) during commit. This might only be seen in a scaled static route setup with VRF (Virtual Routing and Forwarding) and Bi-Directional Forwarding and Detection (BFD). The reason for the CPU spike is that kernel routing table (krt) might get stuck and keeps running for a long time. The high CPU might hamper the rpd functionality in rare cases, however, the system recovers by itself when you encounter this issue. [PR1639252](#)
- Script fails while verifying Access Internal Routes after daemon restart during Advanced DHCP test. [PR1640567](#)
- 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. The exact issue is yet to be isolated. [PR1641107](#)
- On MPC10E cards upon many very quick link down and up events in msec range might not always able to drain all traffic in the queue. This causes lost of traffic going through the interface. Traffic volume and class-of-service configuration does influence the exposure. See also [PR1638410](#).[PR1642584](#)
- When we use request vmhost zeroize command it doesn't show entry for no-forwarding option under possible completions. [PR1642820](#)
- With PTPoIPv6 on MPC2E 3D EQ, PTP slave stays in acquiring state.[PR1642890](#)
- Committing configuration changes during the Packet Forwarding Engine reset pause window (when PFE is disabled, yet the PFE reset proper has not started yet) has the potential of causing errors and traffic loss. In particular, configuration changes that result in re-allocating policers (which are HMC-based) might lead to traffic being entirely policed out (that is, not flowing). Once the PFE reset procedure has started configuration changes ought to be avoided until the procedure is completely done.[PR1644661](#)
- 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:: #set system subscriber-management mode force-broadband-devic. [PR1645075](#)
- On all MX and PTX platforms, EDAC errors are triggered but alarms are not observed until the FPC gets rebooted due to the data corruption in hardware. [PR1646339](#)
- On all MX platforms with the subscriber management scenario, when unified ISSU happens from pre Junos OS Release 18.4 to post Release 18.4, subscribers that re-logged in pre 18.4 are called preNG

subscribers. For any of the preNG subscribers, if the ipv4/ipv6 family interface goes up/down, the issue is triggered. [PR1646846](#)

- Observed un expected traffic steering during the verification of path computation client. [PR1647073](#)
- The `mobile.core-tarball.0.tgz` core file is seen while testing `hcm_dpi_pcef_usf_3.robot`. [PR1648886](#)
- The firewall filter might be incorrectly updated in the MPC10E Packet Forwarding Engine when a change (for example, add, delete, deactivate, or activate) of firewall filter terms occurs in some scenarios, such as large-scale term changes or changes happening during MPC reboot. The incorrect firewall filter might cause the traffic to silently drop or discard and even lead to an MPC crash. It is a timing issue. [PR1649499](#)
- Extra `frr_inh` is seeing in `show route 174.174.174.174/32 table vpn1.inet.0 protocol bgp extensive fib-expanded-nh exact` output. [PR1651103](#)
- On MX Series devices, 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. [PR1657378](#)
- TOS(DSCP+ECN) bits are not getting copied from the Inner Layer 3 header to Outer VXLAN header at the Ingress VTEP. Because of this in the core, ECN marking and DSCP classification are not working. [PR1658142](#)
- DHCPACK is not received at ztp-server after zeroize of the device (client). [PR1658287](#)
- During startup of a cBNG container or when JSD is restarted from the CLI in a cBNG container, JSD might crash creating a core file. JSD should recover from the crash and automatically restart. JSD should function normally after recovering from the crash. [PR1659175](#)
- MPC checks periodic service time. When heavy interrupts occur during periodic service, the periodic service time might exceed 200 microseconds. If it happens, `0inker: Function message will occur`, but it doesn't have function impact. This is applicable to Junos OS 16.1R4 to 16.1R7 releases. [PR1242915](#)
- On vMX, the blockpointer in the ktree is getting corrupted leading to core-file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. [PR1525594](#)
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. [PR1530160](#)
- If you use the source-address NTP configuration parameter and issue the command `set ntp date` from the CLI, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets. [PR1545022](#)

- In rare occurrence Routing Engine kernel might crash while handling TCP sessions if GRES/NSR are enabled. [PR1546615](#)
- Don't use the control-type light under platforms where this feature is not supported at present. At present IPv4 and IPv6 twamp-light is supported on the platforms using TRIO and PE chipsets. [PR1603128](#)
- VM might generate core files, and you might observe Virtual Chassis split with multicast scale scenario. [PR1614145](#)
- Using static labeled switched path (LSP) configuration, the child node is not removed from the flood composite when the core interface goes down. [PR1631217](#)
- With given multi dimensional scale, if a 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](#)
- Observing traffic loss after Routing Engine switchover while changing the BGP hold-down timers. [PR1650940](#)
- Micro BFD sessions which are running in distributed mode might flap if ppm thread does not get scheduled on time. This issue is applicable to MPC9 and below trio based line cards. [PR1668818](#)

## Routing Protocols

- On all platforms, the issue is when the first time when ISIS is coming up sometimes the ISIS route might not get installed. [PR1559005](#)
- On MX platforms, initial multicast register packets might get dropped, this may affect multicast services. [PR1621358](#)
- Protocols (IS-IS, LDP, BFD) flapped during graceful switchover while testing ldp oam. [PR1638882](#)
- On all Junos and Junos OS Evolved platforms, when configuring the network instance for openconfig, an error might be observed while executing a commit if the configured network instance type is default\_instance but the instance name is not default. [PR1644421](#)
- When Junos device receives BGP inetflow route with multiple nexthops, RPD will crash and generate a core file. [PR1670630](#)

## Services Applications

- L2TP LAC functionality is not working in this release. [PR1642991](#)

## User Interface and Configuration

- On all Junos with persist-groups disabled ( on Junos persist-groups feature is enabled by default Junos OS Release 19.4 onwards) and on EVO platforms where persist groups can be disabled (Junos OS Release 21.4R1 onwards persist-groups cannot be disabled on EVO) this issue can be seen. This issue occurs when grafting happens during configuration expansion (when persist-groups is disabled) and a configuration such as a customer configuration is applied (for example, a configuration in which MTU is inherited from a groups configuration).[PR1636085](#)

## VPNs

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RGO failover. [PR1450393](#)
- 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](#)

## Resolved Issues

### IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 58](#)
- [Class of Service \(CoS\) | 59](#)
- [EVPN | 59](#)
- [Flow-based and Packet-based Processing | 59](#)
- [Forwarding and Sampling | 60](#)

- General Routing | 60
- High Availability (HA) and Resiliency | 71
- Infrastructure | 72
- Interfaces and Chassis | 72
- Junos XML API and Scripting | 73
- Layer 2 Ethernet Services | 73
- MPLS | 74
- Network Management and Monitoring | 75
- Platform and Infrastructure | 75
- Routing Policy and Firewall Filters | 76
- Routing Protocols | 76
- Services Applications | 78
- Subscriber Access Management | 78
- User Interface and Configuration | 79
- VPNs | 79

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)

- On Junos OS MX Series, the flowd daemon will crash if the SIP ALG is enabled and specific SIP messages are processed (CVE-2022-22175). [PR1604123](#)
- On Junos OS, flowd core observed if the SIP ALG is enabled and a specific Session Initiation Protocol (SIP) packet is received (CVE-2022-22178). [PR1615438](#)

## Class of Service (CoS)

- The fabric queues priority might not get changed after activate or deactivate CoS configuration. [PR1613541](#)

## EVPN

- Baseline EVPN-VXLAN transition from IPv4 to IPv6 or vice versa does not work in certain sequence. [PR1552498](#)
- Bridge MAC-table learning entries might not be as expected for the EVPN-MPLS routing instance. [PR1600310](#)
- A few ARP, ND, and MAC entries for VLANs are missing with MAC-VRF configuration. [PR1609322](#)
- Missing MAC address entries in EVPN MAC-table despite the presence of the corresponding Type 2 route. [PR1611618](#)
- Traffic loss for profile TI2-Inter-VN-Traffic\_Stream-SH-MH when testing EVPN with VXLAN. [PR1628586](#)
- The l2ald crash might be seen after performing restart routing on EVPN PE. [PR1629426](#)
- Removing configuration statement `es-label-oldstyle` does not take effect if it is the only configuration statement configured under the protocol EVPN. [PR1629953](#)
- In a scenario where multiple VXLAN type-5 tunnels with the same decap prefix (Vnid+ SrcIP + DestIP) are created within a VRF, and they are not handled on MPC10 and MPC11, it might lead to traffic drop. [PR1630163](#)
- The rpd might crash when moving an interface from VPLS to EVPN-VPWS instance. [PR1632364](#)
- The traffic loss might be seen when the link goes down for the local ESI. [PR1632723](#)
- When `no-arp-suppression` is configured in EVPN-MPLS, traffic forwarding is impacted. [PR1646010](#)

## Flow-based and Packet-based Processing

- Unable to execute `/usr/sbin/picinfo: Bad file descriptor` during `clear services inline-monitoring statistics` command is issued. [PR1624094](#)

## Forwarding and Sampling

- Delay in getting the response for `clear interfaces statistics all` command with scale configuration. [PR1605544](#)
- You can commit even if you do not apply the firewall filter to the FPC. [PR1618231](#)
- The FPC might crash when interface participating in **next-interface** filter action flaps. [PR1622585](#)
- Packet loss might be reported after hitting the firewall filter on Junos OS platform. [PR1625309](#)

## General Routing

- Error message **sensord: Error updating RRD file: /var/run/sensord.rrd** might be seen on WRL9 based line card. [PR1420927](#)
- During flooding, MAC is learnt only on normal access port but not on the aggregated Ethernet interface trunk port. [PR1506403](#)  
  
Junos 'et-' interface gets stuck and remains down between two particular ports. <http://prsearch.juniper.net/PR1535078>
- Junos 'et-' interface stuck and remains down between two particular ports. [PR1535078](#)
- On MX480, issuing the `help apropos` command in configuration mode is going to cause an mgd core. The mgd process will come up and as long as the command is not issued again, the core will not occur. [PR1552191](#)
- Egress IP MTU exception and fragmentation are not supported. [PR1558327](#)
- ARP resolution failure might occur in EVPN-VxLAN scenario. [PR1561934](#)
- The `na-grpcd` process might generate core files during the longevity tests. [PR1565255](#)
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile `set security log profile default-profile` can be used to improve this behavior when multiple log profiles are defined. [PR1570105](#)
- Interfaces might fail to come up on MX240, MX480 and MX960 platforms. [PR1571274](#)
- PKID core might occur during cert signature validation. This core is not very frequent and occurs due to memory corruption. [PR1573892](#)

- The chassisd process might crash on all Junos platforms that support Virtual Chassis or Junos fusion. [PR1574669](#)
- When Hwdre application failed on primary Routing Engine, GRES switchover will not happen. [PR1575246](#)
- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might go offline when the device is running on FIPS mode. [PR1576577](#)
- Unexpected close-timeout gets refreshed for TCP session of CGNAT on MX platforms with MS-MPC line card. [PR1576675](#)
- The subscribers over PS interface are not cleared after FPC offline. [PR1580812](#)
- The line cards might fail after hitting the I2C error on MX FPC. [PR1583060](#)
- The multicast traffic is not traversing across PS interface when it is anchored on RLT interface. [PR1584041](#)
- The show route detail might not show Next-hop type IPoIP Chained comp nh in the output (Display only - no operation impact). [PR1584322](#)
- The show security idp counters does not have tenant statement in the syntax. [PR1586220](#)
- A high rate of small packets could cause CPU hogging and the firmware crash in MPC5E and MPC6E line cards. [PR1587551](#)
- On MX10003 routers, PEM capacity shows incorrectly. [PR1587694](#)
- NAT EIM mapping is getting created even for out to in FTP ALG child sessions. [PR1587849](#)
- Some logical interfaces might go down under logical tunnel due to the limited number of MAC addresses in a pool. [PR1591853](#)
- The DCI InterVNI and IntraVNI traffic might get silently dropped and discarded in gateway node due to the tagged underlay interfaces. [PR1596462](#)
- Inconsistency in the platform name used in multiple places, version, snmp mibs, and so on. [PR1597999](#)
- The mspmand daemon memory leak might be observed after the HA primary goes down. [PR1598356](#)
- On MX10008 and MX10016 routers with JNP10K-RE1, unknown SMART attributes for StorFly VSFBM8CC200G SSD occurs. [PR1598566](#)
- EVPN-VXLAN, RE1 went to DB prompt when tried to load profile configurations over LRM configurations. [PR1598814](#)

- During day1 stage of device management from MIST, the cloud LED will remain in green state even if device loses connectivity with cloud. [PR1598948](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- Traffic might get dropped silently upon link flap after a topology change. [PR1599215](#)
- The SFP-T port might stop forwarding traffic. [PR1600291](#)
- The gNMI Telemetry might stop working after Routing Engine switchover. [PR1600412](#)
- Silent drop of traffic might be seen when multicast is configured on the device and there is a interface flap or FPC restarts. [PR1600642](#)
- Observed dcpfe core-dump while testing unified ISSU from 21.1R1.11 to 21.2R1.7. [PR1600807](#)
- Layer 2 host injected packets might not go out of IRB interface. [PR1602131](#)
- Under certain scaling scenarios with EVPN-VXLAN configurations, the l2ald process might be aborted and then recovered. [PR1602244](#)
- The lpv6 link local BFD session might not come up if we do not have child link of an aggregated Ethernet mapped to Packet Forwarding Engine inst 0. [PR1602493](#)
- The show system errors fru detail command is not displaying reset-pfe as the cmerror configured action. [PR1602726](#)
- 21.3TOT:TCP\_TLS\_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd\_spc3.elf.0.tgz is seeing while verifying TCP based logging functionality with GRES with AMS-NextHop style. [PR1603466](#)
- The show commands show services web-filter secintel-policy-status profile p1 and show services web-filter secintel-policy-db ip-prefix-information need to populate IP address count, term count related to blacklist, whitelist of global database and geo-ip database. [PR1603517](#)
- VRRP and BFD might flap on IRB interface on MPC10 and MPC11 line cards. [PR1604150](#)
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams. [PR1604283](#)
- NPC logs seen when vrf localisation is enabled. [PR1604304](#)
- Remote aggregated Ethernet member failures (via disable/laser-off) might cause the high tail drop to result in high traffic loss. [PR1604823](#)
- GRE tunnel might flap when hierarchical-scheduling is configured. [PR1605189](#)
- Traffic is not load balanced across member interfaces while configuring AMS bundle with 8 members interfaces. [PR1605284](#)

- Harmless error message might be seen when downgrading from 21.2/21.3/21.4 to 21.1 or older image on VMHost platform. [PR1605915](#)
- VM host platforms might boot exactly 30 minutes after executing request `vmhost halt` command. [PR1605971](#)
- 5G-CUPS:bbe-cups-5G-setup:wf-eabu-dev.tadcaster:re1 {version} vmcore.0.gz [PR1606146](#)
- Fabric error might be seen when MPC10E to MPC2, MPC3, MPC4, MPC5, MPC6 based FPC fabric traffic is congested. [PR1606296](#)
- Observing continuous SNMP trap for "Over Temperature!" for all the MX10016 line cards (FPC: JNP10K-LC480). [PR1606555](#)
- Random IP assignment might be done on MX Series platforms configured with PCP and DS-Lite. [PR1606687](#)
- The **WO-0: OGEO dequeue watermark hit** might seen with Layer 2 related configuration and receiving jumbo-frame packets. [PR1606967](#)
- IPv6 link-local BFD session might not come up on MX Series platforms. [PR1607077](#)
- The speed auto-negotiated SFP-T transceiver might not be joined to the aggregated Ethernet after performing dcd restart or Routing Engine switchover on MX104. [PR1607734](#)
- Address error case in open message to comply to RFC 8664 in PCCD and PCE\_Server. [PR1608511](#)
- BFD over GRE tunnel interfaces gets stuck in **init** state with GRES enabled. [PR1609630](#)
- DHCP subscribers over PWHT might be dropped upon GRES after the system reboot. [PR1609818](#)
- On MX204, interface flaps might be observed on certain ports. [PR1609988](#)
- AMZN-QFX5200 mib OID `ifOutDiscards` misbehaving and returning value 0 which is not expected. [PR1610540](#)
- Traffic loss might be observed if dot1X is configured with **supplicant multiple** and authenticated user from radius is in single supplicant mode. [PR1610746](#)
- MACsec session might be dropped due to one way congestion. [PR1611091](#)
- Erratic behaviour might be seen on platforms using MPC line cards after unified ISSU is performed. [PR1611165](#)
- Inter-vlan connectivity might be lost in an EVPN-VXLAN with CRB topology. [PR1611488](#)
- The routing protocol engine CPU is getting stuck at 100%. [PR1612387](#)

- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. [PR1612555](#)
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. [PR1612624](#)
- The PFE/SIB/SCBE/FPCs might reboot due to the unexpected fabric errors shown up on MX240, MX480 and MX960 platforms. [PR1612957](#)
- Traffic loss might be observed due to the shaping rate be adjusted incorrectly in a subscriber environment on MX Series platforms. [PR1613126](#)
- Enhanced-hash-key might not take effect when configured with forwarding-options. [PR1613142](#)
- For PS Service IFL configured in MPC2-NG/MPC3-NG interface stats do not show correct (shaped) value when shaping is applied. [PR1613395](#)
- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. [PR1613489](#)
- Unknown SMART attributes for StorFly VSF6M6CC100G-JUN1 SSD might be seen. [PR1614068](#)
- FPCs might be stuck in **onlining** state after the software release upgrade. [PR1614489](#)
- Any irrelevant configuration changes might trigger NAT routes flap on MX in USF mode. [PR1614688](#)
- MPC6E 3D did not comes back up after MIC offline online test. [PR1614816](#)
- Modifying the input service-filter via COA might fail in subscriber management environment. [PR1614903](#)
- Export memory and temperature metrics for all existing components when it subscribes to telemetry sensor. [PR1615045](#)
- The I2ald process might crash in EVPN scenario. [PR1615269](#)
- Traffic drop might occur when huge number of EIM mappings are created or deleted continuously. [PR1615332](#)
- The CDA-BT process generates a core file when you turn the FPC offline. [PR1615343](#)
- Request to provide an API which gives list of potential policy given a session ID. [PR1615355](#)
- The counter might show double value when chassis enhanced-policer is configured. [PR1615373](#)
- The rasdaemon processes memory leak -- triggered by hardware memory errors on VMHost platforms. [PR1615488](#)
- On MX10008, TPI88812 Onchnage: /components/component[name='FPC7']/state/type after event does not have the correct jvalue. [PR1616049](#)

- Slow memory leak (32 bytes each time) of rpd might be seen. [PR1616065](#)
- No filter found error might be seen while deactivating filter attached to interface after MPC reboot. [PR1616067](#)
- VPLS BUM (Broadcast, Unknown Unicast, and Multicast) traffic does not get forwarded to remote PEs over the MPLS core. [PR1616236](#)
- The show subscribers accounting-statistics and show services l2tp session interface asi0.xx statistics might not work on LNS with asi- interfaces. [PR1616454](#)
- Observed traffic error on 100G FPC for DPT deep loopback test on ports et-0/0/6 and et-0/0/7. [PR1616525](#)
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. [PR1616611](#)
- The Strict-Priority-Scheduler (SPS) might not work accurately across port queues. [PR1616772](#)
- The aftermath process generates core files at  
`RtIfaHandler::notifyCommand,EalIfaHandler::registryClientCommand ,EalIfaHandler::OnAdd (this=0x7f2ffe40e9a0 < EalIfaHandler::instance()::handler>, ifah=...) at ../../src/EalIfaHandler.cpp:222.` [PR1616909](#)
- Layer 2 cpd memory leak might lead to l2cpd process crash. [PR1617151](#)
- In MX Series Virtual Chassis spcd running on SPC3 crashes. [PR1617280](#)
- MPC8E in 1.6T bandwidth mode might not work correctly. [PR1617469](#)
- The l2cpd core file is seen with FIP snooping configuration on any interface. [PR1617632](#)
- Unexpected Routing Engine switchover might be observed. [PR1617720](#)
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. [PR1617830](#)
- Match on v6-prefix for prefix lengths less than or equal to 64 bits does not work. [PR1618211](#)
- GMC clock class is seen transmitted for an additional 16 seconds after the PTP source switches from one line card to another. [PR1618344](#)
- Traffic loss might be observed if the router is configured with ECMP over IRB and the traffic go through the MPC10E and MPC11E line cards. [PR1618354](#)
- The traffic loss might be seen after cleaning the large-scaled NAT sessions in MS-SPC3 based Next Gen Services Inter-Chassis Stateful High Availability scenario. [PR1618360](#)
- The clksyncd might crash and PTP/SyncE might not work. [PR1618929](#)

- Support whole (atomic) updates at CNHG level. [PR1619011](#)
- InputIntf is reported incorrectly for MPLS-ipv4 and MPLS-ipv6 ingress sampling in the case of Layer 3 VPN. [PR1619052](#)
- The hardware process might crash when an FPC is pulled out or some power failure or fault occurs for the FPC. [PR1619102](#)
- ACI VLAN session setup might get failed. [PR1619122](#)
- The nsd might crash while validating NAT translation on MX Series platforms with SPC3. [PR1619216](#)
- Traffic might be dropped when the RSVP is configured with the mtu-signaling. [PR1619510](#)
- Additional commit warnings and errors were introduced to improve security log profile usability. [PR1619694](#)
- The /interfaces/interface/subinterfaces/subinterface/state/counters not exported during initial sync for on-change. [PR1620160](#)
- The bbe subscriber access services might be stuck while rebooting the one redundancy line-card of RLT interface. [PR1620227](#)
- On MX480 routers, output packet drop is observed while verifying services PCEF subscribers. [PR1620421](#)
- OAM CFM session does not come Up if ERPS configured and CFM control traffic uses the same VLAN as ERPS control traffic. [PR1620536](#)
- High wired memory utilization might be observed if GRES is enabled. [PR1620599](#)
- The EVPN type 5 routes might not be installed. [PR1620808](#)
- Static subscribers session might get stuck in initializing state after ungraceful routing engine switchover. [PR1620827](#)
- Incorrect sensor modeling or mapping when using /junos/system/linecard/interface/ native telemetry streaming. [PR1621037](#)
- SNMP get for MIB value for jnxRedundancyConfig does not work as expected. [PR1621101](#)
- SNMP get for MID ID for jnxRedundancySwitchoverReason does not work as expected. [PR1621103](#)
- IFLSet COS hierarchy might be missed in the backup leg after rebooting FPC. [PR1621164](#)
- Flapping of all ports in the same Packet Forwarding Engine might cause Packet Forwarding Engine to be disabled. [PR1621286](#)

- NSSU option is not available from Junos OS Release 21.2R1. This option is missing from the time UI component publish has been separated out. [PR1621611](#)
- PIC gets stuck in offlining state when offline command is issued right after transceiver plugin. [PR1621694](#)
- Traffic loss can be seen on the new primary Routing Engine post GRES. [PR1621696](#)
- Telemetry/jvision, system\_id formate of AFT-MPC(MPC10E) is not aligned with non-AFT MPCs. [PR1622073](#)
- Chassis alarm **VMHost RE 0 Secure BIOS Version Mismatch**, firmware upgrade did not solve the issue. [PR1622087](#)
- When the PHY-Sync state of a line card moves to False, it internally disables the PHY-timestamping of PTP packets. [PR1622108](#)
- AFT firewall telemetry (ZT), suppressed **state**'container and modified field numbers in the render proto. This is to sync with uKernel proto. [PR1622313](#)
- Invocation of `netconf get` command will fail if there are no Layer 2 interfaces in the system. [PR1622496](#)
- Constant increase of PCS errors might be seen on channelized port. [PR1622741](#)
- The port speed shows as 100G even though chassis configuration is set for 40G. This is just a cosmetic display issue. [PR1623237](#)
- The ethtraceroute core file is generated. [PR1623443](#)
- Packet loss might be seen when enabling output sampling on the source interface of tunnel. [PR1624057](#)
- The `show pfe route ip` is getting timed out when route table size is large. [PR1624629](#)
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. [PR1624772](#)
- Traffic drop is seen with egress features enabled on interface hosted on MPC10 and MPC11 line cards. [PR1624804](#)
- The process `hwdfpc` might crash. [PR1624841](#)
- On single IPsec tunnel with PMI when sending internet traffic packet processing might get delayed due to session management issue. [PR1624974](#)
- On Junos OS, specific packets over VXLAN cause FPC reset (CVE-2022-22171). [PR1625292](#)

- JNP10008-SF3, SIB-JNP10004 and JNP10016-SF3 memory errors handling improvement. [PR1625305](#)
- The flowd process lost heartbeat for 45 consecutive seconds without alarm raised. [PR1625579](#)
- The bbe-statsd crash might be seen in the LTS subscriber scenario. [PR1625648](#)
- The gNMI set RPC might fail when multiple values within a single gNMI SetRequest are used for the Junos telemetry interface. [PR1625806](#)
- Packet loops in the PIC even after stopping the traffic on MX Series platform with SPC3 line card. [PR1625888](#)
- The bbe-smgd might crash on backup Routing Engine after unified ISSU or GRES. [PR1626091](#)
- Traffic drop might be seen in node slicing scenario. [PR1626115](#)
- Some Interfaces might not come online after line card reboot. [PR1626130](#)
- Implement show task scheduler-slip-history to display number of scheduler slips and last 64 slip details. [PR1626148](#)
- After configuring 4000 bridge domains, messages log file floods with kernal messages. [PR1626381](#)
- The chassisd might crash on MX104. [PR1626486](#)
- The autoconf might not work if the DHCPv4 discover message has option 80 (rapid commit) ahead of option 82. [PR1626558](#)
- Broadcast traffic might not be forwarded to LT interface in VPLS routing instance after LT interface is deleted and then added back. [PR1626714](#)
- VPLS MAC age time-out might not be applied on some MAC addresses. [PR1627416](#)
- S-PTX10K-144C license SKUs do not load, 400G SKUs do load. [PR1627459](#)
- IP not-ECN-capable traffic is not RED-dropped in an ECN-enabled congested queue. [PR1627496](#)
- DHCP clients might not go to BOUND state when the aggregated Ethernet bundle is enabled between DHCP server and snooping device. [PR1627611](#)
- The shell upgrade script fails for releases earlier than Junos Os Release 21.4. [PR1627618](#)
- Tunnel interface statistics displays incorrect values when JFlow sampling is enabled. [PR1627713](#)
- Layer 3 traffic failure might be observed with scaled MC-LAG configuration. [PR1627846](#)
- Invalid IP length packets encapsulated within MPLS might trigger PPE traps. [PR1628091](#)

- Memory leak might occur on PFED process when the flat-file-profile is configured with configuration use-fc-ingress-stats. [PR1628139](#)
- The EAPoL packets over I2circuit might get dropped at the tunnel start. [PR1628196](#)
- EVPN flood filter might not work for MPC10 and MPC11 line cards. [PR1628270](#)
- The traffic might be dropped on xSTP ports that were earlier in FWD/DESG state after unified ISSU. [PR1628358](#)
- Tunnel-service bandwidth should not be changed when there are active subscribers. [PR1628628](#)
- The show system subscriber-management route summary does not report route summary as expected. [PR1629450](#)
- The I2ald might be stuck in **issu state** when unified ISSU is aborted. [PR1629678](#)
- MPC10E crashes in enhanced-cfm-mode when it receives CFM packets from ONT. [PR1629685](#)
- The egress traffic on non-targeted iflset of subscribers might not be forwarded correctly over targeted aggregated Ethernet interface. [PR1629910](#)
- Multiple link flaps and traffic might be lost on the links. [PR1630006](#)
- The kmd daemon might crash with core files every few minutes on MX Series platforms. [PR1630070](#)
- LACP timeout might be observed during high CPU utilization. [PR1630201](#)
- Indirect next-hop (INH) Version ID higher than 255 might cause INH NH FRR Session moved down state and dropping transit traffic. [PR1630215](#)
- With SCBE3+SPC3, fabric drops are seen around 10M PPS/60G TCP traffic with ~750byte packet size with IPv6 SFW on a single PIC. [PR1630223](#)
- LLDP packets might be sent with incorrect source MAC for RETH or LAG child members. [PR1630886](#)
- PCIe bus error associate to PTP FPGA device during chassis reboot. [PR1631300](#)
- The kmd might crash since the pkid requested memory leak happens on M/MX Series platforms. [PR1631443](#)
- The ipv6 host route prefix match disappear from **forwarding-table** after a ping test, ping continues to work, forwarding table entry is not shown. No impact in traffic. [PR1631607](#)
- Adverse effect on subscriber management observed after deactivating chassis pseudowire-service with active subscribers. [PR1631787](#)

- DHCP ALQ Syslog error bbesmgd[26939]: LIBSDB\_RSMON\_PS\_TABLE\_PTR\_FAILURE: sdb\_get\_ps\_interface\_table\_record:2076 failed to get the ps\_table\_header ptr. [PR1631858](#)
- The rpd process generates core file with the warm-standby configurations due to reference counting issues. [PR1631871](#)
- The transit CCM sessions comes up but transit loopback(LB) ping or LinkTrace(LT) PDUs does not go through. [PR1632255](#)
- High-speed key is not reported for MPC11 in AF interface sensor. [PR1632289](#)
- When deleting the VNI and there is another vlan-id-list with a different VNI, it might cause traffic loss. [PR1632444](#)
- Firewall sensors information of MPC10E, MPC11E, MPC12E, and VMX ZT MPC line-card are not getting streamed to telemetry. [PR1632477](#)
- Summit MX chassis communication does not work after Virtual Chassis member-id set/delete. [PR1632645](#)
- The bbe-smgd process might crash after removing and adding a child link from aggregated Ethernet interface. [PR1633392](#)
- Slow chassis memory leak might occur when chassisd related configuration change is committed. [PR1634164](#)
- PTP clock class might incorrectly be downgraded to 248 when PTP is enabled on Linecard/MIC which does not support phy-timestamping. [PR1634569](#)
- When all configured anchor Packet Forwarding Engines are offline on the SAEGW-u, there might be a peer association mis-match between the SAEGW-u and SAEGW-c. [PR1634966](#)
- CFM CCM PDU is not forwarded transparently on core MX if the IFD is configured under protocols OAM. [PR1635293](#)
- BCM SDK publish build failed with error message in description is fixed. [PR1635318](#)
- Data might not be exchanged through EVPN-VxLAN domain. [PR1635347](#)
- Incorrect interface statistics might be reported on MX204. [PR1636654](#)
- Delay might be observed for the interfaces to come up after reboot or transceiver replacement. [PR1638045](#)
- BNG CUPS: ERA & OIU - Core in oiModShMemEntry during OIU modify when restarting smg-service while bouncing subscribers. [PR1638217](#)
- Locally switched traffic might be dropped with ESI configured. [PR1638386](#)

- Packet Forwarding Engine might get stuck after 100G or 400G interface flaps. [PR1638410](#)
- 
- JUNOS: JDI\_FT\_REGRESSION:SUBSCRIBER\_SERVICES:MX480: Time difference is not as expected when DUT exports interface-queue-stats to ipfix-collector tool after changing reporting-interval. [PR1639378](#)
- The show network-agent statistics gnmi detail CLI command is reporting packet drops for some gnmi target-defined mode sensors. [PR1641483](#)
- The KRT queue might get stuck with the error- **ENOMEM -- Cannot allocate memory**. [PR1642172](#)
- CFM traceoptions writes on every other line. [PR1642948](#)
- On MX480 platforms, PFED CPU increased post unified ISSU and remains around 65-75% for 32000 L2VPN sBNG services. [PR1643077](#)
- PCEP SRv6 code points changed as per IANA. [PR1644332](#)
- Multicast traffic drop might be observed after performing Routing Engine switchover or rpd restart. [PR1593810](#)
- The rpd agent might get crash during NSR switchover. [PR1612725](#)
- DHCP relay no-snoop might not work with DHCP local server in the same routing-instance. [PR1613738](#)
- DHCP subscribers might not be synchronized to backup BNG when DHCP ALQ is configured without topology-discover. [PR1620544](#)
- PDT: restart ppmdd triggers **EAL NH NULL for child NH** and **EalNhHandler Modify: Nh with index: 383675 does not exist**. [PR1628049](#)

## High Availability (HA) and Resiliency

- Memory leaking might occur on backup Routing Engine when ksyncd is in inconsistent state and had encountered an initialization error. [PR1601960](#)
- When MTU is configured on an interface a rare ifstate timing issue could occur at a later point, resulting in ksyncd process crash on backup Routing Engine. [PR1606779](#)

## Infrastructure

- A false error related to insufficient space might appear while installing a Junos OS image that is corrupted. [PR1570148](#)
- Net installation (PXE) is not working. [PR1577562](#)
- FreeBSD12: On Panic 0-size vmcore file get generated. [PR1607299](#)
- Egress TCP RST might not have correctly populated DSCP field. [PR1612208](#)
- Primary FPC might crash when user logs into the device post powercycle of a 3 member EX2300-MP VC. [PR1625987](#)

## Interfaces and Chassis

- Traffic loss is seen after restarting the SIB. [PR1560111](#)
- Commit check failure might happen if similar interfaces are configured under VRRP group. [PR1617020](#)
- Delay in application of CLI configuration by DCD when aggregated Ethernet interface members are configured through JET API. [PR1621482](#)
- CFM enhanced SLA iterators monitoring might stop after restarting chassis-control daemon in vMX. [PR1622081](#)
- The subscribers might be deleted when `host-prefix-only` configuration statement is configured on the underlying-interface in GRES scenario. [PR1630229](#)
- The syslog messages and the dcd crash might be seen in Junos OS. [PR1633339](#)
- CFM sessions are not up after `evo-pfemamd` restart or crash. [PR1634721](#)
- VRRP route tracking for routes in VRF might not work if `chained-composite-next-hop ingress l3vpn` is used. [PR1635351](#)
- Some daemons might get stuck when `snmpd` is at 100% CPU utilization. [PR1636093](#)
- FPC might crash if the continuity-check interval under CFM is modified. [PR1636226](#)
- The `show vrrp extensive` doesn't show the next IFL **Interface VRRP PDU statistics**. [PR1637735](#)
- On Junos 20.3 and later release, the tracking routes of VRRP might become unknown after upgradation. [PR1639242](#)

- The aggregated Ethernet interface with 400GE gets flapped on adding or removing a 400GE member link. [PR1641585](#)
- The vrrpd core file might be observed after interface state change. [PR1646480](#)

## Junos XML API and Scripting

- File download using `request system download` might fail. [PR1604622](#)

## Layer 2 Ethernet Services

- Making configuration changes with `apply-group add/delete` associated with DHCP might result in client connection failure. [PR1550628](#)
- DHCP leasequery is failing to restore binding when the reply is received over IRB interface. [PR1611111](#)
- BFD hold-down timer does not work properly when LAG is configured. [PR1616764](#)
- Enabling DHCP on Junos OS platform might cause the router's file system storage to get filled up with log files. [PR1617695](#)
- The Junos OS, the `jdhcpd` crashes upon receiving a specific DHCP packet (CVE-2022-22179). [PR1618977](#)
- Circuit-id handled incorrectly with backup node for ALQ with topology discover configured. [PR1620461](#)
- The `jdhcpd` process crashes in DHCP and DHCPv6 environment. [PR1625011](#)
- The process `jdhcpd` might get stuck at 100% post clients login or logout. [PR1625112](#)
- Option 82 might not be attached on DHCP request packets. [PR1625604](#)
- The `rpdscheduler` might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. [PR1625617](#)
- IPv6 IA\_NA or IA\_PD routes might get deleted from the DHCPv6 client. [PR1629171](#)
- Non-DHCPv4 BOOTP protocol packets might not be processed if enhanced subscriber management is enabled. [PR1629172](#)

- The aggregated Ethernet interface remains UP instead of down on deleting loopback and aggregated Ethernet interface IP on neighbor while verifying BFD sessions on router. [PR1640240](#)

## MPLS

- The node SID might be seen in an unresolved state. [PR1564169](#)
- IPv4 prefixes might be associated into both IPv4 and IPv6 LDP database after Routing Engine switchover. [PR1611338](#)
- Configuring protocols MPLS lsp-external-controller also throws commit error if in-place-lsp-bandwidth-update is configured under any LSP. [PR1612269](#)
- The rpd process might generate core files for a few value configurations of signaling bandwidth on container LSP. [PR1614248](#)
- The RPD crash might happen due to refcount leak in routing table metrics. [PR1615001](#)
- Standby secondary LSP might be stuck on the same path as primary LSP upon reoptimization. [PR1615326](#)
- Protected LSP goes down with strict hops and link protection configured. [PR1616841](#)
- LDP protections paths might not be established when auto-targeted-session configuration is deactivated and activated. [PR1620262](#)
- Underlay Colored SRTE LSP is being wrongly shown as RSVP LSP in express-segments detail. [PR1623643](#)
- Unexpected traffic loss on LSP headend might be observed when downstream IGP metric changes. [PR1625438](#)
- VCCV BFD session keeps flapping between MX and peer device if ultimate-hop popping is enabled. [PR1634632](#)
- [mpls] [LDP-Tunneling] : mx2020 :: rpd core@ldp\_destroy\_lib is observed in mx2020 after post Gress. [PR1635863](#)
- The rpd memory leak might be observed in a subscriber management environment with RSVP. [PR1637645](#)
- LSP over broadcast segment stays down when RSVP setup protection is enabled. [PR1638145](#)
- Dynamic bypass LSP might flap at every re-optimization interval. [PR1639292](#)

## Network Management and Monitoring

- Ephemeral instance configuration is not removed even after deleting the ephemeral instance from set system configuration-database. [PR1553469](#)
- Rtsdbd core file might be seen when IPsec configuration is activated and deactivated. [PR1610594](#)

## Platform and Infrastructure

- The pcmd process might crash after an upgrade. [PR1335526](#)
- The subscribers might not come online after interface flaps on MX Series platforms. [PR1591905](#)
- Traffic through one SPU might stop with potential packet drop issue with alarm as FPC Major Errors raised due to the PIC\_CMERROR\_TALUS\_PKT\_LOSS error. [PR1600216](#)
- On MX Series platforms vmcore on both the Routing Engines might be reported due to mbuf corruption. [PR1602442](#)
- The FPC might crash if flow-table-size is configured on MX Series platforms. [PR1606731](#)
- CFM neighbor adjacency will be failed on the aggregated Ethernet member interface of MPC10 and MPC11 line cards. [PR1611816](#)
- Filter related service will not work when the filter is deleted/re-added frequently for aggregated Ethernet interface. [PR1614480](#)
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic. [PR1619111](#)
- CoS custom classifier might not work on logical interface. [PR1619630](#)
- Accounting and auditd process might not work on secondary node. [PR1620564](#)
- Trio-based line cards might crash when Packet Forwarding Engine memory is hot-banking. [PR1626041](#)
- Configuration commit might fail while configuring the configuration statement authentication-key-chains under groups. [PR1626400](#)
- Unrealistic service accounting statistics might be reported due to firewall counter corruption. [PR1627908](#)
- Error message **gencfg\_cfg\_msg\_gen\_handler drop** might be seen after running commit. command [PR1629647](#)

- The packet drop might be seen on FPC on Trio based platforms. [PR1631313](#)
- When route preferred-metric is different for different RPM policies, the same metric is not reflected in routing records. [PR1634129](#)
- Continuous Fabric Link Sanity Check interrupts in intervals of weeks might cause at some point fabric input block traffic blackholing. [PR1636060](#)
- During unified ISSU certain EA based line cards such as LC2103 might crash, causing them to cold boot. [PR1637618](#)
- AUTO-CORE-PR : JDI-RCT vRCT : vmxt\_Inx core found @ topo\_get\_link jnh\_features\_get\_jnh jnh\_stream\_attach. [PR1638166](#)
- SCB reset with Error : zfchip\_scan line = 844 name = failed due to PIO errors. [PR1648850](#)

## Routing Policy and Firewall Filters

- Evaluation of inet-vpn route-filters might not work with /32 exact statements for BGP flowspec routes. [PR1618726](#)
- Services might not work after committing firewall filter counter configuration with similar name of two terms. [PR1625168](#)
- Existing routing policies might change when global default route-filter walkup is changed. [PR1646603](#)

## Routing Protocols

- When igmp-snooping is removed from the device, the device might encounter inconsistent MCSNOOPD. [PR1569436](#)
- New version of OpenSSL (1.1.1) is not supported for NTF-agent of Junos Telemetry Interface. [PR1597714](#)
- After first parallel unified ISSU aborts, subsequent unified ISSU attempts on failed node aborts with **Aborting Daemon Prepare**. [PR1598786](#)
- Observing commit error while configuring **routing-options rib inet6.0 static** on all Junos OS platforms. [PR1599273](#)
- The rpd core might be observed due to memory corruption. [PR1599751](#)

- Kernel crash might be observed on platforms that have BGP configured with family Layer 2 VPN. [PR1600599](#)
- The BGP replication might be stuck in **InProgress** state. [PR1606420](#)
- The commit should fail when microloop-avoidance post-convergence-path is configured without source-packet-routing. [PR1608992](#)
- The rpd might crash after a commit if there are more than one address in the same address ranges configured under **bgp allow**. [PR1611070](#)
- The interface might receive multicast traffic from a multicast group which it is not interested in. [PR1612279](#)
- Undesired protection path might get selected for some destination prefixes. [PR1614683](#)
- The memory leak on rpd might be observed after running `show route` CLI command. [PR1615162](#)
- BFD sessions flapping might occur after performing GRES. [PR1615503](#)
- The incorrect BGP path might get selected even when a better/preferred route is available. [PR1616595](#)
- Traffic drop will be seen when VPN labels are incorrectly allocated due to change in nexthop. [PR1617691](#)
- Verification of BGP peer count fails after deleting BGP neighbors. [PR1618103](#)
- On Junos OS, OpenSSL Security Advisory. [PR1618985](#)
- The rpd might crash and restart when NSR is enabled. [PR1620463](#)
- The aggregated Ethernet interface might send/receive traffic through child link though BFD status is **client in hold-down state**. [PR1624085](#)
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. [PR1626367](#)
- The rpd core file might be seen while processing the BGP updates. [PR1626717](#)
- Multipath route with List-NH which has Indirect-NH as members fails into BGP-LU. [PR1626756](#)
- eBGP Multipath route stuck in KRT queue. [PR1626966](#)
- For prefixes leaked from BGP to IS-IS, the P flag will be set for Prefix-SID advertised from IS-IS. [PR1627322](#)
- The contributing routes might not be advertised properly if **from aggregate-contributor** is used. [PR1629437](#)

- The multicast forwarding cache might not get updated after deactivating the scope-policy configuration. [PR1630144](#)
- The BGP ECMP might not work and multipath route won't be created. [PR1630220](#)
- The rpd might crash when BGP labeled-unicast family routes are present and BGP multipath is turned on. [PR1630987](#)
- The rpd might crash after clearing IS-IS database. [PR1631738](#)
- The rpd might get into an infinite loop while clearing IS-IS database. [PR1632122](#)
- The BGP session might flap after rpd crash with **switchover-on-routing-crash** and NSR enabled in a highly scaled environment. [PR1632132](#)
- IS-IS database might not be synchronized in some multiple areas scenario. [PR1633858](#)
- OSPF adjacency might take longer time to converge when the neighbour restarts non-gracefully. [PR1634162](#)
- Multipath route gets formed for a VPN prefix due to incorrect BGP route selection logic. [PR1635009](#)
- The BGP peer might stay down in shards after doing a rollback. [PR1643246](#)

## Services Applications

- L2TP tunnels might go down and not be able to re-establish after restarting the bbe-smgd process. [PR1629104](#)
- Tunneled subscribers might be stuck in terminating state in L2TP subscriber scenario. [PR1630150](#)
- DTCP radius-flow-tap fails to program Packet Forwarding Engine when trigger X-NAS-Port-Id exceeds 48 character length. [PR1647179](#)

## Subscriber Access Management

- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. [PR1604967](#)
- Class attribute is corrupted for radius accounting messages since unified ISSU to 19.1 or higher release on MX Series platforms. [PR1624066](#)

- Radius CoA (Change of Authorization) NAK might not be sent with the configured Source Address in a virtual-router environment. [PR1625858](#)
- ESSM sessions might get terminated in radius as class attribute has got corrupted after performing unified ISSU. [PR1626718](#)
- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. [PR1627974](#)
- Event-timestamp in radius Acct-Stop might show future time. [PR1643316](#)

## User Interface and Configuration

- Mgd might generate core files while running any RPC after running copy-config rpc with unreachable host in the URL on the same NETCONF session. [PR1590625](#)
- Interface configuration might get stuck and might not update after several ephemeral commits. [PR1598123](#)
- Unable to delete Linux core files by using `file delete /var/core/*/vmcore*` CLI command. [PR1624562](#)
- Junos OS upgrade might fail with error **configuration database size limit exceeded**. [PR1626721](#)
- The process mgd might crash with errors if `system scripts synchronize` is configured. [PR1628046](#)

## VPNs

- The multicast route is not getting installed after exporting of secondary routes from one instance to another. [PR1562056](#)
- The rpd process might crash during unified ISSU if the auto-sensing configuration statement is enabled for I2circuit. [PR1626219](#)
- Type 7 routes might be lost in MVPN+PIM SSM scenario. [PR1640487](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading to Release 22.1R2 | 81](#)
- [Procedure to Upgrade to FreeBSD 12.x-Based Junos OS | 81](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 84](#)
- [Upgrading a Router with Redundant Routing Engines | 85](#)
- [Downgrading from Release 22.1R2 | 85](#)

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

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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

Platform	FreeBSD 6.x-based Junos OS	FreeBSD 12.x-based Junos OS
MX5, MX10, MX40, MX80, MX104	YES	NO
MX240, MX480, MX960, MX2010, MX2020	NO	YES

## Basic Procedure for Upgrading to Release 22.1R2

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

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

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

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

## Procedure to Upgrade to FreeBSD 12.x-Based Junos OS

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

To download and install FreeBSD 12.x-based Junos OS:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage:  
<https://www.juniper.net/support/downloads/>
2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the Release drop-down list to the right of the Download Software page.
4. Select the Software tab.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.

8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new jinstall package on the routing platform.

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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-22.1R2.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.1R1.9-signed.tgz
```

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-22.1R2.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-22.1R2.9-limited.tgz
```

Replace source with one of the following values:

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

- `ftp:// hostname/ pathname`
- `http:// hostname/ pathname`
- `scp:// hostname/ pathname`

Do not use the `validate` option while upgrading from Junos OS (FreeBSD 6.x, 10.x, and 11.x) to Junos OS (FreeBSD 12.x). This is because programs in the **junos-upgrade-x** package are built based on FreeBSD 12.x, and Junos OS (FreeBSD 6.x, 10.x, and 11.x) would not be able to run these programs. You must run the `no-validate` option. The `no-validate` statement disables the validation procedure and allows you to use an import policy instead.

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

Rebooting occurs only if the upgrade is successful.

**NOTE:**

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).
- Starting in Junos OS Release 22.1R2, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

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

**NOTE:** After you install a Junos OS Release 22.1R2 `jinstall` package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the `jinstall` package that corresponds to the previously installed software.

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

## 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 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
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](#).

## Upgrading a Router with Redundant Routing Engines

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

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

For the detailed procedure, see the [Installation and Upgrade Guide](#).

## Downgrading from Release 22.1R2

To downgrade from Release 22.1R2 to another supported release, follow the procedure for upgrading, but replace the 22.1R1 jinstall package with one that corresponds to the appropriate release.

**NOTE:** You cannot downgrade more than three releases.

For more information, see the [Installation and Upgrade Guide](#).

# Junos OS Release Notes for NFX Series

## IN THIS SECTION

- [What's New | 86](#)
- [What's Changed | 86](#)
- [Known Limitations | 86](#)
- [Open Issues | 87](#)
- [Resolved Issues | 88](#)
- [Migration, Upgrade, and Downgrade Instructions | 89](#)

These release notes accompany Junos OS Release 22.1R2 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

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

## Known Limitations

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

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

## Open Issues

### IN THIS SECTION

- [High Availability | 87](#)
- [Multicast | 87](#)

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.

## High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the `request chassis fpc slot slot restart node local` command or due to dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. [PR1557607](#)

## Multicast

- When an NFX series device forwards a Protocol Independent Multicast (PIM) bootstrap router (BSR) packet over a label-switched interface (LSI), the BSR information might not get advertised over next-generation multicast virtual private networks (MVPN). This might impact the creation of the next-generation MVPN. [PR1664211](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 22.1R2 | 88](#)

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

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

## General Routing

- On NFX250 device, core files are dumped into the device when you delete vmhost VLANs. [PR1637649](#)

## Virtual Network Functions (VNFs)

- On all the NFX devices that have a VNF interface configured with trust mode enabled, VRRP is not functional.

To resolve this issue, you must disable the spoof-check, using the CLI `set virtual-network-functions vnf-name interfaces interface-name mapping interface virtual-function disable-spoof-check`.

### Resolved Issues: 22.1R2

### IN THIS SECTION

- [General Routing | 89](#)
- [Virtual Network Functions \(VNFs\) | 89](#)

## General Routing

- On NFX250 device, core files are dumped into the device when you delete vmhost VLANs. [PR1637649](#)

## Virtual Network Functions (VNFs)

- On all the NFX devices that have a VNF interface configured with trust mode enabled, VRRP is not functional. [PR1643164](#)

To resolve this issue, you must disable the spoof-check, using the CLI `set virtual-network-functions vnf-name interfaces interface-name mapping interface virtual-function disable-spoof-check`.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases | 89](#)
- [Basic Procedure for Upgrading to Release 22.1 | 90](#)

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

**NOTE:** For information about NFX product compatibility, see [NFX Product Compatibility](#).

## Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, 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 7: EOL and EEOL Releases**

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/Downgrade to subsequent 3 releases	Upgrade/Downgrade to subsequent 2 EEOL releases
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](#).

## Basic Procedure for Upgrading to Release 22.1

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

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

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

To download and install Junos OS Release 22.1R2:

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

# Junos OS Release Notes for PTX Series

## IN THIS SECTION

- What's New | 92
- What's Changed | 92
- Known Limitations | 93
- Open Issues | 93
- Resolved Issues | 95
- Migration, Upgrade, and Downgrade Instructions | 97

These release notes accompany Junos OS Release 22.1R2 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

There are no changes in behavior and syntax in this release for PTX Series Routers.

## Known Limitations

### IN THIS SECTION

- [General Routing | 93](#)
- [Infrastructure | 93](#)

Learn about known limitations in this release for PTX Series Routers.

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

## General Routing

- When number of routes resolves over ECMP path, inline BFD sessions might flap during clear IS-IS adjacency or RPD restart trigger. [PR1612802](#)

## Infrastructure

- When upgrading from Junos OS Release 21.2 and earlier to Junos OS Release 21.2 and later, validation and upgrade fails. Use the `no-validate` command to upgrade. [PR1568757](#)

## Open Issues

### IN THIS SECTION

- [General Routing | 94](#)
- [Interfaces and Chassis | 95](#)
- [MPLS | 95](#)

Learn about open issues in this release for PTX 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

- PTX Series platforms with the FPC-PTX-P1-A or FPC2-PTX-P1A line card might encounter a single event upset (SEU) event that causes a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt\_min\_free\_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero Jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 The Junos OS chassis management error handling does detect such a condition, raises an alarm, and performs the disable-pfe action for the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, restart the FPC as needed. Soft errors are transient or non-recurring. FPCs experiencing such SEU events do not have any permanent damage. Contact your Juniper Networks support representative if the issue occurs after an FPC restart. [PR1254415](#)
- Flapping might occur on the channelized ports of PTX Series devices during ZTP, when one of the port gets disabled on the supporting device. [PR1534614](#)
- Unsupported configuration is attempted by the script that then hits the maximum threshold for the given platform. [PR1555159](#)
- On PTX platforms, when Inline Jflow is configured and high sampling rate (more than 4000 per second) is set, high CPU utilization might be observed and this might result in relevant impacts on traffic analysis and billing. [PR1569229](#)
- The output-mac-control-frames and output-mac-pause-frames counters do not increase. [PR1610745](#)
- When sending BGP Labeled Unicast (BGP-LU) traffic or Layer 3 VPN traffic over IPIP tunnels, the remote end device is a purely an IP device that does not understand labels, the labeled unicast or Layer 3 VPN label cannot go on top. [PR1631671](#)
- On all PTX platforms, EDAC errors are triggered but alarms are not observed until the FPC gets rebooted due to the data corruption in hardware. [PR1646339](#)

- V6 default route will not get added after successful DHCPv6 client binding on PTX1000 router during zero-touch provisioning. [PR1649576](#)
- On PTX10002, PTX10003, PTX10008, and PTX10016 devices; if protocols l2circuit and channel tcc is enabled for providing layer 2 transaction, IS-IS connection through the layer 2 domain might get failed and traffic loss might be seen. [PR1590387](#)
- Junos might translate the custom yang configuration even after disabling the custom Yang package. [PR1599107](#)

## Interfaces and Chassis

- The memory usage of the "rpd" process on the backup Routing engine might increase indefinitely due to leak in krt\_as\_path\_t. [PR1614763](#)

## MPLS

- On PTX3000 devices, if RPD thrashes during a GRES switchover, there might be traffic loss on MPLS LSPs. [PR1590681](#)

## Platform and Infrastructure

- In rare occurrence, Routing Engine kernel might crash while handling TCP sessions if you enable GRES or NSR. [PR1546615](#)

## Resolved Issues

### IN THIS SECTION

- [Class of Service | 96](#)
- [General Routing | 96](#)
- [Interfaces and Chassis | 97](#)

- Multicast | 97
- Routing Protocols | 97

Learn about the issues fixed in this release for PTX 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

- The default code-point aliases and respective CoS value bit patterns are inconsistent with Junos OS. [PR1667404](#)

## General Routing

- The `/interfaces/interface/subinterfaces/subinterface/state/counters` not exported during initial synchronization for on-change. [PR1620160](#)
- QSFP in slot `et-0/0/0` might not come up after plug-in. [PR1620527](#)
- CCL:NGPR: RPD\_KRT\_RESPOSE\_ERROR: krt change failed for prefix `<>` error from kernel is EINVAL -- Bad parameter in request. [PR1638745](#)
- KRT queue entries are stuck during Routing Engine switchover when backup RPD is not yet ready. [PR1641297](#)
- Traffic over conditional metric enabled LSP might get null-routed (silent packet drop). [PR1643587](#)
- The MAC-vrf does not support MAC limit configuration. [PR1647327](#)
- BGP sensor `"/bgp-rib/afi-safis/afi-safi/ipv4-unicast/loc-rib/"` not available as a periodic sensor. [PR1649529](#)
- Regressions, VPTX - after restart routing, Junos Telemetry Interface sensors are not getting reset and in result the verification is failing as `/${isis_ae_intf}, ${StreamTxCount1}` objects are coming unequal. [PR1652372](#)
- Configuring gre-key in firewall filter might breaks the DSCP classification. [PR1652762](#)

- SRv6 END.DT46 and END.DT4 configuration might not be supported. [PR1655518](#)
- FPC heap memory leak might be observed with the multicast configuration and modification of multicast group routes. [PR1661286](#)

## Interfaces and Chassis

- The FPCs might not come online after the USB upgrade method. [PR1637636](#)

## Multicast

- Traffic silent packet drop might be seen due to next-hop install failure on Junos PTX platforms. [PR1653920](#)

## Routing Protocols

- The BGP route might still be present in the multi-path route after increased IGP cost. [PR1643665](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading to Release 22.1 | 98](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 100](#)
- [Upgrading a Router with Redundant Routing Engines | 101](#)

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

## Basic Procedure for Upgrading to Release 22.1

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 22.1R2:

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-  
x86-64-22.1R2.9.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-  
x86-64-22.1R2.9-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 22.1 `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](#).

## 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 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
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](#).

## 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](#).

## Junos OS Release Notes for QFX Series

### IN THIS SECTION

- [What's New | 102](#)
- [What's Changed | 103](#)
- [Known Limitations | 104](#)
- [Open Issues | 105](#)
- [Resolved Issues | 110](#)
- [Migration, Upgrade, and Downgrade Instructions | 114](#)

These release notes accompany Junos OS Release 22.1R2 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

### 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

- Junos OS API and Scripting | 103
- Network Management and Monitoring | 103

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

## Junos OS API and Scripting

- **The <request-system-zeroize> RPC response indicates when the device successfully initiates the requested operation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—When the <request-system-zeroize> RPC successfully initiates the zeroize operation, the device emits the <system-zeroize-status>zeroizing re0</system-zeroize-status> response tag to indicate that the process has started. If the device fails to initiate the zeroize operation, the device does not emit the <system-zeroize-status> response tag.

## Network Management and Monitoring

- **Junos XML protocol Perl modules deprecated (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—We no longer provide the Junos XML protocol Perl client for download. To use Perl to manage Junos devices, use the NETCONF Perl library instead.

[See [Understanding the NETCONF Perl Client and Sample Scripts.](#)]

- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

[See [Enable and Configure Instances of the Ephemeral Configuration Database](#).]

- **Support for automatically synchronizing an ephemeral instance configuration upon committing the instance (EX Series, MX Series, MX Series Virtual Chassis, PTX Series, QFX Series, and vMX)**—You can configure an ephemeral database instance to synchronize its configuration to the other Routing Engine every time you commit the ephemeral instance on a dual Routing Engine device or an MX Series Virtual Chassis. To automatically synchronize the instance when you commit it, include the `synchronize` statement at the `[edit system commit]` hierarchy level in the ephemeral instance's configuration.

[See [Commit and Synchronize Ephemeral Configuration Data Using the NETCONF or Junos XML Protocol](#).]

## Known Limitations

### IN THIS SECTION

- [General Routing | 104](#)
- [Infrastructure | 105](#)

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

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

## General Routing

- On QFX5100 devices, NSSU from older Junos OS release with Broadcom SDK 6.3.x to new Junos OS release with Broadcom SDK 6.5.x might not work. As a workaround, perform a normal upgrade from older release to new release. [PR1496765](#)

- On QFX5000 devices, in the EVPN-VXLAN deployment, the BUM traffic replication over VTEP might send out more packets than expected. [PR1570689](#)
- On QFX5000 devices, IRACL filters will not be able to match on the VXLAN tunnel terminated packets. [PR1594319](#)
- On QFX5000 devices, you must configure only one static ARP with multicast-MAC entry per IRB interface. If you configure more than one static ARP with multicast-MAC entry per IRB interface, then the packets with different destination IP having static multicast-MAC always go out with any one of the multicast-MAC configured in the system. [PR1621901](#)
- Unified ISSU on QFX5120-48Y devices are not be supported if there is a change in the Cancun versions of the chipset SDKs between the releases. This is a product limitation as change in the Cancun firmware leads to the chip reset and hence ISSU gets impacted. The Cancun versions in the chipset SDKs should be the same between two JUNOS OS releases for ISSU to work. [PR1634695](#)

## Infrastructure

- When upgrading from Junos OS 21.2 release and earlier to a later release, validation and upgrade fails. Use the `no-validate` command to upgrade. [PR1568757](#)

## Open Issues

### IN THIS SECTION

- [EVPN | 106](#)
- [General Routing | 106](#)
- [Layer 2 Ethernet Services | 108](#)
- [Layer 2 Features | 109](#)
- [Platform and Infrastructure | 109](#)
- [Routing Protocols | 109](#)

Learn about open issues in Junos OS Release 22.1R2 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

- Modifying the I-ESI value is traffic effecting event. If this must be done then follow the below steps in order to avoid the issue:
  - Deactivate interconnect stanza for the routing-instance in question.
  - Modify the I-ESI value.
  - Activate the interconnect stanza.

[PR1600600](#)

- With translation VNI, when you move MAC from DC1 to DC2., VM move across DC where there is not translate VNI configuration in the interconnect works as designed. [PR1610432](#)
- EVPN Local ESI MAC limit configuration might not get effective immediately when it has already learned remote MH MACs. Clear the MAC table from all MH PE devices and configure the MAC limit over local ESI interfaces. [PR1619299](#)
- On QFX5000 and QFX10,000 devices, on interface up or down event loop prevention might not work resulting in BUM traffic being silently discarded. [PR1669811](#)

## General Routing

- When VLAN gets added as an action for changing the VLAN in both ingress and egress filters, the filter does not get installed. [PR1362609](#)
- VXLAN VNI (multicast learning) scaling on QFX5110 device, traffic issue occurs from VXLAN tunnel to Layer 2 interface. [PR1462548](#)
- When running the `show pfe filter hw filter-name` command, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- On QFX5100 devices not running the QFX-5e codes (non-TVP architecture), when an image with the Broadcom SDK upgrade (6.5.x) gets installed, the CPU utilization might go up by around 5 percent. [PR1534234](#)

- 5M DAC connected between QFX10002-60C and MX2010 devices doesn't link up. However, with 1M and 3M DAC this interop works as expected. With QFX10002-60C and ACX or traffic generator the same 5M DAC works seamlessly. There seems to be certain SI or link level configuration on both QFX10002-60C and MX2010, which needs to be debugged with the help from hardware and SI teams. [PR1555955](#)
- To avoid the additional interface flap, interface hold time must be configured. [PR1562857](#)
- In a mixed QFX5100 setup, duplicate traffic might be observed for some Layer 3 multicast traffic streams. [PR1568152](#)
- In a fully loaded devices, at times the firewall programming fails due to scaled prefix configuration with more than 64800 entries. [PR1581767](#)
- PIM VXLAN does not work on the TD3 chipsets enabling the VXLAN flexflow after Junos OS 21.3R1 release. PIM VXLAN or data plane VXLAN must use Junos OS 21.3R1 release. [PR1597276](#)
- On QFX5100 device, the optical power gets displayed after detaching and attaching QSFP on the disable interface. [PR1606003](#)
- The dfwd process generates a core file when accessing the ephemeral database files, which gets deleted through script. [PR1609201](#)
- In QFX10002-60C devices under MAC statistics, the output-mac-control-frames and output-mac-pause-frames does not increment. [PR1610745](#)
- Minimal traffic loss might occur if the number of interfaces in the aggregated Ethernet interface and might observe slight increase if the number of interfaces in the aggregated Ethernet interface is increased but the drop is inconsistent and the packet drop would be expected around ~0.0001%. [PR1629661](#)
- On QFX5000 devices with 5e image, chassis status LED does not work properly. You might observe unexpected state of SYS or MST LED on the primary or backup FPC. [PR1630380](#)
- The backup FPC lose their connection to primary when the new members are added to the VCF (Virtual Chassis Fabric). [PR1634533](#)
- On QFX devices, IPv6 traffic output byte (IPv6-transit-statistics) would not be in expected range as per traffic generator status. [PR1653671](#)
- On QFX5120-48T devices, NSSU fails with below combinations:
  - From 22.1R1.10 to 22.2R1.6
  - From 21.4R1.12 to 22.2R1.6
  - From 21.3R2.11 to 22.2R1.

## PR1669702

- On QFX10,000 devices with scaled number of BFD (Bidirectional Forwarding Detection) sessions configured, addition of a new BFD session might cause flapping in the newly added session and other existing BFD sessions. [PR1621976](#)
- On QFX5000 devices, the MAC address from local CE devices (customer edge) might not get learned when you configure EVPN-VXLAN. The traffic drops as MAC might not be learnt. [PR1651827](#)
- On QFX5100-24Q devices, Virtual Chassis goes in to the Unstable state for 3 to 7 minutes causing traffic loss. [PR1661349](#)
- On QFX5000 devices, when unicast ARP (Address Resolution Protocol) is received for a MAC address that is already learned in an EVPN-VXLAN environment, the ARP request is flooded and duplicate packets might be seen on leaf devices. We might see some service impact where split-horizon might not work or continuous mac-move might be seen. This issue is rare and very unlikely to occur in a production environment due to presence of intermediate switches which might resolve the unicast ARP query. [PR1665306](#)
- On all QFX10002 devices, multihop Bidirectional Forwarding Detection (BFD) over routing instance with inline mode configuration keeps the BFD sessions down. [PR1667751](#)
- On Junos OS Releases 21.4 and 22.1, when QFX5120 device performs IFA init for VLAN flows, the device does not update the congestion field of IFA meta-data stack which needs to be copied from ECN field of outer IP header. [PR1674431](#)
- If LAG interface has VLAN translation configuration and a member interface is deleted or removed from LAG interface than it will delete the VLAN translation programming from PFE on local FPC. If there is another active interface on same FPC in the same LAG then traffic hitting on this LAG member will get drop belongs to VLAN translation. [PR1676772](#)
- On QFX5200-32C devices, unwanted packets gets generated by the router interface even though there was no traffic being sent. [PR1670728](#)

## Layer 2 Ethernet Services

- When the DHCP client configuration comes from the AIU script and vsdk sandbox, the DHCP client configuration coming from AIU script has the serial ID in the vendor ID where as the default configuration from sandbox does not have. There is no impact on functionality or service. [PR1601504](#)

## Layer 2 Features

- In case of the access-side interfaces used as SP-style interfaces, when you add a new logical interface and if there is already a logical interface on the physical interface, there is 20 to 50 milliseconds traffic drop on the existing logical interface. [PR1367488](#)

## Platform and Infrastructure

- When you configure the DHCP relay mode as no-snoop, the offer gets dropped due to incorrect ASIC programming. This issue occurs while running the DHCP relay on EVPN-VXLAN environment. [PR1530160](#)
- If you use the source-address NTP configuration parameter and issue the `set ntp date` command, packets will be sent with the source address of the outgoing interface rather than the manually configured IP address. Typically, the manually configured IP address would be a loopback address. The problem does not apply to automatically generated NTP poll packets. [PR1545022](#)

## Routing Protocols

- When the `accept-remote-source` command under PIM gets removed, the PIM SG entries might not get updated with the correct RPF. [PR1593283](#)
- The `mcsnoopd` process generates core files due to the nexthop index being quickly reused by the Kernel. As a result, when application holds the old nexthop reference, which waits for deletion response from Kernel, the same nexthop Index can be received from other applications like RPD for EVPN core-Nexthop updates as in current case. This will lead to the `mcsnoopd` process wrongly manipulating the nexthop ref counting, leading to using a freed nexthop memory when this nexthop-index finally gets freed. This will be fixed through a feature enhancement underway where the Kernel maintains a timer to ensure a nexthop-index does not put to free pool immediately for reuse and hence can be reused post the new timer expiry. [PR1605393](#)

## Resolved Issues

### IN THIS SECTION

- [Class of Service \(CoS\) | 110](#)
- [EVPN | 110](#)
- [Forwarding and Sampling | 111](#)
- [General Routing | 111](#)
- [Interfaces and Chassis | 113](#)
- [Layer 2 Ethernet Services | 113](#)
- [Network Management and Monitoring | 114](#)
- [Routing Protocols | 114](#)
- [VPNs | 114](#)

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.

## Class of Service (CoS)

- The fixed classifier might not work in the MPLS and VXLAN scenario. [PR1650051](#)

## EVPN

- The MAC address might not be visible in the EVPN-VXLAN environment. [PR1645591](#)
- The spine might have stale vtep entry for the ESI even though the host MAC does not get advertised by the leaf. [PR1648368](#)
- The ARP/NS response to anycast IRB might fail due to missing MAC-IP entry. [PR1650202](#)

## Forwarding and Sampling

- The `jnxL2aldMacNotificationMIBObjects` does not work on some QFX devices. [PR1647660](#)

## General Routing

- On QFX5200 devices, the `dcpfe` process might generate core file while testing ISSU from Junos OS 21.1R1.11 release to Junos OS 21.2R1.7 release. [PR1600807](#)
- On QFX10008 and QFX10016 devices, the `chassisd` process generates the `Cannot read hw.chassis.startup_time value: m` error message every five seconds. [PR1603588](#)
- On QFX5 devices, the ports might remain in the `Down` state. [PR1611354](#)
- The packet drop might occur when packet size exceeds 9000 MTU. [PR1615447](#)
- On QFX5120 devices, one-time interface flap might occur. [PR1618891](#)
- The interface on the peer device might remain up even after disabling the 10G interface. [PR1629637](#)
- On QFX5130 devices as Border Leaf with Layer 3 interface connectivity, traffic forwarding does not occur to multihomed receiver connected to Border Leafs when the Layer 3 interface goes down on the DF side. [PR1631249](#)
- On QFX5120-48T-6c devices, slow response or timeout on the CLI or SNMP with accessing to `sxe-0/0/0` might occur. [PR1632620](#)
- On QFX5120-48Y devices, traffic loss might occur when there is a link flap. [PR1634495](#)
- The `chassisd` process might crash if you configure the `chassis disk-partition`. [PR1635812](#)
- Routes might be slow to install in the LPM table. [PR1635887](#)
- Multicast traffic received on the INET interface might be dropped. [PR1636842](#)
- The Packet Forwarding Engine might crash while removing the port from a VLAN. [PR1637013](#)
- On QFX5000 devices, targeted broadcast or WOL feature might not work. [PR1638619](#)
- MAC address of the hosts might get learned on the incorrect VLAN that might lead to traffic loss. [PR1639938](#)
- ICMP TTL exceeded packets are not sent out of the switch. [PR1643457](#)

- On QFX5000 devices with EVPN-LAG multihoming, packets gets dropped in ingress due to the VP-LAG programming issue. [PR1644152](#)
- VXLAN tunnel termination fails due to a change in configuration. [PR1646489](#)
- The firewall might drop inbound packets if you configure the filter under the IRB interface. [PR1646740](#)
- The CLNP traffic tunneled through EVPN-VXLAN fabric might get dropped [PR1648078](#)
- OSPF control packets might get dropped due to the flow check function in the interoperability case. [PR1648272](#)
- The local-minimum-links feature not working as expected on QFX5100 VC platforms [PR1649637](#)
- In EVPN-VXLAN environment, the non-VXLAN traffic might be dropped if the VXLAN and non-VXLAN traffic shares the same ECMP next-hop. [PR1649841](#)
- Traffic Loss will be observed with Virtual-Router [PR1650335](#)
- L2PT configuration on a transit switch in a Q-in-Q environment breaks L2PT. [PR1650416](#)
- The local-bias might stop working after you reboot the device. [PR1651151](#)
- Transit traffic might get dropped and protocols might be down when you modify the firewall filters. [PR1651546](#)
- Port might be down after inserting a specific SFP. [PR1653723](#)
- The ARP might not resolve with the native-vlan configuration. [PR1654215](#)
- LACP sent IN SYNC to server facing interface when core-isolation is in effect. [PR1654459](#)
- On QFX5200 devices, the interface cannot fetch the FEC details after you disable or enable the interface. [PR1657534](#)
- Traffic loss might occur when a VXLAN port recovers from a failure. [PR1659533](#)
- The OSPF Flow Check function violates RFC6864. [PR1660369](#)
- BUM traffic received on the CE interface loopback to the ingress interface after removing the EVPN VXLAN FRR configuration (reroute-address). [PR1662515](#)
- On QFX5110 devices, the IPv6 ND packets gets dropped. [PR1662707](#)
- ALB status does not display in the CLI. [PR1663881](#)
- Static MACs do not get programmed after reboot, resulting in floods of unicast traffic. [PR1666399](#)

- RIB and Packet Forwarding Engines gets out of synchronization due to a memory leak caused by interface flaps or route churn. [PR1642172](#)
- On QFX5000 devices, an interface might be detached from LACP when you configure the VLAN tagging in the EVPN-VXLAN scenario. [PR1645929](#)
- The inner tag (C-tag) value might get modified to zero for egress traffic when the inner tag values are copied to the outer tag (S-tag). [PR1652976](#)
- Valid software licenses might not be in synchronization between members in the Virtual chassis. [PR1658913](#)
- The slave PTP device does not lock the clock with the primary PTP device. [PR1659453](#)
- On QFX10,000 devices, Junos platforms configuration of IGMP group range might result in traffic loss. [PR1659732](#)
- Verification of status for BFD session is in the Up state while checking the BFD session. [PR1663790](#)
- On specific QFX5000 devices, member links might reduce their configured speed when the other side does not have auto-negotiation disabled. [PR1669436](#)

## Interfaces and Chassis

- VRRP flaps between MC-LAG peers when deleting VLANs on the MC-AE interfaces. [PR1579016](#)
- Traffic might get loss for the MAC addresses learned on the ICL interface. [PR1639713](#)
- Incorrect configuration and rollback might cause issues with ARP learning between ICL interface and local MC-AE interfaces. [PR1648271](#)
- The MAC address might be learned over the incorrect interface in the MC-AE scenario. [PR1658742](#)

## Layer 2 Ethernet Services

- On QFX5210-64C devices, default configurations do not get generated properly from port 32. [PR1639410](#)

## Network Management and Monitoring

- VTEP might report a high speed on the sub-interface causing SNMP alarms. [PR1651774](#)

## Routing Protocols

- The BFD session might be down when you configure multiple addresses of same subnet. [PR1635700](#)
- Ipv6 Inline BFD sessions goes down when neighbor does not get resolved. [PR1650677](#)
- A policy with a community policy action configuration might not work. [PR1660424](#)
- Routing Process Daemon (rpd) crashes and restarts when a specific timing condition is hit with BGP configuration. [PR1659441](#)

## VPNs

- On QFX10000 devices, auto-RP goes down after some time in the NGMVPN scenario. [PR1617620](#)

## Migration, Upgrade, and Downgrade Instructions

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 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
End of Life (EOL)	24 months	End of Engineering + 6 months	Yes	No
Extended End of Life (EEOL)	36 months	End of Engineering + 6 months	Yes	Yes

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

## Junos OS Release Notes for SRX Series

### IN THIS SECTION

- [What's New | 116](#)
- [What's Changed | 116](#)
- [Known Limitations | 117](#)
- [Open Issues | 118](#)
- [Resolved Issues | 120](#)
- [Migration, Upgrade, and Downgrade Instructions | 123](#)

These release notes accompany Junos OS Release 22.1R2 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

### IN THIS SECTION

- [Unified Threat Management \(UTM\) | 116](#)
- [VPNs | 117](#)

Learn about what changed in the Junos OS main and maintenance releases for SRX Series.

## Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:
  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one file-type string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.
  - Renamed the content filtering security logging option `seclog` to `log` to match with the Junos OS configuration standard.
  - Rephrased the reason string associated with content filtering security log message.

[See [content-filtering \(Security UTM Policy\)](#), [content-filtering \(Security Feature Profile\)](#), and [show security utm content-filtering statistics](#).]

## VPNs

- **Unable to connect with OCSP Server for Revocation Check (SRX Series Devices and vSRX)**—When performing revocation check using OCSP, the SRX device does not attempt to connect with the OCSP server when the OCSP server URL contains a domain name that the DNS server cannot resolve. In this case, when the SRX device cannot establish connection to the OCSP server and when one of the following configuration options is set, the OCSP revocation check will either allow or fallback to using CRL:
  - `set security pki ca-profile OCSP-ROOT revocation-check ocs connection-failure disable`
  - `set security pki ca-profile OCSP-ROOT revocation-check ocs connection-failure fallback-crl`

When the SRX device cannot establish connection to the OCSP server and if these options are not configured, then the certificate validation fails.

[See [ocsp \(Security PKI\)](#).]

## Known Limitations

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.

### Infrastructure

- When upgrading from before Junos OS Release 21.2 to Junos OS Release 21.2 and after, validation and upgrade will fail. The upgrading requires using of no-validate configuration. [PR1568757](#)
- On SRX4600 device, the CPU may overrun while performing sanity check due to incompatibility issues between ukern scheduler and Linux driver which might lead to traffic loss. [PR1641517](#)

### VPNs

- On SRX5000 line of devices, in some scenario, the device output might display obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)

## 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.

### Chassis Clustering

- In Z-mode configuration, sometimes the statistics of back-up session may not be correct on fail-over from master to back-up. [PR1667098](#)

### Flow-Based and Packet-Based Processing

- Use an antireplay window size of 512 for IPv4 or IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores \* 32 packets in one batch). Hence, there are no out-of-order packets with 512 antireplay window size. [PR1470637](#)

### High Availability (HA) and Resiliency

- ISSU is getting aborted with ISSU is not supported for Clock Synchronization (SyncE). [PR1652838](#)

### Interfaces and Chassis

- Traffic drop might be seen on irb interface on SRX1500 for network control forwarding class when verifying dscp classification based on single and multiple code-points. [PR1611623](#)

### Platform and Infrastructure

- In Mac-OS platforms when Juniper Secure Connect client connects successfully, the client is not getting minimized to tray icon and needs to be minimized manually. [PR1525889](#)
- With Application-Based Multipath Routing enabled, HTTP sessions take approx 10 minutes to re-establish after a link flap between hub and spoke. [PR1577021](#)
- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- HA AP mode on-box logging in LSYS and Tenant, Intermittently Security log contents of binary log file in LSYS are not as expected [PR1587360](#)

- If a device is rebooted manually or reboots for any other reason, The following messages can be seen on the boot up screen even when the device has valid license and proper configuration to use the features like IDP/UTM [PR1594014](#)
- On the SRX4100 and SRX4200 platforms, it can detect DPDK (data plane development kit) Tx stuck issue and trigger a major chassis alarm goes which might trigger RG1 failover to the healthy node. A DPDK reset will be triggered only to the stuck port and if the reset resolves the tx stuck issue, the major chassis alarm will go off.[PR1626562](#)
- SMTPS sessions are not getting identified when traffic is sent from IXIA (BPS) profile. [PR1635929](#)
- remote-access-juniper-std license might not get freed up while disconnect/reconnect after RGO failover. [PR1642653](#)
- The SKYATP:IMAP/IMAPS Email permitted counter may have incorrect value under certain conditions.[PR1646661](#)
- Firewall-authentication with user-firewall based RADIUS access has syslog missing the username and rule.[PR1654842](#)
- SRX cli command to show fwauth user details like "show security firewall-authentication users identifier 1" and "show security firewall-authentication users address 10.1.1.1" does not display user's group information. [PR1659115](#)
- Device does not drop session with server certificate chain more than 6.[PR1663062](#)
- When client tries to do a TLS 1.3 session resumption and the proxy is not able to honor the resumption request, ideally the cache miss counter has to be incremented once. But due to this bug, it gets incremented twice.[PR1663678](#)

## User Interface and Configuration

- Please use "load update" instead of "load override" to prevent the error messages [PR1630315](#)

## VLAN Infrastructure

- For SOF L2 secure-wire session, if the mac move happen on an existing offloaded session, the packet sent out by SRX will carry old mac address and causing traffic drop on end-user [PR1597681](#)

## VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. [PR1416334](#)

- In some scenario(e.g configuring firewall filter) sometimes srx5K might show obsolete IPsec SA and NHTB entry even when the peer tear down the tunnel. [PR1432925](#)
- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RGO failover. [PR1450393](#)
- On SRX platforms, packets through policy-based IPsec tunnel could be dropped in some case when power-mode is enabled.[PR1663364](#)

## Resolved Issues

### IN THIS SECTION

- [Chassis Clustering | 120](#)
- [Flow-Based and Packet-Based Processing | 121](#)
- [Intrusion Detection and Prevention \(IDP\) | 121](#)
- [J-Web | 121](#)
- [Platform and Infrastructure | 121](#)
- [Routing Protocols | 123](#)
- [Unified Threat Management \(UTM\) | 123](#)
- [VPNs | 123](#)

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.

## Chassis Clustering

- The Create Bearer Request might be dropped on SRX platforms [PR1629672](#)
- MSISDN prepended with additional digits (for example "19") in the logs [PR1646463](#)
- A hardware issue is detected on the RG-0 primary node's CP [PR1651501](#)

## Flow-Based and Packet-Based Processing

- The traffic might get lost when using dedicated HA fabric link [PR1651836](#)
- Performance degradation might be observed when Express Path and PME are both enabled [PR1652025](#)

## Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" [PR1616782](#)

## J-Web

- Significant performance improvements were made to JWeb in this release. [PR1652676](#)
- Various page errors have been corrected in JWeb [PR1658330](#)

## Platform and Infrastructure

- Syslog message "%AUTH-3: warning: can't get client address: Bad file descriptor" is displayed at Jweb login.. [PR1581209](#)
- Juniper Secure Client: traffic gets dropped during reaching JSC installed CLIENT from SERVER behind gateway in TCP path finder enabled VPN gateway [PR1611003](#)
- VPLS interface fails to forward traffic on SRX platform [PR1611400](#)
- Execute RSI on SRX5K platform with IOC2 card installed may trigger data plane failover [PR1617103](#)
- Traffic might be dropped due to the TX queue memory leak on PCI interface [PR1618913](#)
- On SRX Series devices running DNS Security, if a DGA was detected and the action in the configuration was set to 'permit', under rare circumstances, a log would not be generated by the device. [PR1624076](#)

- 21.4R1:IPSEC:pkid.core-tarball found @ pkid\_request\_security\_pki\_local\_cert\_verify (msp=0x1abc940, csb=0xffffdb60, unparsed=0x1a7402e "certificate-id") at ../../../../src/junos/usr.sbin/pkid/pkid\_ui.c:1076 [PR1624844](#)
- Reverse DNS Lookups will no longer be stored in the DNSF Cache when using DNS Security [PR1631000](#)
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache [PR1633519](#)
- Dynamic-address feeds might not work [PR1635705](#)
- 22.1R1:SRX-RIAD:vSRX3.0: SSL: RT:junos-ssl-term is not found in ssl-trace-new logs [PR1640075](#)
- Traffic might be dropped due to the RX queue being full [PR1641793](#)
- 22.1TOT : SnP :SRX5K\_SPC3 : Observing Error "usp\_ipc\_client\_rcv\_ipc\_pipe\_read() " due to coredump,when checking "show security monitoring" cli command, in the latest 22.1(22.1I-20220108.0.0529) build. [PR1641995](#)
- Flowd crash when back to back sigpack is updated at the time of stress traffic [PR1642383](#)
- The SKY ATP integrated service might get impacted on SRX with LSYS [PR1643373](#)
- 21.2R3 : Issue with the command "clear security idp counters packet-log logical-system all" [PR1648187](#)
- The severity of AAMW and SMS' control and submission channel alarms have been reduced from 'major' to 'minor' to avoid triggering a chassis cluster failover in the event of an upstream network issue [PR1648330](#)
- Fabric Board reset with an error message may be observed on certain Junos platforms [PR1648850](#)
- 22.1R1:AUTH:unable to get the "firewall-authentication users" details on node 1 [PR1651129](#)
- SMB File submissions to ATP cloud failed [PR1653098](#)
- Certificate-based VPN tunnel is not established [PR1655571](#)
- The fxp0 interface might remain 'UP' when the cable is disconnected [PR1656738](#)
- Radius responses that take longer than 15 seconds can cause SRX to declare authentication failure [PR1658833](#)

## Routing Protocols

- Delay in BGP session establishment due to longer time for the listening task to be ready on all platforms running "rpd" [PR1651211](#)

## Unified Threat Management (UTM)

- New UTM Content-Filtering CLI is changing from seclog to log [PR1634580](#)
- Modification of Content-Filtering rule order after JunOS 21.4 would not have the desired effect. [PR1653488](#)

## VPNs

- The process "iked" crash might be seen for IKEv1 based VPN tunnels [PR1608724](#)
- Fragmented packets might drop when PMI is enabled [PR1624877](#)
- Severity is unknown at some IPsec syslog messages [PR1629793](#)
- IPsec tunnel might stop processing traffic [PR1636458](#)
- The IPsec tunnel via IPv6 might not establish after rebooting SRX devices [PR1653704](#)
- The Juniper secure connect VPN users may face login issues intermittently [PR1655140](#)
- The device enabled with FIPS mode and rebooted the system fails to boot [PR1655355](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 124](#)

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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 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

Table 10: EOL and EEOL Releases (*Continued*)

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/Downgrade to subsequent 3 releases	Upgrade/Downgrade to subsequent 2 EEOL releases
Extended End of Life (EEOL)	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 | 126](#)
- [What's Changed | 126](#)
- [Known Limitations | 126](#)
- [Open Issues | 126](#)
- [Resolved Issues | 127](#)
- [Upgrade Instructions | 127](#)

These release notes accompany Junos OS Release 22.1R2 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

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

## 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

- [Platform and Infrastructure](#) | 126

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.

## Platform and Infrastructure

- vMX stops as result of riot out of memory condition, reporting Interrupted thread 30 TTP transmit. The memory leak can be observed when checking RSI for pool-0 values. request support information | match pool-0 - Pool-0 Values below 2000 are suspect memory problem.[PR1669261](#)

- On vMX, the blockpointer in the ktree is getting corrupted leading to core-file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. [PR1525594](#)

## Resolved Issues

### IN THIS SECTION

- [Platform and Infrastructure | 127](#)

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.

## Platform and Infrastructure

- AUTO-CORE-PR : JDI-RCT vRCT : vmxt\_Inx core found @ topo\_get\_link jnh\_features\_get\_jnh jnh\_stream\_attach. [PR1638166](#)

## 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.

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

# Junos OS Release Notes for vRR

## IN THIS SECTION

- [What's New | 128](#)
- [What's Changed | 128](#)
- [Known Limitations | 128](#)
- [Open Issues | 129](#)
- [Resolved Issues | 129](#)

These release notes accompany Junos OS Release 22.1R2 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## 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 21.1R2, see "[Known Limitations](#)" on page 43 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

### IN THIS SECTION

- [Platform and Infrastructure](#) | 129

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.

## Platform and Infrastructure

- The video console for vRR might not work after an upgrade to Junos with upgraded FreeBSD. [PR1644806](#)

# Junos OS Release Notes for vSRX

## IN THIS SECTION

- [What's New | 130](#)
- [What's Changed | 130](#)
- [Known Limitations | 131](#)
- [Open Issues | 132](#)
- [Resolved Issues | 133](#)
- [Migration, Upgrade, and Downgrade Instructions | 135](#)

These release notes accompany Junos OS Release 22.1R2 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at [https://www.juniper.net/documentation/product/en\\_US/junos-os](https://www.juniper.net/documentation/product/en_US/junos-os).

## What's New

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

## What's Changed

### IN THIS SECTION

- [Unified Threat Management \(UTM\) | 131](#)
- [VPNs | 131](#)

Learn about what changed in this release for vSRX.

## Unified Threat Management (UTM)

- **Content filtering CLI updates (SRX Series and vSRX)**—We've the following updates to the content filtering CLI:
  - Trimmed the list of file types supported for content filtering rule match criteria. Instead of uniquely representing different variants of a file type, now only one file-type string represents all variants. Hence, the `show security utm content-filtering statistics` output is also updated to align with the new file types available in the rule match criteria.
  - Renamed the content filtering security logging option `seclog to log` to match with the Junos OS configuration standard.
  - Rephrased the `reason` string associated with content filtering security log message.

[See [content-filtering \(Security UTM Policy\)](#), [content-filtering \(Security Feature Profile\)](#), and [show security utm content-filtering statistics](#).]

## VPNs

- **Unable to connect with OCSP Server for Revocation Check (SRX Series Devices and vSRX)**—When performing revocation check using OCSP, the SRX device does not attempts to connect with the OCSP server when the OCSP server URL contains a domain name that the DNS server cannot resolve. In this case, when the SRX device cannot establish connection to the OCSP server and when one of the following configuration options is set, the OCSP revocation check will either allow or fallback to using CRL:
  - `set security pki ca-profile OCSP-ROOT revocation-check ocsf connection-failure disable`
  - `set security pki ca-profile OCSP-ROOT revocation-check ocsf connection-failure fallback-crl`

When the SRX device cannot establish connection to the OCSP server and if these options are not configured, then the certificate validation fails.

[See [ocsp \(Security PKI\)](#).]

## Known Limitations

There are no known limitations in hardware or software 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.

## Open Issues

Learn about open issues in this release for vSRX.

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

### Flow-Based and Packet-Based Processing

- The ICMPv6 tcp sequence info is missing in the icmp v6 error generated. [PR1611202](#)
- Due to JUNOS CLI framework's implementation, Current fix has a caveat that customer had better keep 1~2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. [PR1625531](#)

### Platform and Infrastructure

- With ssl-proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- AMR when it is enabled in non-cso v6 over v6 mode with IPsec tunnels, the first session after reboot or forward restart, will not have multipath treatment, post that the feature works fine. [PR1643570](#)
- Device does not drop session with server certificate chain more than 6. [PR1663062](#)
- When client tries to do a TLS 1.3 session resumption and the proxy is not able to honor the resumption request, ideally the cache miss counter has to be incremented once. But due to this bug, it gets incremented twice. [PR1663678](#)

### 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

### IN THIS SECTION

- [Flow-Based and Packet-Based Processing](#) | 133
- [Intrusion Detection and Prevention \(IDP\)](#) | 133
- [J-Web](#) | 134
- [Network Address Translation \(NAT\)](#) | 134
- [Platform and Infrastructure](#) | 134
- [Unified Threat Management \(UTM\)](#) | 134
- [VPNs](#) | 135

Learn about the issues fixed in this release for vSRX.

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

## Flow-Based and Packet-Based Processing

- traffic in the power-mode still passthrough when the ingress logic interface is manually disabled [PR1604144](#)
- TCP-MSS override for GREoIPSec does not work [PR1630124](#)

## Intrusion Detection and Prevention (IDP)

- 21.2R3:SRX345:vSRX3.0:Device is hanging while checking the cli " show security idp attack attack-list policy combine-policy" [PR1616782](#)

## J-Web

- Significant performance improvements were made to JWeb in this release. [PR1652676](#)
- Various page errors have been corrected in JWeb [PR1658330](#)

## Network Address Translation (NAT)

- Datapath daemon might crash resulting in total traffic and service failure [PR1645039](#)

## Platform and Infrastructure

- SRX\_RIAD:CSRX:LOG: RT-Log pattern is not matching in 21.1R1, 21.2R2, 21.2R1 and 21.4R1. [PR1565153](#)
- PKID core during auto-re-enrollment of CMPv2 certificates. [PR1580442](#)
- On SRX Series devices running DNS Security, if a DGA was detected and the action in the configuration was set to 'permit', under rare circumstances, a log would not be generated by the device. [PR1624076](#)
- On SRX Series devices running DNS Security, a dataplane memory leak may occur within the DNSF plugin when entries age-out of the DNSF cache [PR1633519](#)
- Application group name is not found for micro apps in CLI show output [PR1640040](#)
- 22.1R1:SRX-RIAD:vSRX3.0: SSL: RT:junos-ssl-term is not found in ssl-trace-new logs [PR1640075](#)
- Certificate-based VPN tunnel is not established [PR1655571](#)
- The crash files may be seen on SRX platforms [PR1655808](#)

## Unified Threat Management (UTM)

- New UTM Content-Filtering CLI is changing from seclog to log [PR1634580](#)
- Modification of Content-Filtering rule order after JunOS 21.4 would not have the desired effect. [PR1653488](#)

- Web browser traffic might get blocked when matched to the content-filtering rule with file-types 7z [PR1656266](#)

## VPNs

- IPsec tunnel might stop processing traffic [PR1636458](#)
- 22.4DCB-PCT:"ipsec tunnel-events-statistics" is not coming as expected while Verifying IPv4 Auto-VPN in point-to-multipoint mode using IKEv2 with DUT as spoke with latest DCB [PR1669110](#)

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 141](#)

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 22.1R2 for vSRX using J-Web (see [J-Web](#)) or the Junos Space Network Management Platform (see [Junos Space](#)).

Starting in Junos OS release 21.2R1, all Junos OS products which were previously running on FreeBSD 11.x based Junos OS are migrated to FreeBSD 12.x based Junos OS, except EX4400. Starting with Junos OS release 21.3R1, EX4400 platforms are migrated to FreeBSD 12.x based Junos OS.

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 22.1R2 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/eedebg_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 22.1R2 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-x86-64-22.1-2022-10-12.0_RELEASE_22.1_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-
x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING: This package will load JUNOS 22.1 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-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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-22.1-2022-10-12.0_RELEASE_22.1_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 22.1R2 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 22.1-2022-10-12.0_RELEASE_22.1_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: 22.1-2022-10-12.0_RELEASE_22.1_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 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](#).

## 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

- Self-Help Online Tools and Resources | 144
- Creating a Service Request with JTAC | 145

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/content/dam/www/assets/resource-guides/us/en/jtac-user-guide.pdf>.
- Product warranties—For product warranty information, visit <https://support.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://support.juniper.net/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://supportportal.juniper.net/s/knowledge>

- Download the latest versions of software and review release notes: <https://support.juniper.net/support/downloads/>
- Search technical bulletins for relevant hardware and software notifications: <https://supportportal.juniper.net/s/knowledge>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://supportportal.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://support.juniper.net/support/requesting-support/>
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

## Revision History

10 August 2023—Revision 4, Junos OS Release 22.1R2.

2 June 2023—Revision 3, Junos OS Release 22.1R2.

24 November 2022—Revision 2, Junos OS Release 22.1R2.

10 August 2022—Revision 1, Junos OS Release 22.1R2.

---

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2023 Juniper Networks, Inc. All rights reserved.