

Release Notes

Published
2024-08-08

Junos OS Release 23.1R1®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, QFX Series, SRX Series, vMX, vRR, and vSRX. These release notes accompany Junos OS Release 23.1R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

Table of Contents

Junos OS Release Notes for ACX Series

What's New | 1

Class of Service | 1

MPLS | 2

Routing Protocols | 3

VPNs | 3

Additional Features | 3

What's Changed | 4

Known Limitations | 5

Open Issues | 6

Resolved Issues | 7

Migration, Upgrade, and Downgrade Instructions | 9

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 9

Junos OS Release Notes for cRPD

What's New | 10

What's Changed | 11

Known Limitations | 11

Open Issues | 11

Resolved Issues | 11

Junos OS Release Notes for cSRX

What's New | 12

What's Changed | 12

Known Limitations | 12

Open Issues | 12

Resolved Issues | 13

Junos OS Release Notes for EX Series

What's New | 13

Hardware | 14

Authentication and Access Control | 25

Dynamic Host Configuration Protocol | 26

EVPN | 26

Interfaces | 28

J-Web | 28

Licensing | 28

VLANs | 28

Additional Features | 29

What's Changed | 30

Known Limitations | 31

Open Issues | 32

Resolved Issues | 34

Migration, Upgrade, and Downgrade Instructions | 38

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 38

Junos OS Release Notes for JRR Series

What's New | 40

Routing Policy and Firewall Filters | 40

What's Changed | 40

Known Limitations | 40

Open Issues | 41

Resolved Issues | 41

Migration, Upgrade, and Downgrade Instructions | 42

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 42

Junos OS Release Notes for Juniper Secure Connect

What's New | 44

VPNs | 44

What's Changed | 45

Known Limitations | 47

Open Issues | 47

Resolved Issues | 47

Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 48

What's Changed | 48

Known Limitations | 48

Open Issues | 49

Resolved Issues | 49

Migration, Upgrade, and Downgrade Instructions | 49

Junos OS Release Notes for Junos Fusion for Provider Edge

What's New | 55

What's Changed | 56

Known Limitations | 56

Open Issues | 56

Resolved Issues | 56

Migration, Upgrade, and Downgrade Instructions | 56

Junos OS Release Notes for MX Series

What's New | 66

EVPN | 67

High Availability | 69

Interfaces | 71

Junos Telemetry Interface | 72

Licensing | 73

MPLS | 74

Network Address Translation (NAT) | 75

Network Management and Monitoring | 76

Precision Time Protocol (PTP) | 77

Routing Protocols | 77

Securing GTP and SCTP Traffic | 79

Source Packet Routing in Networking (SPRING) or Segment Routing | 79

Subscriber Management and Services | 79

VPNs | 81

Additional Features | 81

What's Changed | 82

Known Limitations | 84

Open Issues | 87

Resolved Issues | 95

Migration, Upgrade, and Downgrade Instructions | 110

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 111

Junos OS Release Notes for NFX Series

What's New | 112

What's Changed | 113

Known Limitations | 113

Open Issues | 114

Resolved Issues | 115

Migration, Upgrade, and Downgrade Instructions | 115

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 116

Junos OS Release Notes for PTX Series | 117

Junos OS Release Notes for QFX Series

What's New | 117

Authentication and Access Control | 118

Dynamic Host Configuration Protocol | 118

EVPN | 119

Licensing | 119

Routing Policy and Firewall Filters | 120

Routing Protocols | 120

Virtual Chassis | 120

VPNs | 120

Additional Features | 121

What's Changed | 121

Known Limitations | 123

Open Issues | 124

Resolved Issues | 126

Migration, Upgrade, and Downgrade Instructions | 131

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 144

Junos OS Release Notes for SRX Series

What's New | 145

- Authentication and Access Control | 146
- Chassis Cluster-specific | 146
- Flow-based and Packet-based Processing | 146
- Intrusion Detection and Prevention | 146
- J-Web | 147
- Licensing | 149
- Network Address Translation (NAT) | 149
- Network Management and Monitoring | 149
- Securing GTP and SCTP Traffic | 151
- Software Installation and Upgrade | 151
- Content Security | 151
- VPNs | 152

What's Changed | 153**Known Limitations | 160****Open Issues | 161****Resolved Issues | 162****Migration, Upgrade, and Downgrade Instructions | 166**

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 167

Junos OS Release Notes for vMX**What's New | 168**

- EVPN | 168
- Interfaces | 169
- Junos Telemetry Interface | 170
- MPLS | 170

What's Changed | 171

Known Limitations | 172

Open Issues | 172

Resolved Issues | 173

Upgrade Instructions | 173

Junos OS Release Notes for vRR

What's New | 174

Routing Policy and Firewall Filters | 174

Routing Protocols | 174

What's Changed | 175

Known Limitations | 175

Open Issues | 175

Resolved Issues | 175

Junos OS Release Notes for vSRX

What's New | 176

Authentication and Access Control | 177

Chassis Cluster-specific | 177

Flow-based and Packet-based Processing | 177

Intrusion Detection and Prevention | 177

Network Management and Monitoring | 178

Platform and Infrastructure | 178

Content Security | 179

VPNs | 179

What's Changed | 180

Known Limitations | 187

Open Issues | 187

Resolved Issues | 188

Resolved Issues: 23.1R1 | **189**

Migration, Upgrade, and Downgrade Instructions | 189

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | **195**

Licensing | 196**Finding More Information | 197****Requesting Technical Support | 198****Revision History | 199**

Junos OS Release Notes for ACX Series

IN THIS SECTION

- [What's New | 1](#)
- [What's Changed | 4](#)
- [Known Limitations | 5](#)
- [Open Issues | 6](#)
- [Resolved Issues | 7](#)
- [Migration, Upgrade, and Downgrade Instructions | 9](#)

What's New

IN THIS SECTION

- [Class of Service | 1](#)
- [MPLS | 2](#)
- [Routing Protocols | 3](#)
- [VPNs | 3](#)
- [Additional Features | 3](#)

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

Class of Service

- **Hierarchical class of service (HCoS) support on AE and MCAE interfaces (ACX710)**—Starting in Junos OS Release 23.1R1, you can apply up to four levels of hierarchical traffic scheduling and shaping features to aggregated Ethernet (AE) and multicast AE (MCAE) interfaces on the ACX710 routers.

[See [Hierarchical Class of Service in ACX Series Routers](#).]

MPLS

- **OAM support for labeled IS-IS and labeled OSPF flex algo segment routing paths (ACX5448, ACX6360, and MX Series)**—Starting in Junos OS Release 23.1R1, Junos OS supports the following Operation, Administration, and Maintenance (OAM) capabilities for labeled IS-IS Flexible Algorithm (flex algo) segment routing paths:
 - IPv4 and IPv6 MPLS ping
 - IPv4 and IPv6 MPLS traceroute
 - Equal-cost multipath (ECMP) traceroute

Junos OS also supports IPv4 MPLS ping and IPv4 MPLS traceroute for labeled OSPF flex algo segment routing paths. The OAM functionality is used to detect data plane failures in segment routing paths for the purposes of fault detection and isolation.

To enable these OAM capabilities, we've introduced the `algorithm` option in the following commands:

- `ping mpls segment routing isis fec algorithm algorithm-id`
- `ping mpls segment routing ospf fec algorithm algorithm-id`
- `traceroute mpls segment routing isis fec algorithm algorithm-id`
- `traceroute mpls segment routing ospf fec algorithm algorithm-id`

[See [ping mpls segment routing isis](#), [ping mpls segment routing ospf](#), [traceroute mpls segment-routing ospf](#), and [traceroute mpls segment-routing isis](#).]

- **Enable TLS for PCEP sessions (ACX5448, ACX5448-D, ACX5448-M, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can enable Transport Layer Security (TLS) in a Path Computation Client (PCC) to establish a TCP connection with the Path Computation Element (PCE). This connection creates a secure Path Computation Element Protocol (PCEP) session to transport PCEP messages.

To enable TLS in a PCC process (PCCD) and to establish a PCEP session, set the `tls-strict` configuration statement at the `[edit protocols pcep]` hierarchy level.

[See [Enabling Transport Layer Security for PCEP Sessions](#).]

- **Support to report path optimization and computed metrics in PCEP (ACX710, ACX5448, ACX5448-M, ACX5448-D, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, we report PCEP path optimization metrics (IGP, TE, and delay) for RSVP and segment routing-traffic engineering (SR-TE) label-switched paths (LSPs).

To configure the interior gateway protocol (IGP), traffic engineering, and path delay optimization metrics for RSVP LSPs, include the metric-type `igp/te/delay/delay minimum` CLI statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level.

To configure the optimization metrics for SR-TE LSPs, include the metric-type `igp/te/delay/delay minimum` CLI statement at the [edit protocols source-packet-routing compute-profile *compute-profile-name*] hierarchy level.

[See [Reporting Path Optimization Metrics in PCEP](#).]

Routing Protocols

- **Support for BGP-LS NLRI to carry confederation ID (ACX710, ACX5448, MX10003, QFX5120-48YM, QFX5200, and QFX5210, and vRR)**—Starting in Junos OS Release 23.1R1, Junos OS enables BGP Link State (BGP-LS) network layer reachability information (NLRI) to carry the confederation ID in TLV 512 when BGP confederation is enabled. The NLRI carries the confederation ID along with the member autonomous system number (AS number) in TLV 517 as defined in RFC 9086. In releases before Junos OS Release 23.1R1, BGP-LS NLRI carries only the member AS number in TLV 512 and the confederation ID is not encoded in the `Isdist.0` routing table.

[See [Link-State Distribution Using BGP Overview](#).]

VPNs

- **Support for native IPv6 in carrier-of-carrier VPNs (ACX Series, MX Series, and QFX Series)**—Starting in Junos OS Release 23.1R1, you can configure LDP and IGPs using IPv6 addressing to support carrier-of-carriers VPNs. Junos OS supports native IPv6 prefix exchanges in the carrier-of-carriers deployments.

[See [Carrier-of-Carriers VPNs, LDP Native IPv6 Support Overview](#), and [LDP Configuration](#).]

Additional Features

Support for the following features has been extended to these platforms.

- **OpenConfig authentication, authorization, and accounting (AAA) configuration support** (ACX5448, ACX5448-M, ACX5448-D, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, and EX9214)

[See [Mapping OpenConfig AAA Commands to Junos Operation](#).]

What's Changed

IN THIS SECTION

- [General Routing | 4](#)
- [EVPN | 4](#)
- [Network Management and Monitoring | 5](#)

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

General Routing

- When subscribing to the resource path `/junos/system/linecard/environment`, the prefix for the streamed path at the collector side was displaying as `/junos/linecard/environment`. This issue is resolved in Junos OS 23.1R1 and Junos OS Evolved 23.1R1 and the subscription path and the streamed path match to display `/junos/system/linecard/environment`.

EVPN

- Flow-label configuration status for EVPN ELAN services The output for the `show evpn instance extensive` command now displays the flow-label and flow-label-static operational status for a device and not for the routing instances. A device with `flow-label` enabled supports flow-aware transport (FAT) flow labels and advertises its support to its neighbors. A device with `flow-label-static` enabled supports FAT flow labels but does not advertise its capabilities.
- Specify the UDP source port in a ping overlay or traceroute overlay operation — In Junos OS releases prior to 22.4R1, you could not configure the `udp` source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other `hash-*` options that may be used to determine the source port value.

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the `get-system-yang-packages` RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `get-system-yang-packages` RPC reply replaces the `xmlproxy-yang-modules` tag with the `proxy-xml-yang-modules` tag in the XML output.
- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is `error` instead of `warning`, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

Known Limitations

There are no known limitations in hardware or software in this release for ACX Series routers.

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

Open Issues

IN THIS SECTION

- [General Routing](#) | 6

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

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

General Routing

- On all ACX platforms, the hosts will not receive multicast traffic when snooping is configured in a EVPN-MPLS (Ethernet Virtual Private Network - Multiprotocol Label Switching) enabled broadcast domain. [PR1613462](#)
- On all Junos OS platforms, incorrect sensor base telemetry data are collected when multiple SR-TE tunnels are configured with at least one uncolored, sharing the same single hop segment list. [PR1665943](#)
- The Queue statistics might show constant PPS / bps after interface is disabled. The statistics does not increment and remain same when the interface went down. [PR1685344](#)
- Reserved buffers might be shown as 0, but internally reserved buffers do get used to queue and transmit traffic on the queue. [PR1689183](#)
- The aggregate Ethernet statistics might show 0 bps for output traffic. It is a CLI output display issue. It does not impact the traffic output. [PR1689185](#)
- dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. [PR1692400](#)
- Convergnace time can be more than 60ms for OSPF TILFA Node protection testing. [PR1695292](#)
- FIPS mode is not supported in this release for SRXSME devices. [PR1697999](#)
- On Junos OS ACX5048 and ACX5096 platforms, if the link-speed is configured under the aggregated-ether-options hierarchy of the Aggregated Ethernet (AE) interface and the link-speed value does not match with the member link-speed, the member interface will not be added to the AE bundle. [PR1713699](#)

Resolved Issues

IN THIS SECTION

- [General Routing | 7](#)
- [Interfaces and Chassis | 8](#)
- [Routing Protocols | 9](#)

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

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

General Routing

- Delegated BFD sessions configured on routing-instance might fail to come up. [PR1633395](#)
- For ACX5448 device, if a non-default ssh port is configured for system login, after upgrade to 21.4 release, the FPC is stuck in offline. [PR1660446](#)
- Na-grpcd process core observed in telemetry services. [PR1665516](#)
- Inline BFDv6 sessions might go DOWN and stay in that state on ACX5448 and ACX710 devices. [PR1666746](#)
- Traffic loss is observed when the VRRP is configured over the aggregate Ethernet interface. [PR1666853](#)
- New BFD sessions will not come up on ACX5448 and ACX710 devices due to continuous flaps. [PR1670684](#)
- The LLDP packets will not be transmitted over I2circuit on the ACX platform. [PR1678752](#)
- Memory leak is seen on ACX710/5448 when the core link flaps. [PR1681980](#)
- The traffic drop would be observed with inter-vlan configuration when deactivating and activating the EVPN routing instance. [PR1683321](#)

- On Junos OS ACX platforms the IP packets with VLAN tags do not get a response when sent out on the IRB interface in a certain condition. [PR1683770](#)
- ACX5448:ACX710 L2Circuit traffic drop with control-word enabled or control-word configuration change. [PR1683900](#)
- ACX710 : Auto-mdix is not working in ACX710. [PR1685431](#)
- Traffic null route during l2circuit pseudowire redundancy neighbor switchover. [PR1686260](#)
- The subscriber-management-helper is thrashing, not restarted, messages seen on ACX5448. [PR1688107](#)
- The jdchpd core seen with dhcp-snooping persistent configuration. [PR1688644](#)
- The LACP would get stuck in a continuous update loop in the MC-LAG scenario. [PR1688958](#)
- EVPN packets might go to incorrect queues due to the wrong classification and might lead to packets drop during congestion. [PR1689604](#)
- Packet forwarding fails on specific ACX Junos OS platforms due to flapping of core interface member link in the MPLS-EVPN environment. [PR1690590](#)
- PCS errors and framing errors on 100GE interfaces on certain Junos OS platforms. [PR1692063](#)
- [interface] [acx_ifd] ACX7100-48L :: 400g-ZR-M link is not up between storm-01 and wolverine-01 due to **Optics Over Temperature Shutdown**. [PR1698342](#)
- On ACX5448 devices, an interface with SFP-T optic set to 100m and auto-negotiation disabled will remain down after reboot or on chassis-control restart. [PR1702239](#)
- CoS rewrite rules will not work in L3VPN scenario. [PR1703840](#)
- SNMP MIB OID output showing wrong temperature value if device running under negative temperature. [PR1717105](#)

Interfaces and Chassis

- Incompatible or unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. [PR1692404](#)

Routing Protocols

- Wrong SR-TE secondary path weight makes the secondary path active in forwarding table.
[PR1696598](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 9

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

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

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

We have two types of releases, EOL and EEOL:

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence,

you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 1: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for cRPD

IN THIS SECTION

- [What's New | 10](#)
- [What's Changed | 11](#)
- [Known Limitations | 11](#)
- [Open Issues | 11](#)
- [Resolved Issues | 11](#)

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

Learn about the issues fixed in this release for cRPD.

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

Routing Protocols

- Traffic blackholing is observed when removing the BGP routes take a long time to get removed from RIB. [PR1695062](#)
- The changes in script /usr/sbin/rpd-helper for sysctl returns an error while starting up the rpd-helper. [PR1707633](#)

Junos OS Release Notes for cSRX

IN THIS SECTION

- [What's New | 12](#)
- [What's Changed | 12](#)
- [Known Limitations | 12](#)
- [Open Issues | 12](#)
- [Resolved Issues | 13](#)

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 | 13](#)
- [What's Changed | 30](#)
- [Known Limitations | 31](#)
- [Open Issues | 32](#)
- [Resolved Issues | 34](#)
- [Migration, Upgrade, and Downgrade Instructions | 38](#)

What's New

IN THIS SECTION

- [Hardware | 14](#)
- [Authentication and Access Control | 25](#)
- [Dynamic Host Configuration Protocol | 26](#)
- [EVPN | 26](#)

- [Interfaces | 28](#)
- [J-Web | 28](#)
- [Licensing | 28](#)
- [VLANs | 28](#)
- [Additional Features | 29](#)

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

Hardware

- **New extension module (EX4400)**—Starting in Junos OS Release 23.1R1, EX4400 switches support the new 1x100GbE QSFP28 extension module (model number: EX4400-EM-1C).

The extension module supports Media Access Control Security (MACsec) with AES-256 encryption.

You can install one 40GbE QSFP+ transceiver or one 100GbE QSFP28 transceiver in the extension module. You can channelize the port on the extension module to support 10-Gbps and 25-Gbps speeds by using a breakout cable.

See [EX4400 Switch Hardware Guide](#).

- **New EX4400 switch model (EX Series)**—In Junos OS Release 23.1R1, we introduce the new EX4400-24X model of the EX4400 Switch. The EX4400-24X model has 24 1GbE/10GbE SFP/SFP+ ports on the front panel and two 100GbE QSFP28 ports on the front panel. The model supports 550-W AC or 550-W DC power supplies and front-to-back or back-to-front airflow directions.

EX4400 switches are our first cloud-ready switches. You can deploy EX4400 switches in cloud networks and manage them by using Juniper Mist Wired Assurance.

The EX4400 switches provide connectivity for high-density environments and scalability for growing networks. Typically, you use EX4400 switches in large branch offices, campus wiring closets, and data centers. In data centers, you can position EX4400 switches as top-of-rack switches to provide connectivity for all devices in the rack.

EX4400 switches support channelization (see [Port Settings](#)).

To install the EX4400 switch hardware and perform initial software configuration, routine maintenance, and troubleshooting, see [EX4400 Switch Hardware Guide](#). See [Feature Explorer](#) for the complete list of features for any platform.

Table 2: Features Supported by the EX4400-24X

Feature	Description
Authentication and Access Control	<ul style="list-style-type: none">• Support for 802.1X authentication. [See 802.1X Authentication.]• Support for captive portal authentication. [See Captive Portal Authentication.]
Chassis	<ul style="list-style-type: none">• Software support for platform infrastructure, fan, and power management.• Support for Cloud LED (CLD). [See EX4400 Chassis.]
Class of Service	<ul style="list-style-type: none">• Support for class-of-service (CoS) configuration. [See Class of Service User Guide (EX Series Switches Except EX4600 and EX9200 Switches).]

Table 2: Features Supported by the EX4400-24X (Continued)

Feature	Description
EVPN	<ul style="list-style-type: none"> • Support for the following Layer 2 VXLAN gateway features in an EVPN-VXLAN network: <ul style="list-style-type: none"> • Active/active multihoming • Proxy Address Resolution Protocol (ARP) usage and ARP suppression, and Neighbor Discovery Protocol (NDP) usage and NDP suppression on interfaces without integrated routing and bridging • Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding <p>[See EVPN Feature Guide.]</p> • Support for Layer 2 VXLAN gateway services in an EVPN-VXLAN network: <ul style="list-style-type: none"> • 802.1X authentication, accounting, central Web authentication (CWA), and captive portal • Class of service • DHCPv4 and DHCPv6 snooping, dynamic ARP inspection (DAI), neighbor discovery inspection, IP source guard and IPv6 source guard, and router advertisement (RA) guard (no multihoming) • Firewall filters and policing • Storm control, port mirroring, and MAC filtering <p>[See EVPN Feature Guide.]</p> • Support for the following Layer 3 VXLAN gateway features in an EVPN-VXLAN network: <ul style="list-style-type: none"> • Default gateway using IRB interfaces to route traffic between VLANs • IPv6 data traffic routing through an EVPN-VXLAN overlay network with an IPv4 underlay

Table 2: Features Supported by the EX4400-24X (Continued)

Feature	Description
	<ul style="list-style-type: none"> • EVPN pure Type 5 routes <p>The Virtual Chassis doesn't support EVPN-VXLAN multihoming, but you can use the standalone switch as an EVPN-VXLAN provider edge (PE) device in multihoming use cases.</p> <p>[See EVPN Feature Guide.]</p> <ul style="list-style-type: none"> • Support for VXLAN-GBP—The EX4400-24X model supports the existing Layer 3 VXLAN network identifiers (VNI) in conjunction with firewall filter policies to provide microsegmentation at the level of a device or a tag, independent of the underlying network topology. IoT devices, for example, typically need access to only specific applications on the network. Group-based policy (GBP) keeps this traffic isolated by automatically applying security policies without the need for Layer 2 (L2) or L3 lookups or access control lists (ACLs). <p>[See Example: Micro and Macro Segmentation using Group Based Policy in a VXLAN.]</p>
High Availability and Resiliency	<ul style="list-style-type: none"> • Support for high availability includes nonstop software upgrade (NSSU), GRES, nonstop bridging (NSB), and nonstop active routing (NSR). <p>[See High Availability User Guide.]</p> <ul style="list-style-type: none"> • Resiliency support for inter-integrated controller (I2C), disk failure, and disk health. <p>[See High Availability User Guide.]</p>

Table 2: Features Supported by the EX4400-24X (Continued)

Feature	Description
Interfaces	<ul style="list-style-type: none"> • Network interfaces support— Support for the following features: <ul style="list-style-type: none"> • 24x10G SFP fixed ports • 2x100G network ports, which can be converted to VC ports and vice versa • 4x25G modular uplink with VC port conversion support • 4x10G modular uplink • 1x100G modular uplink with VC port conversion support • OAM based resiliency • Supported transceivers, optical interfaces, and DAC cables— Select your product in the Hardware Compatibility Tool to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the tool and provide the first supported release information when the optic becomes available.
Junos Telemetry Interface	<ul style="list-style-type: none"> • Flow-based telemetry, inline monitoring services, and secure packet capture to the cCloud using Junos telemetry interface (JTI). <p>[See Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface), Flow-Based Telemetry (EX4100, EX4100-F, and EX4400 Series), Inline Monitoring Services Configuration, and Telemetry Sensor Explorer.]</p>

Table 2: Features Supported by the EX4400-24X *(Continued)*

Feature	Description
Layer 2 features	<ul style="list-style-type: none"> • Support for the following Layer 2 features: <ul style="list-style-type: none"> • Bridge protocol data unit (BPDU) protection • Ethernet ring protection switching (ERPS) • IEEE 802.1p • Resilient hashing on LAGs • Layer 3 VLAN-tagged subinterfaces • LLDP (IEEE 802.1AB) • Loop protection • MAC address accounting • MAC address aging • MAC address filtering • Disable MAC learning • Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s) • Multiple VLAN Registration Protocol (MVRP) (IEEE 802.1ak) • Persistent MAC (sticky MAC) • Per VLAN MAC learning (limit) • Port-based VLAN • Proxy ARP • Redundant trunk group (RTG) • Root protection • Routed VLAN interface (RVI)

Table 2: Features Supported by the EX4400-24X (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) • Static and dynamic link aggregation with LACP (fast and slow LACP) • Static MAC address assignment for interface • Storm control • STP (IEEE 802.1D) • Uplink failure detection • VLAN • VLAN—IEEE 802.1Q VLAN trunking • VSTP <p>[See Ethernet Switching User Guide, Security Services Administration Guide, and Spanning-Tree Protocols User Guide.]</p>

Table 2: Features Supported by the EX4400-24X (*Continued*)

Feature	Description
Layer 3 features	<ul style="list-style-type: none"> • Support for the following Layer 3 features: <ul style="list-style-type: none"> • 32-way ECMP • BFD (for RIP, OSPF, IS-IS, BGP, and PIM) • BGP 4-byte ASN support • BGP Add Path (BGP-AP) • Filter based forwarding (FBF) • IP directed broadcast traffic forwarding • IPv4 BGP • IPv4 multiprotocol BGP (MBGP) • IPv4 over GRE • IPv6 BGP • IPv6 CoS (BA, classification and rewrite, scheduling based on traffic class) • IPv6 IS-IS • IPv6 Neighbor Discovery Protocol (NDP) • IPv6 OSPFv3 • IPv6 ping • IPv6 stateless auto-configuration • IPv6 static routing • IPv6 traceroute • IS-IS • OSPFv2

Table 2: Features Supported by the EX4400-24X (*Continued*)

Feature	Description
	<ul style="list-style-type: none"> • Path MTU discovery • RIPv2 • Static routing • Unicast reverse path forwarding (unicast RPF) • Virtual router for IS-IS, RIP, OSPF, and BGP • Virtual Router Redundancy Protocol (VRRP) • VRRPv3 <p>[See High Availability User Guide, BGP User Guide, Routing Policies, Firewall Filters, and Traffic Policers User Guide, IS-IS User Guide, Security Services Administration Guide, and OSPF User Guide.]</p>
Multicast features	<ul style="list-style-type: none"> • Support for the following multicast features: <ul style="list-style-type: none"> • IGMP snooping • IGMP: version 1 through version 3 • Multicast Listener Discovery (MLD) snooping • PIM-SM, PIM-SSM, PIM-DM <p>[See Multicast Protocols User Guide.]</p>

Table 2: Features Supported by the EX4400-24X (Continued)

Feature	Description
Network Management and Monitoring	<ul style="list-style-type: none"> Support for the following Ethernet OAM link fault management (LFM) and CFM features: <ul style="list-style-type: none"> Monitor faults by using the continuity check message (CCM) protocol to discover and maintain adjacencies at the VLAN or link level. Discover paths and verify faults by using the Link Trace Message (LTM) protocol to determine the path taken from an endpoint to a destination MAC address. Isolate faults by using loopback messages. <p>[See Ethernet OAM and CFM for Switches and OAM Link Fault Management.]</p> <ul style="list-style-type: none"> Support for local and remote port mirroring, and remote port mirroring to an IP address (GRE encapsulation). <p>[See Port Mirroring and Analyzers.]</p> <ul style="list-style-type: none"> Support for the sFlow network monitoring technology. <p>[See sFlow Monitoring Technology.]</p> <ul style="list-style-type: none"> Support for Juniper Mist Wired Assurance—You can automatically onboard and provision Juniper Networks EX4400 switches to the Juniper Mist cloud by using a single activation code. Juniper Mist Wired Assurance provides automated operations. It also enables the use of service-level expectations (SLEs) for IoT devices, Juniper access points driven by Mist AI, and other network devices. <p>[For an overview of Juniper Mist Wired Assurance and deployment instructions, see Cloud-Ready Switches with Mist and Overview of EX Series Switches and the Juniper Mist Cloud.]</p>
Precision Time Protocol	<ul style="list-style-type: none"> Support for Precision Time Protocol (PTP) transparent clock. <p>[See PTP Transparent Clocks.]</p>

Table 2: Features Supported by the EX4400-24X (*Continued*)

Feature	Description
Routing Policies and Firewall Filters	<ul style="list-style-type: none"> Support for firewall filters and policers. <p>[See Firewall Filters Overview.]</p>
Security	<ul style="list-style-type: none"> Support for Media Access Control Security (MACsec) with 256-bit cipher suite. <p>[See Understanding Media Access Control Security (MACsec).]</p> <ul style="list-style-type: none"> Support for distributed denial-of-service (DDoS) protection. <p>[See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]</p> <ul style="list-style-type: none"> Support for the following port security features: <ul style="list-style-type: none"> DHCP snooping (IPv4 and IPv6) Dynamic ARP inspection (DAI) IPv6 neighbor discovery inspection <p>[See Security Services Administration Guide.]</p>

Table 2: Features Supported by the EX4400-24X (Continued)

Feature	Description
Software Installation and Upgrade	<ul style="list-style-type: none"> • Support for secure boot. The implementation is based on the UEFI 2.4 standard. [See Software Installation and Upgrade Guide.] • Support for phone-home client (PHC). The PHC can securely provision an EX4400 Virtual Chassis without requiring user interaction. [See Provision a Virtual Chassis Using the Phone-Home Client.] • Support for zero-touch provisioning (ZTP). Zero-touch provisioning enables you to install or upgrade the software on your device with minimal manual intervention. [See Zero Touch Provisioning.] • Support for DHCP option 43 suboption 8 to provide proxy server information in a PHC. During the bootstrapping process, the PHC can access the redirect server or the phone-home server (PHS) through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]
Virtual Chassis	<ul style="list-style-type: none"> • Support for Virtual Chassis—EX4400-24X switches support Virtual Chassis formation in the HGoE mode. You can connect up to 10 EX4400-24X/EX4400 switches in a Virtual Chassis and manage them as a single device. [See EX4400 Switches in a Virtual Chassis.]

Authentication and Access Control

- **802.1X MAC RADIUS authentication with global password (EX Series except EX4300 and QFX Series that support 802.1X authentication)**—In earlier releases, you used the client's media access control (MAC) address as the username and the password for MAC RADIUS authentication. Starting in Junos OS Release 23.1R1, you can configure a global password for all the MAC RADIUS

authentication sessions by using the password *password-string* configuration statement at the [edit protocols dot1x authenticator mac-radius] hierarchy level.

[See [Configuring MAC RADIUS Authentication \(CLI Procedure\)](#) and [password \(MAC RADIUS Authentication\)](#).]

Dynamic Host Configuration Protocol

- **Additional client options from DHCP snooping (EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS Release 23.1R1, you can configure DHCP snooping to collect additional client options such as the hostname, server ID, and client ID. The additional client options can be used for analytics using Juniper Mist Cloud Services.

To configure DHCP snooping to collect additional client options, use the `mine-dhcp-client-options` and `mine-dhcpv6-client-options` (for DHCPv6) configuration statements at the [edit vlans *vlan-name* forwarding-options dhcp-security] hierarchy level.

To view the DHCP client options along with other binding information, use the `show dhcp-security binding detail` and `show dhcp-security ipv6 binding detail` (for DHCPv6) operational commands.

[See [dhcp-security](#), [mine-dhcp-client-options](#), [mine-dhcpv6-client-options](#), [show dhcp-security binding](#), and [show dhcp-security ipv6 binding](#).]

EVPN

- **IPv4 multicast with IGMPv3 and IPv6 multicast with MLDv1 and MLDv2 in EVPN-VXLAN—centrally routed bridging overlay fabrics (EX4300-48MP, EX4400-48MP, EX4400-24MP, EX4400-48P, EX4400-48T, EX4400-24P, EX4400-24T, EX4400-48F)**—Starting in Junos OS Release 23.1R1, you can configure multicast with Internet Group Management Protocol version 3 (IGMPv3) and Multicast Listener Discovery versions 1 (MLDv1) and 2 (MLDv2) in an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) centrally routed bridging (CRB) overlay fabric. With this feature, you can enable multihoming for the following IPv4 and IPv6 multicast traffic use cases:

- Intra-VLAN forwarding
- Inter-VLAN routing

IGMPv3 or MLD multicast works with these multicast optimizations:

- IGMP or MLD snooping
- Selective multicast Ethernet tag (SMET) forwarding

- Assisted replication (AR)

These devices process:

- MLDv1 reports as any-source multicast (ASM) (*,G) reports
- MLDv2 reports in one of these modes:
 - Any-source multicast (ASM) (*,G) reports by default
 - Source-specific multicast (SSM) (S,G) reports (only if you explicitly configure this mode)

These devices process IGMPv3 reports in one of two modes:

- Any-source multicast (ASM) (*,G) reports by default
- Source-specific multicast (SSM) (S,G) reports when you explicitly configure this mode

[See [Overview of Multicast Forwarding with IGMP Snooping or MLD Snooping in an EVPN-VXLAN](#), [Overview of Selective Multicast Forwarding](#), [Assisted Replication Multicast Optimization in EVPN Networks Environment](#), and [evpn-ssm-reports-only](#).]

- **Determine IRB interface state changes based on local and remote connectivity states in EVPN fabrics (EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX2010, MX2020, vMX, QFX5110, QFX5120-48T, QFX5120-48Y, QFX5210, QFX10002, QFX10002-60, and QFX10008)**—Starting in Junos OS Release 23.1R1, the provider edge (PE) devices in an EVPN fabric consider the following factors when determining the state (up or down) of an L3 integrated routing and bridging (IRB) interface. These factors apply to an L3 IRB interface that is associated with a bridge domain or a VLAN in an EVPN instance (EVI).

- Associated local L2 interface states

To customize the L2 interface name and other parameters that the device uses to compute the IRB interface state, configure the `interface-state` statement at the `[edit interfaces irb unit n]` hierarchy.

- Remote provider edge (PE) device reachability based on the network isolation state of the bridge domain or the EVI

The device includes the states of the associated EVPN overlay tunnel interfaces in the network isolation state evaluation.

To define the parameters that determine when an EVI or a bridge domain is in a network isolation state:

1. Configure the network-isolation group `group-name` statement at the `[edit protocols]` hierarchy level to define a network isolation profile using the available options.

2. Assign the network isolation group profile to a bridge domain or an EVI using the `network-isolation-profile group network-isolation-group-name` statement at these hierarchy levels:

- Bridge domain—[edit bridge-domain *bd-name* bridge-options]
- EVI—[edit routing-instance *instance-name* switch-options]

[See [Determine IRB Interface State Changes from Local and Remote Connectivity States in EVPN Fabrics](#), [interface-state](#), and [network-isolation](#).]

Interfaces

- **New extension module (EX4400)**—Starting in Junos OS Release 23.1R1, we support a new 1x100GbE QSFP28 extension module (model number: EX4400-EM-1C). The extension module port can act both as a network port or a Virtual Chassis port (VCP). The module can support MACsec AES256 in network port mode. You can also channelize the extension module to support 4x25 GbE and 4x10 GbE. Channelization is not supported on VCP port.

[See [Channelizing Interfaces on EX4400 Switches](#) and [Port Speed](#).]

J-Web

- **Support for EX4400-24X switches (EX Series)**—Starting in Junos OS Release 23.1R1, you can configure, monitor, and manage EX4400-24X switches using J-Web. To configure the EX4400-24X switch, you must connect the Ethernet cable from the PC's Ethernet port to the port labeled **MGMT** on the switch's front panel. The chassis viewer on the Dashboard page supports both the standalone device view and the Virtual Chassis configuration view (graphical view of each member switch).

[See [Dashboard for EX Series Switches](#) and [Connecting and Configuring an EX Series Switch \(J-Web Procedure\)](#).]

Licensing

- **Support to trigger license alarm at configured time interval (EX Series, MX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 23.1R1, you can set the time interval at which you want to trigger alarms for features or capacity that do not have licenses installed.

To set the alarm log frequency, use the command `log-frequency` in the `set system license` hierarchy.

[See [Managing Licenses](#).]

VLANs

- **Exclusive VoIP MAC address support (EX2300-MP, EX2300-C, EX2300-VC, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 23.1R1, Enhanced Layer 2 Software (ELS) access

switches support learning MAC addresses for specific interfaces exclusively in the VoIP VLAN. With this feature enabled, MAC addresses for the specified interface will not be learned on a data VLAN, and any MAC address that had been previously learned on a data VLAN will be removed.

To configure this feature on an interface, use the `voip-mac-exclusive` statement at the `[edit switch-options voip interface name]` hierarchy level.

[See [VoIP on EX Series Switches](#).]

Additional Features

Support for the following features has been extended to these platforms.

- **MACsec on logical interfaces (EX9208).**

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

- **MACsec with 256-bit cipher suite (EX4400).**

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

- **OpenConfig authentication, authorization, and accounting (AAA) configuration support (ACX5448, ACX5448-M, ACX5448-D, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4300VC, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4600-VC, EX4650, EX4650-48Y-VC, EX9204, EX9208, and EX9214)**

[See [Mapping OpenConfig AAA Commands to Junos Operation](#).]

- **On-box monitoring support on the control plane (EX Series, QFX Series, and SRX Series)**—The memory monitoring system monitors the system memory and raises a major or minor alarm using the `set system monitor memory system alarm` command statement on the devices. The alarm is raised when the device is running low on memory.

[See [Memory \(System\)](#).]

- **Supported transceivers, optical interfaces, and DAC cables**—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and direct attach copper (DAC) cables for your platform or interface module. We update the tool and provide the first supported release information when the optic becomes available.
- **Support for PTP transparent clock (EX4400-EM-1C)**—The transparent clock computes the variable delay as the Precision Time Protocol (PTP) packets pass through the switch or the router. The client clock can use this information to account for a delay due to queuing or buffering.

The uplink module does not support the PTP transparent clock if the EX4400 chassis is on the Virtual Chassis mode.

[See [PTP Transparent Clocks](#).]

- **Support for platform infrastructure, fan and power management (EX4400-24X devices)** – [See [EX440 Hardware Guide](#).]

What's Changed

IN THIS SECTION

- [Network Management and Monitoring](#) | 30

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

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the `get-system-yang-packages` RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `get-system-yang-packages` RPC reply replaces the `xmlproxy-yang-modules` tag with the `proxy-xml-yang-modules` tag in the XML output.

- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

Known Limitations

IN THIS SECTION

- [EVPN | 31](#)
- [General Routing | 31](#)
- [Virtual Chassis | 32](#)

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

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

EVPN

- **EVPN-VXLAN:** After RE switchover, a momentary traffic loss may be observed with EVPN VxLAN on EX4400 switches. [PR1659315](#)

General Routing

- **MVRP on PVLAN promiscuous port** is not supported. If you configure MVRP on promiscuous port, then hosts connected to secondary VLAN ports will not be able to reach external world through promiscuous port carrying primary VLAN tags. [PR1693345](#)

- There is increase in memory footprint across different demons after an image upgrade resulting increase in the system memory. [PR1694522](#)

Virtual Chassis

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

Open Issues

IN THIS SECTION

- [General Routing | 32](#)
- [Platform and Infrastructure | 33](#)
- [Virtual Chassis | 34](#)

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

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

General Routing

- runt, fragment and jabber counters are not incrementing on EX4300-MPs. [PR1492605](#)
- When launching a guest virtual machine to run a third party application on Junos OS Release 15.1R1 and later, the guest VM show as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. [PR1529596](#)
- On EX2300, EX3400, EX4300-48MP, and EX4300, pause frame counters does not get incremented when pause frames are sent. [PR1580560](#)

- On the EX4600 device with SFP-LX10/SFP-SX, after a power cycle or software reboot, all ports are initialized and links are up with auto-negotiation enabled. Few ports are up and traffic flow whereas a few ports are up but no traffic flows through them. [PR1672583](#)
- On enabling MVRP on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch. [PR1686596](#)
- Factory reset and mode button on the far right side of the front panel is used to toggle the status LED to show the different port parameters for the network ports. You can tell which port parameter is indicated by the status LED by looking at which port status mode LED (SPD, DX, EN, and PoE) is lit. Factory reset/mode button will be unable to toggle status mode LED (SPD, DX, EN, and PoE). [PR1687407](#)
- When a sfp is unplugged or plugged in, it might not be recognized. [PR1696444](#)
- On all Junos OS and Junos OS Evolved platforms supporting MACsec, traffic drop can be seen when MACsec primary and fallback sessions are configured and there is a higher transmit-delay time of approximately 6 seconds. This is a timing issue and occurs when switching from primary to fallback or vice-versa when changing the pre-shared-key's connectivity association key (CAK) value in the CLI on the non-key-server side and at the same time key-server generates a new Secure Association Key (SAK) for pre-shared-key due to expiration of sak-rekey timer, that is, sak-rekey and primary to fallback key-switch both occurs at the same time. This issue is self-recovered once the SAK from fallback is recovered. [PR1698687](#)
- On 1G speed ethernet, auto-negotiation is responsible for exchanging Remote-fault and additional capability options (Pause etc) between link partners. So any link failure (Rx LOS) will not be reported to the peer link via Remote-fault if it configures without auto-negotiation / speed 1g. In such situation, the link on local side goes down, but the link on far end keeps Up, which will cause traffic blackhole. Configuring auto-negotiation explicitly under gigether-options is recommended to avoid traffic blackhole. [PR1705461](#)
- In a Virtual Chassis scenario, sometimes the alarms raised on the line-card or backup Routing Engine might not show on the master. [PR1707798](#)

Platform and Infrastructure

- On EX4300 platform, when you configure the encapsulation ethernet-bridge statement, the interface get programmed as trunk instead of access in VLAN membership. This leads to untagged traffic drop. [PR1665785](#)
- On EX4300-Virtual Chassis platforms, Packet Forwarding Engine process (pfex) crashes when physical interface card 2 (PIC 2) is detached. This deletes the physical interface before the logical interface get deleted. [PR1680225](#)

Virtual Chassis

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

Resolved Issues

IN THIS SECTION

- [Forwarding and Sampling | 34](#)
- [General Routing | 35](#)
- [Interfaces and Chassis | 37](#)
- [Layer 2 Ethernet Services | 37](#)
- [Platform and Infrastructure | 37](#)
- [Routing Protocols | 37](#)
- [Virtual Chassis | 38](#)

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

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

Forwarding and Sampling

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

General Routing

- DHCP packets getting looped in EVPN-VXLAN setup. [PR1657597](#)
- EX4100 MACsec interface statistics of encrypted or decrypted bytes do not increment further after reaching a 40-bit limit (1099511627775). [PR1658584](#)
- The fxpc crash might be observed with the RPF check enabled. [PR1662508](#)
- Shaping-rate is not taking 20 bytes of overhead into account. [PR1667879](#)
- EX4100 and EX4100-F series: On device reboot in scaled PoE scenario with perpetual PoE configured, it takes some time (a few minutes) for the CLI to reflect the correct status for LLDP enabled ports. [PR1671311](#)
- The vmcore might be seen with the back-to-back reboot. [PR1672731](#)
- Aggregated Ethernet interface will receive unknown unicast traffic on FPC3 reboot of a VC. [PR1678430](#)
- On EX2300 and EX3400, set system ports console log-out-on-disconnect does not allow user to log in via console. [PR1680408](#)
- Multicast traffic loss is seen with igmp-snooping running on EX4100. [PR1681478](#)
- On EX4100-24mp, EX4100-48mp, EX4100-48p, EX4100-48t, EX4100-24p, and EX4100-24t line of switches, the LED activity is lit on some ports if 1G optic is inserted without link being present or up. [PR1682633](#)
- EX Series switches SNMP: jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. [PR1683753](#)
- EX4100 and EX4100-F series: The secondary console (USB-C type) does not show the boot logs. [PR1684032](#)
- The l2cpd process might crash when disabling RSTP on an interface. [PR1684072](#)
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an agile licensing-based release. [PR1684842](#)
- MAC address learning might not happen on specific EX Series and QFX Series platforms. [PR1685938](#)
- The l2ald core file is seen after zeroizing. [PR1686097](#)
- EX4100 and EX4100-F series: On configuring console logout-on-disconnect, password configuration via console does not work. [PR1686364](#)

- EX4300-48MP Factory Reset/Mode button cannot toggle status mode LED (SPD, DX, EN, and PoE). [PR1687407](#)
- EX4400 SNMP: Removing or inserting the Fan tray or PIC will not generate the FRU removal or insertion trap. [PR1687848](#)
- FPC will crash when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregated Ethernet interfaces. [PR1688455](#)
- jdchpd core file is generated with dhcp-snooping persistent configuration. [PR1688644](#)
- On EX4100 and EX4400 platform, alarm 'PEM is not supported' might be seen. [PR1690674](#)
- The factory default config does not have xe-0/2/0. [PR1691174](#)
- Few uplink ports of EX2300-48MP are not coming up. [PR1692579](#)
- The dot1x reauthentication will not work for a port with VoIP VLAN. [PR1693640](#)
- PFE will crash on all QFX5K and EX4600 line of switching platforms with L2PT configuration. [PR1694076](#)
- On a PVLAN with DAI ARP, packets are forwarded between isolated ports. [PR1694800](#)
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. [PR1695057](#)
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. [PR1696428](#)
- The dot1x authentication will not be enabled on interfaces with specific configuration combination. [PR1696906](#)
- Dot1x authentication failure for EVPN VXLAN enabled port [PR1697995](#)
- Adaptive sampling will not work if the system clock is turned backward. [PR1699585](#)
- TCAM space might exhaust when learning DHCP snooping entries on a trusted port. [PR1699777](#)
- Dot1x memory is spiking up even after clearing the dot1x sessions. [PR1702388](#)
- The PXE BIOS recovery fails on EX9204, EX9208, and EX9214 Virtual Chassis setup. [PR1704457](#)
- Traffic drops with hierarchal overlay ECMP configuration. [PR1704470](#)
- EAP authentication might not be successful with 802.1X server-fail configuration. [PR1705490](#)
- Layer 3 forwarding issues for IRB. [PR1706845](#)
- The PoE firmware upgrade fails on EX4400 platforms. [PR1706952](#)

- A dot1xd crash is seen on EX2300 platforms. [PR1711422](#)

Interfaces and Chassis

- VRRP master-master condition might occur when there are more than two devices in the VRRP group. [PR1680178](#)
- The unicast traffic will drop on the QFX5100 and EX4600-VC line of switching platforms. [PR1695663](#)

Layer 2 Ethernet Services

- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance. [PR1689005](#)
- phone-home and SZTP may fail if phone-home daemon restarts. [PR1693124](#)

Platform and Infrastructure

- EX9000 Series and MX Series devices do not relay a DHCP offer with a broadcast flag under EVPN-VXLAN scenario. [PR1670923](#)
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. [PR1678506](#)
- The vmcore might crash in low memory conditions. [PR1694463](#)

Routing Protocols

- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. [PR1711153](#)

Virtual Chassis

- Instability observed after mastership switchover on members with SFP-T pluggable installed on EX4600-VC. [PR1689946](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 38

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

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

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

We have two types of releases, 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 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
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 JRR Series

IN THIS SECTION

- [What's New | 40](#)
- [What's Changed | 40](#)
- [Known Limitations | 40](#)
- [Open Issues | 41](#)
- [Resolved Issues | 41](#)
- [Migration, Upgrade, and Downgrade Instructions | 42](#)

What's New

IN THIS SECTION

- [Routing Policy and Firewall Filters](#) | 40

Learn about new features introduced in this release for JRR Series Route Reflectors.

Routing Policy and Firewall Filters

- **Support for the IPv6 unicast address-specific BGP extended community attribute (JRR200, QFX Series, and vRR)**—Starting in Junos OS Release 23.1R1, we support the IPv6 unicast address-specific BGP extended community attribute. You can configure the VRF route target with the IPv6 extended community. You can encode each IPv6 unicast address-specific extended community as a 20-octet file.

To accommodate the IPv6 unicast address-specific extended community, set the IPv6 community configuration under the `[edit policy-options]` hierarchy and set the following configuration statements in the `[edit policy-options community community-name members]` hierarchy:

- `ipv6-target:<IPv6 unicast address>:operator-defined local values`
- `ipv6-origin:<IPv6 unicast address>:operator-defined local values`
- `ipv6-extended:type-and-subtype value:<IPv6 unicast address>:operator-defined local values`

[See [show route detail](#), [show route advertising-protocol](#), [Understanding BGP Communities, Extended Communities, and Large Communities as Routing Policy Match Conditions](#), [Understanding How to Define BGP Communities and Extended Communities](#), [ipv6-extended](#), [ipv6-origin](#), and [ipv6-target](#).]

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

IN THIS SECTION

- [General Routing](#) | 41

Learn about the issues fixed 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.

General Routing

- With BMP RIB-IN and BMP RIB-OUT configured on MX or PTX Platforms, large number of BGP routes remain in Holddown state after route churn. [PR1685510](#)
- A 802.1Q tagged Ethernet traffic with an expected VLAN ID and with a non-zero 802.1P value ingressing a JRR200 VLAN enabled interface is dropped. [PR1691694](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 42

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, EOL and EEOL:

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

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

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 4: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

- [What's New | 44](#)
- [What's Changed | 45](#)
- [Known Limitations | 47](#)
- [Open Issues | 47](#)
- [Resolved Issues | 47](#)

What's New

IN THIS SECTION

- [VPNs | 44](#)

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

VPNs

- **Introduction of prelogon compliance checks (SRX Series and vSRX 3.0)**—In Junos OS Release 23.1R1, we introduce prelogon compliance for Juniper Secure Connect. This functionality validates the current status of a connecting client device prior to the authentication (that is, before user's login). You can configure different match criteria on the SRX Series firewall to allow or reject client devices.

You can configure this feature using the statement `compliance pre-logon name` at:

- `[edit security remote-access]` hierarchy level to configure prelogon compliance rules.
- `[edit security remote-access profile realm-name]` hierarchy level to associate a prelogon compliance rule to the remote-access profile.

[See [prelogon compliance checks](#).]

- **Support for application bypass in Juniper Secure Connect (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can use Juniper Secure Connect to send specific application traffic directly to its destination instead of passing it through the VPN tunnel. You can accomplish this functionality by specifying domain names and protocols for the specified applications that would bypass the VPN tunnel. The bypass feature simplifies the administrator and end-user experience.

When you configure the application bypass feature and establish a remote-access VPN tunnel, the configuration automatically enables a stateful firewall rule rejecting incoming connections on other adapters, which prevents the device from becoming a bastion host.

You can configure this feature on SRX Series firewalls and on vSRX 3.0 virtual firewalls by using `application-bypass` at the `[edit security remote-access client-config name]` hierarchy level.

[See [Application Bypass](#).]

- **Support for multiple certificates and multiple domains (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, with support for multiple certificates and multiple domains, we now allow Juniper Secure Connect connection profiles with different URLs without any certificate warning.

[See [Multiple certificates and domains support.](#)]

What's Changed

IN THIS SECTION

- [VPNs](#) | 45

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

VPNs

- **Change format of remote-access profile names (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've changed the format of remote-access profile names to enhance end-user experience using Juniper Secure Connect. In releases before Junos OS Release 23.1R1, you configure the remote-access profile name using the realm name at the [edit security remote-access profile *realm-name*] hierarchy level. But with organizations connecting to several gateways, using the remote-access profile names, such as **hr**, multiple times in the remote-access connection profile becomes unmanageable.

To address this issue, we introduce a new convention for configuring remote-access profile names. You can now configure profile names with URLs using any of the following formats at the [edit security remote-access profile *realm-name*] hierarchy level, so that end users can connect to the relevant gateway:

- *FQDN/RealmName*
- *FQDN*
- *IP address/RealmName*
- *IP address*

For example, you can now use **ra.example.com/hr**, **ra1.example.com/hr** and **ra.example.com** as realm names.

With the introduction of this convention, we need to deprecate the existing default-profile option at the [edit security remote-access] hierarchy level. Your remote-access profiles names will refer to URLs either with an FQDN or with an IP address, depending on how the end users would connect—for example, **ra.example.com/hr**, **ra.example.com**, **192.168.1.10/hr** or **192.168.1.10**. With this change, the end user will now see the connection profile name in the Juniper Secure Connect application as **ra.example.com/hr** instead of **hr**, as was the case in earlier releases.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name **hr** in the current configuration to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the follow commands -

- `user@host# rename security remote-access profile hr to profile ra.example.net/hr`

- `user@host# rename security remote-access profile hr to profile 192.168.1.10/hr`

[See [profile \(Juniper Secure Connect\)](#).]

- **Unavailability of default-profile option for remote-access VPN solution (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've hidden the default-profile option at the [edit security remote-access] hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the default-profile option.

We've deprecated the default-profile option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However, modifying the current configuration does not affect existing deployments.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name in the current configuration **hr** to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the following commands -

- `user@host# rename security remote-access profile hr to profile ra.example.net/hr`

- `user@host# rename security remote-access profile hr to profile 192.168.1.10/hr`

For new configurations, consider the following scenarios to create a new remote-access profile based on how your end users connect using the Juniper Secure Connect application:

- If your end users connect using an IP address, specify the IP address in the profile name.
- If your end users connect using an FQDN, specify the FQDN in the profile name.
- If you need to separate users with different realm values such as **hr**, append **/hr** to the IP address or FQDN as follows:
 - [edit security remote-access profile *ra.example.net/hr*]
 - [edit security remote-access profile *192.168.1.10/hr*]

[See [default-profile \(Juniper Secure Connect\)](#) .

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 | 48](#)
- [What's Changed | 48](#)
- [Known Limitations | 48](#)
- [Open Issues | 49](#)
- [Resolved Issues | 49](#)
- [Migration, Upgrade, and Downgrade Instructions | 49](#)

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for enterprise.

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

Resolved Issues

There are no resolved issues 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.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading Junos OS on an Aggregation Device | 50](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 51](#)
- [Preparing the Switch for Satellite Device Conversion | 52](#)
- [Converting a Satellite Device to a Standalone Switch | 54](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 54](#)
- [Downgrading Junos OS | 55](#)

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 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 Junos OS

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

NOTE: You cannot downgrade more than three releases.

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

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

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

- [What's New | 55](#)
- [What's Changed | 56](#)
- [Known Limitations | 56](#)
- [Open Issues | 56](#)
- [Resolved Issues | 56](#)
- [Migration, Upgrade, and Downgrade Instructions | 56](#)

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 provider edge.

Known Limitations

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

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

Open Issues

There are no known issues in hardware or software in this release for Junos Fusion for provider edge.

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

Resolved Issues

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

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device](#) | 57
- [Upgrading an Aggregation Device with Redundant Routing Engines](#) | 60

- [Preparing the Switch for Satellite Device Conversion | 60](#)
- [Converting a Satellite Device to a Standalone Device | 62](#)
- [Upgrading an Aggregation Device | 64](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 64](#)
- [Downgrading from Junos OS Release 23.1 | 65](#)

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 23.1R1 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/jinstall64-23.1R1.SPIN-
domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-23.1R1.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/jinstall64-23.1R1.SPIN-
export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-23.1R1.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 23.1R1 *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, unbundle 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 23.1R1, 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 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](#).

Downgrading from Junos OS Release 23.1

To downgrade from Release 23.1 to another supported release, follow the procedure for upgrading, but replace the 23.1 `jinstall` package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

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

Junos OS Release Notes for MX Series

IN THIS SECTION

- [What's New | 66](#)
- [What's Changed | 82](#)
- [Known Limitations | 84](#)
- [Open Issues | 87](#)
- [Resolved Issues | 95](#)
- [Migration, Upgrade, and Downgrade Instructions | 110](#)

What's New

IN THIS SECTION

- [EVPN | 67](#)
- [High Availability | 69](#)
- [Interfaces | 71](#)
- [Junos Telemetry Interface | 72](#)
- [Licensing | 73](#)
- [MPLS | 74](#)
- [Network Address Translation \(NAT\) | 75](#)
- [Network Management and Monitoring | 76](#)

- Precision Time Protocol (PTP) | 77
- Routing Protocols | 77
- Securing GTP and SCTP Traffic | 79
- Source Packet Routing in Networking (SPRING) or Segment Routing | 79
- Subscriber Management and Services | 79
- VPNs | 81
- Additional Features | 81

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

EVPN

- **Automatically derived ESI support on EVPN-MPLS (MX240, MX480, MX960, MX2010, MX2020, and vMX)**—Starting in Junos OS Release 23.1R1, you can configure multihomed devices in an EVPN-MPLS network to automatically generate the Ethernet segment identifier (ESI) from:
 - System ID and administrative key on the remote customer edge (CE) device (partner).
 - Locally configured MAC and local discriminator values.

[See [Other Methods to Auto-Derive the ESI](#) .]

- **EVPN-MPLS E-LAN flow-aware transport (FAT) label load balancing (MX Series with Advanced Forwarding Toolkit (AFT) cards)** —Starting in Junos OS Release 23.1R1, you can configure provider edge (PE) devices to use FAT labels in an Ethernet VPN-MPLS (EVPN-MPLS) routing instance, according to Request for Comments (RFC) 6391. P devices (transit/core router devices) use these labels to load-balance EVPN-MPLS unicast packets across equal-cost multipaths (ECMPs) without performing deep packet inspection of the MPLS payload. This feature supports emulated LAN (ELAN) with single-homing and multi-homing active/standby and active/active topologies and supports the VLAN-based, VLAN-bundle, and VLAN-aware bundle EVPN-MPLS variants.

NOTE: On MX Series devices, a configuration where the local PE has a static-flow-label and the remote PE does not have a static-flow-label, the remote PE can process packets without dropping any traffic.

Enabling Load Balancing Using Fat Labels for EVPN Routing Instances:



CAUTION: Configuring a flow label or deleting a flow label with the following CLI commands causes a catastrophic event for the routing instance. As a best practice, perform these CLI commands during a maintenance period to avoid network disruptions.

- Configure the flow-label-static statement at the [edit routing-instances routing-instance-name protocols evpn] hierarchy level on PE devices to insert FAT flow labels into pseudowire packets sent to remote PE devices.
- Configure the flow-label statement at the [edit routing-instances routing-instance-name protocols evpn] hierarchy level on PE devices to signal flow-label capability in the EVPN Layer 2 Attributes Extended Community by setting the flow-label (F) bit in the EVPN Type 3 route.

[See [flow-label](#) and [flow-label-static](#).]

- **EVPN with transport class tunnels (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can configure EVPN services over transport class tunnels. We support Ethernet VPN–virtual private wireless service (EVPN-VPWS), Ethernet VPN–emulated LAN (EVPN-ELAN), and EVPN–ETREE services over the following transport tunnels:
 - Segment routing–traffic engineering (SR-TE)
 - Interior Gateway Protocols Flexible Algorithm
 - RSVP-TE
 - BGP Labeled Unicast (BGP-LU) with BGP classful transport (BGP-CT)

[See [Configuring EVPN over Transport Class Tunnels](#) and [Example: Configuring EVPN-VPWS over Transport Class Tunnels](#) .]

- **Support for BPDU protection (MPC10E-10C-MRATE MPC, MPC10E-15C-MRATE MPC, MX2K-MPC11E MPC, MX10K-LC9600 line card, and MX304 router)**—Starting in Junos OS Release 23.1R1, we support bridge protocol data unit (BPDU) protection on the line cards and routers that are based on Advanced Forwarding Toolkit (AFT).

[See [BPDU Protection for Spanning-Tree Protocols](#).]

- **Determine IRB interface state changes based on local and remote connectivity states in EVPN fabrics (EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX2010, MX2020, vMX, QFX5110, QFX5120-48T, QFX5120-48Y, QFX5210, QFX10002, QFX10002-60, and QFX10008)**—Starting in Junos OS Release 23.1R1, the provider edge (PE) devices in an EVPN fabric consider the following factors when determining the state (up or down) of an L3 integrated routing and bridging

(IRB) interface. These factors apply to an L3 IRB interface that is associated with a bridge domain or a VLAN in an EVPN instance (EVI).

- Associated local L2 interface states

To customize the L2 interface name and other parameters that the device uses to compute the IRB interface state, configure the `interface-state` statement at the `[edit interfaces irb unit n]` hierarchy.

- Remote provider edge (PE) device reachability based on the network isolation state of the bridge domain or the EVI

The device includes the states of the associated EVPN overlay tunnel interfaces in the network isolation state evaluation.

To define the parameters that determine when an EVI or a bridge domain is in a network isolation state:

1. Configure the network-isolation group `group-name` statement at the `[edit protocols]` hierarchy level to define a network isolation profile using the available options.
2. Assign the network isolation group profile to a bridge domain or an EVI using the `network-isolation-profile group network-isolation-group-name` statement at these hierarchy levels:
 - Bridge domain—`[edit bridge-domain bd-name bridge-options]`
 - EVI—`[edit routing-instance instance-name switch-options]`

[See [Determine IRB Interface State Changes from Local and Remote Connectivity States in EVPN Fabrics](#), [interface-state](#), and [network-isolation](#).]

High Availability

- **Support for running unified ISSU on MPC10E line cards (MPC10E line cards on MX240, MX480, and MX960 routers)**—Starting in Junos OS Release 23.1R1, you can run in-service software upgrade (ISSU) on MPC10E line cards. In previous releases in which ISSU was available, upgrades on line cards required a rapid restart of the new software. Those previous upgrades left the forwarding path untouched because the line cards don't have hardware redundancy. Now you can run ISSU on the line cards by issuing the command `request system software in-service-upgrade`. This new feature reduces packet loss by reducing the line card's downtime during ISSU.

We recommend that you run ISSU only on stable working systems.

Before you issue the ISSU command, ensure that you've enabled GRES and nonstop active routing (NSR).

See caveats and limitations in [Unified ISSU System Requirements](#).

[See [request system software in-service-upgrade.](#)]

- **Support for routing protocols when running unified ISSU on MPC10E line cards (MPC10E line cards on MX240, MX480, and MX960 routers)**—Starting in Junos OS Release 23.1R1, we support routing protocols when you run ISSU on MPC10E line cards by issuing the command `request system software in-service-upgrade`.

We support these routing protocols:

- BGP add-path with multipath
- BGP BMP
- BGP flowspec
- BGP multipath
- BGP Prefix-Independent Convergence (PIC) Edge
- BGP with resource public key infrastructure (RPKI)
- CCC
- L2 circuit
- L2VPN
- L3VPN
- L3VPN-CSC
- MPLS LDP
- MPLS-over-GRE tunnels
- MPLS-over-UDP tunnels
- MPLS RSVP
- OSPF
- PIM-ASM
- PIM-SSM
- VPN

[See [request system software in-service-upgrade.](#)]

- **Support for Layer 2 forwarding when running unified ISSU on AFT-based line cards (MPC-10E line cards on MX240, MX480, and MX960 routers)**—Starting in Junos OS Release 23.1R1, we support Layer 2 forwarding when you run ISSU on Advanced Forwarding Toolkit (AFT)-based line cards.

We support the following Layer 2 forwarding features:

- EVPN-VXLAN
- LACP
- LAGs
- LLDP
- Q-in-Q interfaces
- VLAN

[See [request system software in-service-upgrade](#) .]

Interfaces

- **Support for 1G speed (MX304)**—As of Junos OS Release 23.1R1, the MX304 now supports 1G speeds. The addition of 1G support is beneficial for customers maintaining older 1G connections and for low-speed uplink/downlink applications. The chassis offers 1G options in the port profile configuration, which is available on all ports. Previously, MX devices only supported speeds of 400G, 100G, 40G, 10G, and 25G.

[See [Port speed on MX304 Router Overview](#)].

- **Permanent MAC address for aggregated Ethernet interface (MX240, MX480, MX960, MX2008, MX2010, MX2020, and VMX)**—Starting in Junos OS Release 23.1R1, the number of static MAC addresses increases for:

- VMX, MX240, MX480, and MX960 from 16 to 80.
- MX2008, MX2010, and MX2020 from 0 to 80.

The chassisd process (chassisd) now allocates MAC addresses to aggregated Ethernet interfaces in this pattern:

- First 16 interfaces receive addresses from a private MAC pool.
- Next 64 ae interfaces receive addresses from a reserved public MAC pool.
- Rest of the ae interfaces receive addresses from a public MAC pool.

[See [static-mac](#).]

Junos Telemetry Interface

- **Number of configurable BMP monitoring stations increases to a maximum of eight (MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, and vMX)**—Starting in Junos OS Release 23.1R1, Junos telemetry interface (JTI) delivers initial sync and ON_CHANGE BGP routing information base (also known as routing table) statistics by using remote procedure calls (gRPC) or the gRPC network management interface (gNMI) from a device to an outside collector for a maximum of eight BMP monitoring stations.
- **Network slicing telemetry support for slice queue statistics (MX480, MX960, MX10003, and MX2020)**—Starting in Junos OS Release 23.1R1, Junos telemetry interface (JTI) supports slice queue statistics on network slices (logical networks). Network slicing enables network operators to define logical networks on a physical network. A slice comprises a set of nodes, links, and prefixes of a transport network.

Subscribe to the native sensor `/junos/system/linecard/cos/interface/slice/out-queue/` to export egress queue statistics.

[See [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#) for sensor information. See [Hierarchical Class of Service for Network Slicing](#) for network slicing information.]

- **Support for OpenConfig QoS fabric priority classifiers and state sensor (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.1R1, we support OpenConfig QoS fabric priority classifiers for IPv6 and MPLS. Support includes configuration and streaming of operational state data.

[For OpenConfig to Junos configuration mappings, see [Mapping OpenConfig QoS Commands to Junos Configuration](#). For state sensors, see [Telemetry Sensor Explorer](#).]

- **OpenConfig QoS schedulers and rewrite support and state sensor support (MX150 (MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016 and vMX)**—Starting in Junos OS Release 23.1R1, we support OpenConfig QoS for forwarding classes, classifiers and rewrites, classifiers and rewrite bindings, schedulers, drop profiles, and scheduler maps. Support includes sensor configuration and streaming of operational state data.

[For OpenConfig to Junos configuration mappings, see [Mapping OpenConfig QoS Commands to Junos Configuration](#). For state sensors, see [Telemetry Sensor Explorer](#).]

- **Segment routing telemetry for OSPFv2 (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and VMX)**—Starting in Junos OS Release 23.1R1, we support collection and streaming of telemetry data for segment routing with the OSPFv2 protocol. You can record statistics for the Source Packet Routing in Networking (SPRING) traffic per interface, per link aggregation group, and per segment identifier. Support includes OpenConfig and native Junos sensors. To enable collection and export of SR statistics, include the `sensor-based-stats` statement at the `[edit protocol ospf source-packet-routing]` hierarchy level.

[See [Telemetry Sensor Explorer](#) for OpenConfig sensors and [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#) for native Junos sensors.]

- **Support for vtnet0|1 interface statistics (MX2010 and MX2020 with MPC9E and MPC11E line cards in a Junos node-slicing environment)**—Starting in Junos OS Release 23.1R1, Junos telemetry interface (JTI) supports interface sensors for the vtnet0|1 interfaces. A vtnet0 interface communicates between Routing Engines and Packet Forwarding Engines. A vtnet1 interface communicates between the primary and secondary Routing Engines. An MX Series router supports vtnet0|1 interface statistics in either of these scenarios:
 - The router operates as the base system (BSYS).
 - You assign line cards to the router, enabling it to operate as a guest network function (GNF).

[See [Telemetry Sensor Explorer](#).]

Licensing

- **Bandwidth-based MACsec license support (MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.1R1, the Media Access Control security (MACsec) support on the listed devices requires installation of MACsec bandwidth licenses. These licenses are perpetual.

The MACsec feature licenses are available in the following variants:

- S-MX-1C-MSEC-P—100-Gigabit Ethernet license
- S-MX-4C-MSEC-P—400-Gigabit Ethernet license
- S-MX-4C8-MSEC-P—480-Gigabit Ethernet license

The minimum number of MACsec bandwidth licenses installed must be greater than or equal to the configured bandwidth of MACsec-enabled ports.

You can view the MACsec bandwidth license usage by using the command `show system macsec license`. You can view the usage of different feature licenses by using the command `show system license`.

Juniper Agile Licensing supports soft enforcement for MACsec bandwidth licenses. With soft enforcement, the feature remains operational even without a valid license. However, you will receive commit warnings and periodic alarms insisting on installation of a valid license.

[See [Flex Software License for MX Series Routers and MPC Service Cards](#) and [Managing Licenses](#).]

- **Support to trigger license alarm at configured time interval (EX Series, MX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 23.1R1, you can set the time interval at which you want to trigger alarms for features or capacity that do not have licenses installed.

To set the alarm log frequency, use the command `log-frequency` in the `set system license` hierarchy.

[See [Managing Licenses](#).]

MPLS

- **OAM support for labeled IS-IS and labeled OSPF flex algo segment routing paths (ACX5448, ACX6360, and MX Series)**—Starting in Junos OS Release 23.1R1, Junos OS supports the following Operation, Administration, and Maintenance (OAM) capabilities for labeled IS-IS Flexible Algorithm (flex algo) segment routing paths:

- IPv4 and IPv6 MPLS ping
- IPv4 and IPv6 MPLS traceroute
- Equal-cost multipath (ECMP) traceroute

Junos OS also supports IPv4 MPLS ping and IPv4 MPLS traceroute for labeled OSPF flex algo segment routing paths. The OAM functionality is used to detect data plane failures in segment routing paths for the purposes of fault detection and isolation.

To enable these OAM capabilities, we've introduced the `algorithm` option in the following commands:

- `ping mpls segment routing isis fec algorithm algorithm-id`
- `ping mpls segment routing ospf fec algorithm algorithm-id`
- `traceroute mpls segment routing isis fec algorithm algorithm-id`
- `traceroute mpls segment routing ospf fec algorithm algorithm-id`

[See [ping mpls segment routing isis](#), [ping mpls segment routing ospf](#), [traceroute mpls segment-routing ospf](#), and [traceroute mpls segment-routing isis](#).]

- **Include IGP metric to RSVP routes using conditional metric (MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.1R1, you can include the actual IGP metric to RSVP routes that use the conditional metric. Including the IGP metric helps preserve its value for use in certain use cases—for example, in calculating the BGP MED.

[See [Preserving the IGP metric in RSVP LSP routes](#), and [include-igp-metric](#)include-igp-metric.]

- **Targeted load-balancing support for business edge customers using PWHT service interfaces (MX Series)**—Starting in Junos OS Release 23.1R1, we support targeted load balancing on pseudowire headed termination (PWHT) service interfaces. If you configure the member links of a redundant logical tunnel (RLT) in active-active mode with targeting on PWHT service interfaces, then traffic gets distributed to specific logical tunnel interfaces on different Packet Forwarding Engines. You use distribution lists to manage targeted load balancing. With this feature, you guarantee accurate shaping or policing by adding only a one-member logical tunnel interface to a distribution list.

[See [PWHT RLT Configuration Modes](#).]

- **PWHT Support for family mpls (MX Series)**—Starting in Junos OS Release 23.1R1, we support family mpls on pseudowire headend termination (PWHT) service interfaces using inter-AS Option B. MX Series devices support for the following features on PWHT service interfaces:

- MPLS, including MPLS-IPv4 and MPLS-IPv6
- MPLS CoS
- MPLS inline active flow monitoring

[See [Interprovider VPNs](#), [Inline Flow Monitoring Overview](#), and [MPLS CoS Configuration](#).]

- **Enable TLS for PCEP sessions (ACX5448, ACX5448-D, ACX5448-M, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can enable Transport Layer Security (TLS) in a Path Computation Client (PCC) to establish a TCP connection with the Path Computation Element (PCE). This connection creates a secure Path Computation Element Protocol (PCEP) session to transport PCEP messages.

To enable TLS in a PCC process (PCCD) and to establish a PCEP session, set the `tls-strict` configuration statement at the `[edit protocols pcep]` hierarchy level.

[See [Enabling Transport Layer Security for PCEP Sessions](#).]

- **Support to report path optimization and computed metrics in PCEP (ACX710, ACX5448, ACX5448-M, ACX5448-D, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, we report PCEP path optimization metrics (IGP, TE, and delay) for RSVP and segment routing–traffic engineering (SR-TE) label-switched paths (LSPs).

To configure the interior gateway protocol (IGP), traffic engineering, and path delay optimization metrics for RSVP LSPs, include the `metric-type igp/te/delay/delay minimum` CLI statement at the `[edit protocols mpls label-switched-path lsp-name]` hierarchy level.

To configure the optimization metrics for SR-TE LSPs, include the `metric-type igp/te/delay/delay minimum` CLI statement at the `[edit protocols source-packet-routing compute-profile compute-profile-name]` hierarchy level.

[See [Reporting Path Optimization Metrics in PCEP](#).]

Network Address Translation (NAT)

- **Inline NAT support (MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.1R1, you need a license to use the inline NAT feature on the listed devices. The inline NAT feature is part of the Premium tier of licenses.

[See [Flex Software License for MX Series Routers and MPC Service Cards](#).]

- **Source NAT port overload (MX240, MX480, and MX960 devices with MX-SPC3)**—Starting in Junos OS Release 23.1R1, we support port overloading with and without enhanced port overloading hash algorithm. MX-SPC3 with port-overloading supports:
 - Maximum number of IP Address = 2048 per NPU.
 - Maximum port-overloading factor value = 32.

We've updated the hash algorithm to determine the port-overloading index for a destination address. The hash algorithm uses the reverse traffic from the server, matches the existing sessions, and reuses the same Network Address Translation (NAT) resources. To configure enhanced algorithm, it is mandatory to have port-loading.

You can configure the updated hash algorithm using the `enhanced-port-overloading-algorithm` statement at the `[services nat source pool pool-name port]` hierarchy level. Enhanced port overloading algorithm provides better utilization of port overloading.

[See [pool \(Source NAT Next Gen Services\)](#).]

- **CGNAT services on MX-SPC3 (MX240, MX480, and MX960 with MPC10)**—Starting with Junos OS Release 23.1R1 CGNAT services support is added in MPC10 for access side subscribers.

[See [Junos OS Enhanced Subscriber Management Overview](#).]

- **AMS support for load balancing on MX-SPC3 (MX240, MX480, and MX960 with MPC10)**—Starting in Junos OS Release 23.1R1, we support load balancing using the new CLI option `modulo-key` in the `set interfaces ams0 unit 1 load-balancing-options` command.

[See [Configuring Load Balancing on AMS Infrastructure](#).]

Network Management and Monitoring

- **YANG data models for Junos RPCs include accurate output schemas (MX480)**—Starting in Junos OS Release 23.1R1, the YANG data models for Junos RPCs include accurate output schemas. In earlier releases, the RPC output schemas use the `anyxml` statement to represent a chunk of XML in the RPC reply. The Juniper [yang](#) GitHub repository includes the updated schemas, and Junos OS emits the new schemas by default. To emit the alternate RPC schemas containing the `anyxml` statement on the local device, configure the `emit-anyxml-in-rpc-output` statement at the `[edit system services netconf yang-modules]` hierarchy level. After you configure the statement, the `show system schema` command generates the schemas that use `anyxml`.

[See [Understanding the YANG Modules for Junos Operational Commands](#).]

Precision Time Protocol (PTP)

- **G.8275.1 telecom profile and PTPoE encapsulation support (MX10004 with MX10K-LC480)** — Starting in Junos OS Release 23.1R1, the MX10K-LC480 line card on the MX10004 supports the Precision Time Protocol over Ethernet (PTPoE) encapsulation as defined in the G.8275.1 telecom profile. PTPoE supports:
 - PTP hybrid-over-aggregated Ethernet and PTP hybrid over LAG profile.
 - Primary and secondary Synchronous Ethernet, and PTP passive ports on different line cards.
 - Mixed mode of aggregated Ethernet (link with different speeds).
 - master and slave statements to configure asymmetry on primary and secondary links. Primary and secondary links in an aggregated interface can have different asymmetry.
 - PTP with hyper mode profile to enable the distribution of phase and time with full timing support. You must ensure that all the devices in the network operate in combined or hybrid mode with PTP and Synchronous Ethernet enabled on all devices. PTPoE implements the packet-based technology and helps operators deliver synchronization services on aggregated Ethernet interfaces in mobile backhaul (MBH) networks.
 - Configuration of PTP client and synchronous Ethernet source on the same or different line cards.

[See [Precision Time Protocol Overview](#).]

- **G.8275.1 profile with Building Integrated Timing Supply (BITS) as a frequency source in hybrid mode (MX10008 with MX10K-LC2101)**—You can configure BITS as a frequency source with the G.8275.1 profile in hybrid mode. G.8275.1 also supports PTPoE over LAG with BITS as the frequency source. If you configure Synchronous Ethernet and BITS as the frequency source, then based on the clock selection, either Synchronous Ethernet or BITS is chosen as the frequency source in hybrid mode.

[See [show ptp hybrid](#) and [show chassis synchronization \(MX Series Router\)](#).]

Routing Protocols

- **BFD for VXLAN (MX2020)**—Starting in Junos OS Release 23.1R1, we support BFD for VXLANs.

[See [Understanding BFD](#).]

- **IS-IS maximum LSP size (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can configure the maximum LSP size for IS-IS in the range 512 through 9192 bytes to support advertising a higher number of prefixes.

[See [max-lsp-size](#).]

- **Block route redistribution from a specific protocol into IS-IS (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can block the export policy from redistributing the routes from other non-desired protocols into IS-IS. You can block the redistribution using the `set protocol isis no-external-export protocol` statement at the `[set protocols isis]` hierarchy level.

[See [no-external-export \(Protocols IS-IS\)](#).]

- **Prevent IS-IS from entering overload state on reaching prefix limit (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can prevent IS-IS from entering the overload state even after the prefixes reach the configured limit. You can configure the `set protocols isis dynamic-overload no-overload-on-prefix-export-limit` statement at the `[set protocols isis]` hierarchy level.

[See [no-overload-on-prefix-export-limit \(Protocols IS-IS\)](#).]

- **Autorecovery from IS-IS overload state (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can configure IS-IS to automatically exit from an overload state. The configuration prevents IS-IS from flushing all the fragments on overload so that when the fragment space is available, IS-IS automatically exits from the overload state. You can configure the autorecovery using the `set protocols isis dynamic-overload auto-recovery` command.

[See [auto-recovery \(Protocols IS-IS\)](#).]

- **Support for BGP-LS NLRI to carry confederation ID (ACX710, ACX5448, MX10003, QFX5120-48YM, QFX5200, and QFX5210, and vRR)**—Starting in Junos OS Release 23.1R1, Junos OS enables BGP Link State (BGP-LS) network layer reachability information (NLRI) to carry the confederation ID in TLV 512 when BGP confederation is enabled. The NLRI carries the confederation ID along with the member autonomous system number (AS number) in TLV 517 as defined in RFC 9086. In releases before Junos OS Release 23.1R1, BGP-LS NLRI carries only the member AS number in TLV 512 and the confederation ID is not encoded in the `Isdist.0` routing table.

[See [Link-State Distribution Using BGP Overview](#).]

- **Support for Policy based ORR (MX Series)**—The policy based ORR helps you to select the paths to advertise to achieve your traffic engineering requirements. You can specify a subset of the paths as candidate paths for path selection. The existing path selection algorithms select the best paths and you can choose to modify the attributes of the selected paths or reject the selected paths. The policy based ORR can work alone or with IGP based ORR and `add-path`.

To enable this feature in BGP peer groups, configure `export <policy>` at the `protocols bgp group <name> optimal-route-reflection` hierarchy level.

[See [export \(Protocols BGP\)](#), [optimal-route-reflection](#), and [show bgp group](#).]

Securing GTP and SCTP Traffic

- **VRF support with SCTP (MX Series)**—Starting in Junos OS Release 23.1R1, we support virtual routing and forwarding (VRF) for SCTP associations. You can use this feature to manage remote IP addresses. When an SCTP association is established over a VRF instance, the kernel must consider an additional parameter—the VRF ID—in addition to the traditional 4-tuple (source IP, source port, destination IP, destination port) when searching for unique associations.

[See [SCTP Support for Virtual Routing and Forwarding \(VRF\)](#)].

RELATED DOCUMENTATION

https://www.juniper.net/documentation/us/en/software/junos/gtp-sctp/topics/ref/statement/mask_uli.html

<https://www.juniper.net/documentation/us/en/software/junos/agf-user-guide/agf/topics/concept/agf-sctp-amf.html>

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for SRv6 SID in BGP export policy (MX Series)**—Starting in Junos OS Release 23.1R1, you can list multiple Segment Routing for IPv6 (SRv6) segment identifiers (SIDs) for different services under a single routing instance or under a default instance in a BGP export policy. In earlier Junos OS releases, BGP allows only one SRv6 SID, which is the default SID per routing instance or under a default instance. This feature enables BGP to steer the traffic for each service (per service prefix) based on the best effort or Flexible Algorithm (flex algo) tunnel.

[See [srv6 \(BGP\)](#).]

- **Support for unnumbered interfaces for IS-IS with SPRING TI-LFA (MX Series)**—Starting in Junos OS Release 23.1R1, we support IS-IS over unnumbered interfaces on point-to-point links with SPRING topology-independent loop-free alternate (TI-LFA). You can configure unnumbered interfaces to share the same subnet across multiple interfaces to conserve IPv4 addresses. Note that we do not currently support unnumbered interfaces for IPv6.

[See [Configuring Topology-Independent Loop-Free Alternate with Segment Routing for IS-IS](#).]

Subscriber Management and Services

- **Load and Overload Control Information for Wireless CUPS (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 23.1R1, we support load and overload control information reports for wireless control and user plane separation (wireless CUPS). You can use these information reports to troubleshoot and maintain the usage load of your system.

You can see the following data in the load control information report:

- CPU Usage
- Session Capacity
- Memory Usage
- Bandwidth Usage
- Metric Calculation and Report

You can see the following data in the overload control information report:

- UE registration surges
- UE Mobility and Application signal
- Packet Forwarding Engine Congestion Signal
- Routing Engine and anchor Packet Forwarding Engine failover monitoring

[See [Load and Overload Control Information](#)].

- **Wireless CUPS: Load and Overload Control Maintenance Mode (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 23.1R1, if you enable load control, overload control, or both, then you can prevent new sessions from starting. You can then perform load control, overload mitigation, system upgrades, and other back-end maintenance. You can enter maintenance mode using the `service-mode` command.

[See [Load and Overload Control Information](#), [Maintenance Mode](#), and [service-mode](#)].

- **Wireless CUPS: Mobile-Edge Configuration Commit Check (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 23.1R1, if any active sessions are logged in to the User Plane Function (UPF), you will not be able to modify or delete any configuration. If any active sessions exist, Junos OS displays an error message and rejects your modifications.

[See [Load and Overload Control Information](#) and [Mobile-edge Configuration Commit Check](#)].

- **Wireless CUPS: Downlink Forwarding Queues (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 23.1R1, we support queue sets on the virtual routing and forwarding (VRF) loopback interface for each anchor Packet Forwarding Engine. The use of queue sets provides service differentiation for all mobile subscriber traffic traveling in the downlink direction. The queues are preconfigured, but can be customized with CoS commands.

[See [Downlink Forwarding Queues](#) and [Downlink-dscp-to-egress-forwarding-class](#)].

- **Wireless CUPS: IPv4 Framed Routing (MX240, MX480, and MX960)**—Starting in Junos OS Release 23.1R1, we support IPv4 framed routing on User Plane Functions (UPFs). You can use framed routes to provide a routable IP network behind a User Endpoint.

[See [Wireless CUPS Overview](#)].

VPNs

- **Support for native IPv6 in carrier-of-carrier VPNs (ACX Series, MX Series, and QFX Series)**—Starting in Junos OS Release 23.1R1, you can configure LDP and IGPs using IPv6 addressing to support carrier-of-carriers VPNs. Junos OS supports native IPv6 prefix exchanges in the carrier-of-carriers deployments.

[See [Carrier-of-Carriers VPNs](#), [LDP Native IPv6 Support Overview](#), and [LDP Configuration](#).]

- **Passive mode tunneling support for MX-SPC3 (MX240, MX480 and MX960)**—Starting in Junos OS Release 23.1R1, we support passive mode tunneling on the MX-SPC3 Services Processing Card. You enable this feature to allow IPsec tunneling of malformed packets bypassing the usual active IP checks.

[See [Configuring IPsec VPN on MX-SPC3 Services Card](#).]

Additional Features

Support for the following features has been extended to these platforms.

- **Support for flexible cross-connect on EVPN-VPWS (MPC10, MPC11, MX304, and MK10K-LC9600)**

We support the following flexible cross-connect (FXC) operation in an Ethernet VPN–virtual private wireless service (EVPN-VPWS):

- Interoperability with access routers that are configured for either VLAN-aware or VLAN-unaware FXC services
- VLAN demultiplexing on single and dual VLAN tags
- Support for single label use per EVI for VLAN-aware and VLAN-unaware FXC services

[See [Overview of Flexible Cross-Connect Support on VPWS with EVPN](#).]

- **Support for timing SyncE (MX304)**—We now support the timing SyncE.

[See [Understanding the Time Management Administration Guide](#) and [profile-type](#).]

- **Broadband network gateway (BNG) support**—We support BNG on MX304 router and MX480 router with MPC10E for interface-shared filters and ADFs.

[See [Interface-Shared Filters Overview](#), [adf \(Dynamic Firewalls\)](#).]

- **Support for DHCP functionality on MX304**—We support the DHCP functionality (Server, relay, and client features for DHCP versions 4–6) on MX304.

[See [DHCP Relay Agent](#).]

What's Changed

IN THIS SECTION

- [Network Management and Monitoring | 82](#)
- [PKI | 83](#)

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

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the `get-system-yang-packages` RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `get-system-yang-packages` RPC reply replaces the `xmlproxy-yang-modules` tag with the `proxy-xml-yang-modules` tag in the XML output.
- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

PKI

- Deprecating options related to certificate enrollment (Junos)**—Starting in Junos OS Release 23.2R1, we're deprecating earlier CLI options related to Public Key Infrastructure (PKI) to enroll and reenroll local certificate through Simple Certificate Enrolment Protocol (SCEP). The table below shows the Junos CLI commands and configuration statements with the options being deprecated. You can find the same CLI options now available under `scep` option in these commands and statements.

Table 7: Deprecated Junos CLI Options

Junos CLI Commands and Statements	Deprecated Options
<code>set security pki auto-re-enrollment</code>	<code>certificate-id</code>
<code>request security pki local-certificate enroll</code>	<code>ca-profile</code> <code>certificate-id</code> <code>challenge-password</code> <code>digest</code> <code>domain-name</code> <code>email</code> <code>ip-address</code> <code>ipv6-address</code> <code>logical-system</code> <code>scep-digest-algorithm</code> <code>scep-encryption-algorithm</code> <code>subject</code>

Table 7: Deprecated Junos CLI Options *(Continued)*

Junos CLI Commands and Statements	Deprecated Options
<code>request security pki node-local local-certificate enroll</code>	<code>ca-profile</code> <code>certificate-id</code> <code>challenge-password</code> <code>digest</code> <code>domain-name</code> <code>email</code> <code>ip-address</code> <code>ipv6-address</code> <code>logical-system</code> <code>scep-digest-algorithm</code> <code>scep-encryption-algorithm</code> <code>subject</code>

[See [auto-re-enrollment \(Security\)](#), [request security pki local-certificate enroll scep](#), and [request security pki node-local local-certificate enroll](#).]

Known Limitations

IN THIS SECTION

- [General Routing | 85](#)
- [MPLS | 85](#)
- [Passive Mode Tunneling | 86](#)
- [Platform and Infrastructure | 86](#)
- [Routing Protocols | 86](#)
- [User Interface and Configuration | 87](#)

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

- For IPv6 traffic that is ingressing into an abstract fabric (AF) interface via MPC11E card, and also sampled, the OutputIntf in the flow records may not be captured if nexthop-learning knob is not enabled. [PR1680873](#)
- because of the scale and PPS, race condition between sessions can occur to get a port bitmap which is leading to few out of port errors. Once the bitmap race condition is cleared the same resource will be allocated to subsequent NAT allocation request(resource not wasted). Because of the race condition, we see the resource momentarily unavailable for the allocation as two sessions are trying to allocate the same resource. [PR1693824](#)
- There is increase in memory footprint across different demons after an image upgrade resulting increase in the system memory. [PR1694522](#)
- MX304: When 1G interface is disabled, the interface active defect alarm is not set in show interfaces extensive. [PR1712831](#)

MPLS

- Traceroute in MPLS OAM may fail with unreachable in ECMP case when topology has multiple ecmp paths in each transit router. This is because destination address is not available. Destination address is computed using base address + bitmap index(available for that leg).Junos currently supports 64 bitvector size.Each transit ecmp legs consumes available bitmap indexes in the echo request packet. When all the bitmap indexes are consumed by the previous transit routers/ecmp legs, then for other ecmp legs bitmap indexes are not available hence multipath information tlv bitmap will be zero leading to unreachable issue as no destination address is available. Even RFC 8029 section 4.1 says full coverage is not possible as below, If several transit LSRs have ECMP, the ingress may attempt to compose these to exercise all possible paths. However, full coverage may not be possible. Hence this is an expected behavior.[PR1699685](#)

Passive Mode Tunneling

Passive Mode Tunneling support for MX-SPC3 Services Card (MX240, MX480 and MX960)— Passive mode tunneling has following limitations:

- MX-SPC3 services card supports header-integrity-check option in service-set configuration to verify the packet header for anomalies in IP, TCP, UDP, and ICMP information. This functionality is opposite to the functionality supported by passive-mode-tunneling option. If you configure both the header-integrity-check statement and the passive-mode-tunneling statement, the configuration will result in error during the commit.
- MX-SPC3 services card with passive-mode-tunneling support, and header-integrity-check in service-set has following implications with multiple VPNs configuration -
 - If you enable header-integrity-check option, passive-mode-tunneling option should be disabled for all VPNs and service-set can't have two or more IPsec VPNs with different passive-mode-tunneling value. This means if header-integrity-check option is enabled, a service-set can have only one type of VPN configured with either passive-mode-tunneling enabled or disabled.
 - If you disable header-integrity-check option, then a service-set can have two or more IPsec VPNs with different passive-mode-tunneling value.
- No flow session output is seen with show security flow session output with packet based processing of IPsec traffic via passive mode tunnels.

Platform and Infrastructure

- When the deactivate services rpm and deactivate routing-options rpm-tracking CLIs are applied together and then committed, some of the rpm tracked added routes are not deleted from the routing table. Issue cannot be seen using the following steps. 1. deactivate routing-options rpm-tracking 2. commit the configuration then all the rpm tracked routes will be deleted. If the RPM service needs to be deactivated, 3. deactivate services rpm 4. commit. [PR1597190](#)

Routing Protocols

- When routing-options transport-class fallback none is not configured more than 10 transport-classes or advertise more than 10 distinct colors in SRTE. [PR1648490](#)

User Interface and Configuration

- On all Junos OS platforms with persist-group-inheritance might lead to mustd process crash in highly scaled configuration. [PR1638847](#)

Open Issues

IN THIS SECTION

- [General Routing | 87](#)
- [Interfaces and Chassis | 92](#)
- [Junos XML API and Scripting | 93](#)
- [Layer 2 Features | 93](#)
- [MPLS | 93](#)
- [Network Management and Monitoring | 93](#)
- [Platform and Infrastructure | 94](#)
- [Routing Protocols | 94](#)
- [Services Applications | 94](#)
- [VPNs | 94](#)

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.

General Routing

- 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](#)

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. [PR1462548](#)
- For the MPC10E card line, the IS-IS and micro-BFD sessions do not come up during baseline. [PR1474146](#)
- 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](#)
- runt, fragment and jabber counters are not incrementing on EX4300-MPs [PR1492605](#)
- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. [PR1529596](#)
- The Sync-E to PTP transient simulated by Calnex Paragon Test equipment is not real network scenario. In real network deployment model typically there will be two Sync-E sources (Primary and Secondary) and switchover happens from one source to another source. MPCE7 would pass real network SyncE switchover and associated transient mask [PR1557999](#)
- VE and CE mesh groups are default mesh groups created for a given Routing instance. On vlan/bridge-domain add, flood tokens and routes are created for both VE and CE mesh-group/flood-group. Ideally, VE mesh-group doesn't require on a CE router where IGMP is enabled on CE interfaces. Trinity based CE boxes have unlimited capacity of tokens, so this would not be a major issue. [PR1560588](#)
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the Junos OS Release 21.3R1. [PR1597276](#)
- When user tries to disable AMS ifd using config knob, the ipsec tunnels are not deleted. Deactivating the services will provide the desired result. [PR1613432](#)
- In some NAPT44 and NAT64 scenarios, Duplicate SESSION_CLOSE Syslog will be seen. [PR1614358](#)
- For a topology with VSTP and VRRP configured and IPV6 traffic, if VSTP bridge priority is changed a couple of times (to trigger toggling of root bridge), it is possible that V6 traffic drop is seen on some of the streams. [PR1629345](#)
- mspmand daemon running on MS-MPC/MS-MIC cards can occasionally crash when the service card (fpc/pic) is turned offline and then online at regular intervals when the number of service-set configured is moderately high and when extensive hardware crypto operations are being performed. Exact issue is yet to be isolated. [PR1641107](#)
- Source MAC should not be configured on the underlying static interface on the UP for PPPoE login to work correctly. [PR1641495](#)

- vMX: "input fifo errors" drops reported under pfe shell "show ifd" but not seen in "show interface extensive" output [PR1642426](#)
- bb device has to be manually enabled in configuration for DHCP and PPP access models for BNG CUPS. Configuration to enable bb device is as follows:: #set system subscriber-management mode force-broadband-device [PR1645075](#)
- When per-interface egress and per-sid egress SR sensor stats are configured using the CLI commands below, the (pushed) MPLS label length does not get included in the output/Tx octets field that gets exported from the sensor. set protocols isis source-packet-routing sensor-based-stats per-interface-per-member-link egress set protocols isis source-packet-routing sensor-based-stats per-sid egress This is a day-1 behavior on all Trio ASIC based FPCs on the MX platform. [PR1646799](#)
- On all QFX platforms, Ethernet VPN (EVPN) Type-5 traffic drops are observed when the device is configured only with Type-5 Virtual Routing and Forwarding (VRF) and without an Integrated Routing and Bridging (IRB) interface. [PR1663804](#)
- If the physical link status of the ethernet link between the RE and FPC goes down, there are recovery attempts to bring up the link again. Log messages indicate the recovery attempts and the success/failure status of the attempt. However an alarm is not raised when this failure occurs [PR1664592](#)
- Not all MAC addresses are learnt for some VPLS instances after "clear vpls mac-table" command is executed [PR1664694](#)
- Few protocol sessions remain down causing traffic loss in certain prefixes after quick arpd process disable and enable. The system can be recovered from erroneous state by executing "restart routing gracefully" in CLI. [PR1665362](#)
- On all Junos platforms, incorrect sensor base telemetry data are collected when multiple SR-TE tunnels are configured with at least one uncolored, sharing the same single hop segment list. [PR1665943](#)
- UDP Telemetry may not work when subscribes to /junos/system/linecard/intf-exp/sensor [PR1666714](#)
- Faulty FPC (Flexible PIC Concentrator) on the MX platform chassis exhibiting multibit ECC (Error Checking and Correction) error (L2 cache error) will trigger this issue. The whole chassis goes down until the faulty FPC is removed from the chassis. [PR1670137](#)
- In case Port is DOWN then Tx Laser need to enable via cli-pfe> prompt. [PR1673892](#)
- On SyncE over LAG interfaces, if the end points have different ESMC QL configured, on one of configured syncE interface, ESMC QL is toggling between PRC and DNU and sync-E does not lock and moves to holdover state. [PR1677131](#)

- Not fixed in the Current release, the issue was recreated only with IXIA connection. Arp response is not received in the DUT port to store the destination MAC address. unable to determine if the issue is with the MX port or medium or IXIA port. [PR1677624](#)
- There will be drop of syslog packets seen for RT_FLOW: RT_FLOW_SESSION_CREATE_USF logs until this is fixed. This will not impact the functionality. [PR1678453](#)
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. [PR1679919](#)
- The issue here is that we see ?MQSS(0): DRD: Error: WAN reorder ID timeout error? once per PFE during bootup of FPC. This happens because during the FPC bootup some control packet from vmhost comes before the PFE init is fully complete. Because of this the EA Asic is not able to process the packet and throwing the error. The fix involves complex changes in the bootup sequence of ASICS and will result in other major issues. The original issue has no functionality impact. It is just one error per PFE seen during the FPC reload case only. At that time the traffic is not started yet and once the system is up no other impact is seen due to the Error. Hence the issue will not be fixed. Any "WAN reorder ID timeout error" during the bootup of FPC can be safely ignored. [PR1681763](#)
- The Queue stats may show constant PPS / bps after interface is disabled. The stats don't increment and remain same when the interface went down. However it is a display issue which will be fixed in future releases [PR1685344](#)
- New CLI commands addition to support RE and Chassis power-cycle under request vmhost hierarchy [PR1686577](#)
- If MVRP is enabled on an MSTP enabled interface, the interface will be made part of all the existing instances on the switch, So, if there are two interfaces between R1 and R2 as below: R1(et-0/0/1 and et-0/0/2)=====(et-0/0/1 and et-0/0/2)R2 And one interface is MVRP enabled (say et-0/0/1), and et-0/0/2 is not MVRP enabled. By configuration et-0/0/1 is part of MSTI-1 and et-0/0/2 is part of MSTI-2. MSTI-1 is running on vlan-100 and MSTI-2 is running on Vlan-200. R2 in this case, is advertising only vlan-100. The MVRP enabled interface will become part of all the MSTIs(MSTI-1 and MSTI-2 both) configured on the device and it will take part in the FSM of all the MSTIs. Although et-0/0/1 is not member interface of vlan-200(corresponding to MSTI-2). This potentially can cause a problem where et-0/0/1 although not a vlan-200 member, will go into FWD state and et-0/0/2, genuine member of vlan-200 goes into BLK state for MSTI-2. So, when traffic is received in vlan-200 it will be sent out of et-0/0/1, and it will be dropped. [PR1686596](#)
- Junos has a limitation of 255 characters for resource names. Increasing the limit will have implications on the CLI output and same changes will needed to be propagated to lower layers where the resources are served from. [PR1695980](#)

- "suppressed-prefix-count" can be retrieved with the following RPC via Netconf, as this is not included as part of OpenConfig yang model. `rpc get-bgp-summary-information get-bgp-summary-information`
rpc[PR1696022](#)
- set routing-options transport-class auto-create When the above command is configured, RPD creates/deletes tables dynamically. There is a flaw in the Delete Flow, which does not delete the table from the kernel, and when the next time RPD is adding the same table, the operation is stuck with EEXISTS error, as previous delete was never done. Any subsequent commit will resolve this issue.[PR1696199](#)
- FIPS mode is not supported in this release for SRXSME devices.[PR1697999](#)
- On all Junos and Junos Evolved platforms supporting MACsec (Media Access Control security), traffic drop can be seen when MACsec Primary and fallback sessions are configured and there is a higher transmit-delay time (~6 sec). This is a timing issue and occurs when switching from primary to fallback or vice-versa when changing the pre-shared-key's CAK (Connectivity Association Key) value in CLI (Command Line Interface) on the non-key-server side and at the same time key-server generates a new SAK (Secure Association Key) for pre-shared-key due to expiration of sak-rekey timer, i.e. sak-rekey and primary to fallback key-switch both occurs at the same time. This issue is self-recovered once the SAK from fallback is recovered.[PR1698687](#)
- When subscribing to sensor paths `"/junos/system/linecard/packet/usage/"`, `"/junos/services/label-switched-path/usage/"` or other line card (PFE) sensor paths in gNMI subscription mode, packet drops may be seen in the CLI command `"show network-agent statistics gnmi detail"` output. The collector output may also contain missing sequence numbers. For example, the sequence number output may be 0, 3, 6, 9, 12, etc. instead of 0, 1, 2, 3, 4, etc. [PR1703418](#)
- Port-location start or stop command option is not available for all active 1g ports in request chassis port-led start port. [PR1705298](#)
- In Chassisd, Junos Telemetry Interface thread takes more time in streaming of Junos Telemetry Interface packets because of volume of data and number of sensors involved with this daemon. Junos Telemetry Interface thread engages for more time to process streaming events causing Chassisd master thread to lose receive or send keepalive messages to or from other Routing Engine, which eventually causes automatic Routing Engine switchover in most of the cases. [PR1706300](#)
- Current stack and display is correctly set to 128 ports that is qualified on all MX10K8 linecards[PR1706376](#)
- MX10K-LC480: G.8275.1: PTP to PTP and PTP to 1PPS Noise transfer performance not meeting G.8273.2 mask[PR1707127](#)
- MX10K-LC480: G.8275.1: SyncE to PTP and SyncE to 1PPS Noise transfer performance not meeting G.8273.2 mask[PR1707128](#)

- MX10K-LC480: G.8275.1: SyncE to PTP and SyncE to 1PPS Transient Response not meeting G.8273.2 mask [PR1707129](#)
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed, results in a few packet drops for a very short duration. PTP remains lock and there is no further functional impact. [PR1707944](#)
- When the 4X10G SR optics is connected with peer 1G SX the links come up and traffic will flow normally. But if there is any link fault on DUT having 4x10G SR (due to cable cut, peer 1GSX optics OIR), the links at local end may or may not come up and the RX LOS alarm will be present at the local 4x10G SR optics lane. The links can be brought up back by doing \$x10G optics OIR (jack out and JAck in) at the DUT. [PR1712421](#)
- When we change speed from 100G to 1G on a given port i.e. port config was 100G and then we change to 1G the links dont come up. This is not applicable to scenario where we are in default 100G pic-mode on bootup i.e. all ports in 100G and then we configure one port to 1g (it will work there). [PR1712665](#)
- When LAG is configured with mixed speed interfaces switching to a secondary interface of different port speed - 1G to 10G link, results in a short spike at Max TE. There is no other functional impact and PTP remains locked. [PR1716124](#)

Interfaces and Chassis

- MediaType value in SNMP/Jvision is not correct at the beginning after the switch comes up only for the DOWN interfaces where copper mediaType is connected till the link is not UP. This value is correct always in CLI output. Below are the recovery ways 1. Bring the link up (Connect the other side) 2. Restart dcd daemon [PR1671706](#)
- This issue is specific to MXVC only and the issue is not seen during manual execution of the test case. Issue is seen only with the test script that too rarely and hence the exact trigger of the issue is not clear. [PR1686425](#)
- The link-local address is not assigned for the loopback interface after the upgrade or the device reboot on all Junos OS Evolved platforms. The impact depends on how the loopback interface is used in the configuration. It can cause a connectivity issue and traffic impact when it is used for the routing process. [PR1695502](#)

Junos XML API and Scripting

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

Layer 2 Features

- In a H-VPLS network with VPLS hot-standby and the knob 'routing-options forwarding-table vpls-hotstandby-convergence' enabled on spokes, if the active hub is rebooted, 20-25 seconds loss for inter-zone traffic stream is seen. This is due to hubs in other zones connected by full-mesh ldp, starting global repair before spokes starting local repair. [PR1699645](#)

MPLS

- Ingress will retry after LSP stay down for extended period of time or customer can clear lsp to speed up the retry. [PR1631774](#)
- When instance loopback interface is disabled. That happens due to change of router-id when a loopback interface is disabled and LDP sets the new router id as LDP label space id for IPv4 connection in primary Routing Engine instead of the id from dual-transport configuration but backup Routing Engine picks IPv4 connection id from dual transport configuration. This way there is a mismatch between the LDP IPv4 connection id in primary and secondary Routing Engine and results in failure of synchronization. [PR1703176](#)
- Tag rnh appears to be freed somewhere in the corner case, but the relevant pat node has been missed to delete from the tag patricia tree. That makes tag rnh/(pat_node->Tnh) a dangling pointer and later on, it results in a crash while accessing invalid pointer addresses in the tag rnh/Tnh structure. [PR1707053](#)
- When an LSR acts as a Point of Local Repair (PLR) as well as a Merge Point (MP) for an LSP during a double failure scenario, the LSR incorrectly originates one or two PathErr messages with RoutingProblem (code=24/2) instead of originating PathErr with NotifyError (code/subcode=25/3). This will not cause any service impact if the ingress LER would not react adversely to RoutingProblem error (code=24/2). [PR1713392](#)

Network Management and Monitoring

- After upgrading the device, yang package with lower revisions are available. [PR1693646](#)

Platform and Infrastructure

- BFD flap is observed after executing VPLS `mac-table clear` command. [PR1686220](#)

Routing Protocols

- On all Junos OS and Junos OS Evolved platforms, the rpd can crash when protocol independent multicast (PIM), multicast only fast reroute (MoFRR) configuration is present and some network churn event such as continuous interface cost changes, resulting in a change of active and backup paths for equal cost multi-path (ECMP) occurs. There will be service impact because of the rpd crash but the system self-recovers until the next crash. [PR1676154](#)
- The IS-IS yang is uplifted to 1.0.0 version which has major change in existing OC path that was supported earlier. Since OC path has change, same need to be reflected in translation script which is not done. As part of D27 release for cloud, translation script will be modified with newer OC path. Till then supported older OC config is broken. eventually D27 code will come back to DCB and things will work fine after that. [PR1686751](#)

Services Applications

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

VPNs

- When MVPN protocol has separate route targets configured, then the both address families are disabled. RPD infrastructure parsing does not check if MVPN protocol is disabled. Therefore, it creates the auto policies for route-targets if configured. So, if those policies are not marked as active in MVPN configuration flow, it does not get resolved and thereby the policy object might not be valid thus generating a core file. [PR1700345](#)

Resolved Issues

IN THIS SECTION

- [Class of Service \(CoS\) | 95](#)
- [EVPN | 96](#)
- [Forwarding and Sampling | 96](#)
- [General Routing | 96](#)
- [High Availability \(HA\) and Resiliency | 104](#)
- [Interfaces and Chassis | 104](#)
- [Layer 2 Ethernet Services | 105](#)
- [Junos Fusion Satellite Software | 105](#)
- [MPLS | 105](#)
- [Network Management and Monitoring | 106](#)
- [Platform and Infrastructure | 106](#)
- [Routing Policy and Firewall Filters | 107](#)
- [Routing Protocols | 107](#)
- [Subscriber Access Management | 109](#)
- [User Interface and Configuration | 109](#)
- [VPNs | 110](#)

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

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

Class of Service (CoS)

- The oid tree `jnxCosQstatEntry` returns nothing for some interfaces after restarting class-of-service. [PR1693977](#)
- The aggregated Ethernet link flaps on MX Series platforms with MPC10, MPC11, and LC9600 when you configure high or medium priorities on the queue. [PR1699714](#)

EVPN

- PBB-EVPN PE cannot learn remote CE MAC address on enabling ARP suppression. [PR1529940](#)
- The kernel might crash in an EVPN multi-homed scenario. [PR1649234](#)
- In EVPN-MPLS multihoming scenario DF election will get stuck in the preference-based state. [PR1662954](#)
- Layer3 inter-subnet routing will fail if there is no reachability for the remote IP-host route. [PR1669585](#)
- EVPN MPLS traffic drop can be observed in a multi-vendor PE CE setup with single-active LAG. [PR1680421](#)
- In the EVPN-MPLS multihoming scenario, MAC-IP route deletion and addition result in traffic drop. [PR1691132](#)
- RPD core file is observed due to remote bgp routes being flashed as active routes. [PR1692249](#)
- A configuration change leads to generate an rpd core file for the EVPN migrated instance. [PR1701632](#)
- ARP/ND doesn't resolve when extended-vlan-list is configured for the specific VLAN. [PR1702016](#)

Forwarding and Sampling

- Deactivating and activating the GRES causes churn in dfwd filter addition or deletion. [PR1697959](#)

General Routing

- Error message seen in clksyncd logs with SyncE/PTP configuration "ESYNC-Error:ferrari_zl30362_reg_write: Error, EEC(0) not yet initialized". [PR1583496](#)
- During reboot, "warning: requires 'idp-sig' license" can be seen on the screen even when the device has valid license. [PR1594014](#)
- On backup Routing Engine during GRES, you might see "RPD_KRT_KERNEL_BAD_ROUTE: krt unsolic client.128.0.0.5+62000: lost ifl 0 for route" warning messages. [PR1612487](#)
- Configuring delegated BFD sessions on routing-instance might fail to come up. [PR1633395](#)

- IPv6 master-only IP address does not move to the new master Routing Engine after a switchover. [PR1648371](#)
- The user-defined speed does not take effect on the aggregated Ethernet interface in certain scenarios on Junos OS platforms. [PR1649958](#)
- MX960:: Syslog errors HALP-trinity_vbf_flow_unbind_handler:1107: vbf flow 624626: ifl 526 not found,fpc5 vbf_var_get_ifs:754: ifl not found,PFE_ERROR_NOT_FOUND seen frequently on MPC7E in 5.5K DCIP/10kPPPoE FTTB Stress Test. [PR1650598](#)
- Telemetry is reporting In-Errors when you configure the ignore-l3-incompletes statement. [PR1655651](#)
- DHCP packets getting looped in EVPN-VXLAN setup. [PR1657597](#)
- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. [PR1657704](#)
- MX204 - SSH non-default port configuration causes FPC offline after upgrading to Junos OS Release 21.4. [PR1660446](#)
- The port LEDs do not light up when 40G/100G physical interfaces are up. [PR1660532](#)
- Family bridge disappears on commit check when you configure network-services LAN. [PR1661057](#)
- GNF : No streaming data received for /telemetry-system/subscriptions/dynamic-subscriptions/ [PR1661106](#)
- The fxpc crashes on enabling RPF check. [PR1662508](#)
- Primary and backup NHG late binding is not supported, so the backup nhg should be created before the primary nhg and removed in the reverse order. [PR1663310](#)
- RE1 alarms persistent even after removed from slot. [PR1664544](#)
- Switch Fabric Board information for supporting PTP on MX10008 with MX10K-LC2101 LC(s). [PR1664569](#)
- Na-grpcd process generates a core file in the telemetry services. [PR1665516](#)
- Traffic loss might occur when you configure the VRRP over the aggregated Ethernet interface. [PR1666853](#)
- Shaping-rate is not taking 20 bytes of overhead into account. [PR1667879](#)
- GRPC server do not decode leaf-list correctly. [PR1668319](#)
- Performance monitoring for 400ZR optics reporting data as suspect with reason "Int Too Short". [PR1670033](#)

- EVPN multicast traffic might impact because of routes getting stuck in the kernel routing table (krt) queue. [PR1670435](#)
- Fragment frames errors will be seen on the 400G interface. [PR1671065](#)
- Traffic loss may be seen due to SPC3's packets getting stuck. [PR1671649](#)
- You will observe traffic loop on configuring ESI on the physical interface. [PR1672631](#)
- The vmcore might be seen with the back-to-back reboot. [PR1672731](#)
- Packet Forwarding Engine core file is seen when the CPCD service is modified. [PR1675985](#)
- On LC480 MX Series line-card with 1G interface PTP performance will not be good. [PR1677471](#)
- Traffic drop can be seen for MPC7/8/9 during unified ISSU in a specific scenario. [PR1678130](#)
- Packet Forwarding Engine memory usage impacts after the GRES. [PR1678217](#)
- show interfaces diagnostics optics interface shows all 0 on 100/400G port on MPC10E card. [PR1678716](#)
- MX304 MACSEC over pseudowire issues. [PR1678726](#)
- Physical interface delete before MACsec object delete causing the interface link to go down. [PR1678755](#)
- The rpd process crashes when a delegated LSP with IPv6 install prefix is configured. [PR1678874](#)
- PTP servo is stuck in ACQUIRING state with high CF when configured with LAG on MX10k8 with JNP10K-LC480 linecards. [PR1679657](#)
- GNMI: "/components/component[name=*/state/oper-status" has duplicate entries for FPC and Routing Engine components. [PR1679823](#)
- Destination mask length reported in sFlow exported packet is lesser compared to the value seen in show route forwarding-table destination. [PR1680040](#)
- The process bbe-smgd on the router might stop processing new PPPoE subscribers session. [PR1680453](#)
- LED status on backup RCB never turns on after reboot. [PR1681609](#)
- System uptime display is shown in minutes instead of seconds. [PR1681656](#)
- FPC going to fault state with major alarm - Power Failure on upgrading. [PR1682659](#)
- Auto-negotiation is not getting reflected on the MPC7E-10GE line card. [PR1682962](#)

- Traffic loss is seen with port-mirroring is enabled on aggregated Ethernet interface in multicast downstream. [PR1683192](#)
- clear interfaces statistics all takes more than 9 minute due to invalid PIC configuration inside GNF. [PR1683312](#)
- You'll observe a traffic drop with inter-vlan configuration when deactivating and activating the EVPN routing instance. [PR1683321](#)
- Query returned nothing from the database while validating sync_response. [PR1683552](#)
- [MAP-E] PPE errors seen during deactivate/activate of partial reassembly - ZTCHIP_MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x227fa5). [PR1683845](#)
- srv6-oam: more than one label stack is not supporting,gives as "Maximum number of sids supported is 0" error in srv6 ping in LC9600. [PR1683883](#)
- The rpd crashes when SRv6 service routes resolve over SRv6 SRTE policies using older resolution scheme. [PR1683993](#)
- The l2cpd process crash may be observed when disabling RSTP on an interface. [PR1684072](#)
- MFT: rpd generates a core file at **spring_te_stats_info_lookup_transit_stats_info_from_ingress_stats_info** on Backup Routing Engine by deactivating and then activating the source-packet routing multiple times. [PR1684111](#)
- TI-LFA backup path is not computed which effects slow convergence in case of failures. [PR1685064](#)
- You'll observe multiple bbe-smgd core files resulting in subscribers being lost or failing to login in the Enhanced subscriber scenario. [PR1685070](#)
- license-check might generate a core file on the MX Series routers. [PR1685433](#)
- PICs on the GNF failed to come online after the chassisd restarts. [PR1685453](#)
- Errors are seen on committing CoS configurations.[PR1685482](#)
- With BMP RIB-IN and BMP RIB-OUT configured on MX Series routers, large number of BGP routes remain in holddown state after route churn. [PR1685510](#)
- The fibd process will crash when a large number of interfaces are deleted and added back. [PR1685995](#)
- The 100G interfaces on an MPC11E remain in a down state on MX Series platforms after a system or FPC restart. [PR1685997](#)
- The l2ald core seen after zeroize. [PR1686097](#)

- The rpd might crash when two separate next-hops in rpd map to the same next-hop-index in the kernel. [PR1686211](#)
- VPLS traffic loss might be seen when deleting and adding a routing-instance. [PR1686523](#)
- MPC10E line card will reboot due to the sensord crash. [PR1686766](#)
- The PIMv6 is not getting enabled for L2TP subscribers. [PR1687138](#)
- The rpd process crash is seen when the BGP SR-TE tunnel is marked for deletion. [PR1687287](#)
- Traffic loss is seen with latest ZR-M firmware (61.23) during optics power up. [PR1687583](#)
- CoS memory errors are seen when chassis traffic-manager enhanced-priority-mode is configured. [PR1687642](#)
- The FPC crashes with a "flexible-match-mask" condition. [PR1687862](#)
- On Junos OS and Junos OS Evolved platforms delegated LSP control will not be returned to the PCC in a specific scenario. [PR1687885](#)
- The LLDP output packets are not transmitting on the em0 interface of Junos OS and Junos OS Evolved platforms. [PR1688023](#)
- A kernel crash can be seen with MIC-3D-8DS3-E3 installed. [PR1688315](#)
- The CoS queue burst size computation was incorrect when the explicit queue shaping rate was not configured, causing initial packet drops. [PR1688416](#)
- Telemetry sensor will not stream data if using key value as wildcard '*' character for gNMI in the Packet Forwarding Engine supported sensor. [PR1688613](#)
- All VPLS/Ethernet L2 traffic destined to VMAC will be flooded across the VPLS instance. [PR1688629](#)
- Rapid interface configuration changes on MPC11E might result in interfaces not coming up. [PR1688767](#)
- The LACP might get stuck in a continuous update loop in the MC-LAG scenario. [PR1688958](#)
- Packet Forwarding Engine wedge will be seen due to fast link flaps. [PR1688972](#)
- DCSPF LSPs remain down indefinitely after changing the router-id of the ingress router. [PR1689067](#)
- The logical interface policer is not working as expected when applied to filter input-list/output-list. [PR1689199](#)
- "failed to get template var id" error messages are generated by FPC when BFD liveness detection is negotiated by DHCP subscriber which has lawful intercept enabled. [PR1689621](#)

- A 1G port on a QSFP-4x10G transceiver will be down sometimes after the FPC restart. [PR1689644](#)
- Traffic drop on the system when traffic hits an unresolved destination. [PR1690679](#)
- The process rpd crash will be observed with the SRTE tunnel delete. [PR1691459](#)
- PCS errors and framing errors on 100GE interfaces on certain Junos OS platforms. [PR1692063](#)
- The firewall bridge filter policers (attached to AE interface) are not working on all Junos MX Series platform with MPC10 card upon deactivate-activate a term intended to limit overall traffic. [PR1692070](#)
- CBC-FPGA and RE-FPGA firmware upgrades fail. [PR1692186](#)
- JNP10K-LC9600: G.8275.1: SyncE to PTP and SyncE to 1PPS Transient Response not meeting G.8273.2 mask. [PR1692202](#)
- ALG child session will not be transported through the DS-Lite tunnel which might lead to traffic failures in absence of a direct route to the host. [PR1692525](#)
- JNP10K-LC9600: G.8275.1: 2way/cTE fails to meet class-B with asymmetric port combinations. [PR1692746](#)
- The rpd crash will be observed when there is a temporary recursion loop and routes are flapping. [PR1692776](#)
- The FPC crash is observed with out-of-bound access to the filter action table. [PR1692781](#)
- The fxpc core file is generated and an FPC restart results in traffic impact. [PR1692993](#)
- Traffic loss is observed when the ECMP path is IRB over AE (IPv4->MPLS). [PR1693424](#)
- Context deadline exceeds on while adding NH, IPv4. [PR1693567](#)
- The fabspoked-pfe process crashes when a FATAL ERROR occurs in the Packet Forwarding Engine. [PR1693697](#)
- CM alarm is not triggering for Packet Forwarding Engine going into fault state. [PR1693710](#)
- Traffic loss will be seen when MACsec is configured. [PR1693730](#)
- NDP can't resolve neighbor after clearing IPv6 neighbor. [PR1694009](#)
- dot1xd.core-tarball.0.tgz is observed at #0x009113f0 in __mem_assert(). [PR1694129](#)
- license-check warning reported on backup Routing Engine by commit or commit check. [PR1694935](#)
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device [PR1695057](#)

- On Junos OS MX Series Virtual chassis with LC2101 upstream SyncE source interface stuck in abort state. [PR1695156](#)
- BMP EOR is sent with wrong peer address causing BMP failure. [PR1695320](#)
- MPC11E goes offline with "fpc-slice" configured. [PR1695510](#)
- The Routing Engine mastership switchover will not be triggered when the internal master interface on VM Host is down. [PR1695794](#)
- An rpd crash is observed while creating indirect-next-hop in the BGP sharding environment with bgp.l3vpn.0 with next-shop as a color route [PR1696035](#)
- FPC crash is observed in GNF scenario with CoS configuration [PR1696089](#)
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash [PR1696428](#)
- PTX10004/8/16 EVO : LC Status LED MIB jnxLEDDescr.3.7.x.0.0 returns undefined 0 value due to read error [PR1696500](#)
- MX304 : Occasionally, after a chassis power cycle, the backup Routing Engine is in Present state and the "Loss of communication with Backup Routing Engine" alarm is seen [PR1696816](#)
- License key is not installed after upgrade [PR1696879](#)
- Time error spikes seen during switchover of upstream source clock [PR1696880](#)
- The dot1x authentication will not be enabled on interfaces with specific configuration combination [PR1696906](#)
- In the rare scenario, huge PTP Time errors are introduced and propagated to the downstream devices after the chassis reboot [PR1696957](#)
- Time error observed on JNP10K-LC2101. [PR1697167](#)
- Stoppage of statistics update on MPC10E .[PR1697215](#)
- FPC crash will be observed when firewall filter is unconfigured and reconfigured with same index [PR1697404](#)
- The agentd process crash might crash in a telemetry scenario [PR1697986](#)
- On Junos OS platforms where the MPLS is resolving over IPv6 route traffic drop is seen. [PR1698516](#)
- Transit tunnels fails and remains down on all Junos OS based MX Series platform with IKE-NAT-ALG enabled .[PR1699115](#)
- Output of show chassis ethernet-switch statistics includes 32 bit values which may overflow. [PR1699136](#)

- rpd core is generated while doing a few PRPD operations at backtrace @task_mem_cookie_findsizes, @grpc_slice_refcount::Unref, @grpc_slice_unref_internal, @grpc_core::CallCombiner::~~CallCombiner [PR1699356](#)
- The rpd crash is observed when rib-sharding configured [PR1699557](#)
- VLAN tags are imposed incorrectly when traffic is routed over IRB going out of the access interface [PR1700321](#)
- User plane subscriber management daemon process crash when distributed multicast service is activated on several hundred subscribers [PR1700571](#)
- Enabling optic configuration mismatch alarm for MPC11 and LC9600 [PR1700606](#)
- JDI-REG:MX10008 :: core-renault-bbe-fpc0-indus.elf-crashinfo.0 core seen during teardown [PR1700909](#)
- JNP10K-LC9600: G.8275.1: Multiple GRES operation resulting in huge time error [PR1701017](#)
- FPC restart and core dump generated in MPLS scaled scenario with "always-mark-connection-protection-tlv" configured [PR1701147](#)
- Traffic loss is seen due to interface flap when changing speed from 10G and 1G [PR1701183](#)
- On Junos platforms with MS-MPC cards the IKE ALG inactivity timeout value stays fixed [PR1701305](#)
- Traffic loss is seen on MPC10E due to null pointer access without any safe check [PR1701320](#)
- On Junos OS Evolved platforms, the traffic impact is seen as the "set system process routing enable/disable" knob is not working as expected [PR1702734](#)
- The l2ld process will crash when an IFL is changed to trunk mode and a new VLAN is added [PR1703226](#)
- RPF firewall filter errors during DHCP dual stack subscriber logout [PR1703270](#)
- Routing Engine will crash when static route duplicates with an interface IP address [PR1703940](#)
- EAP authentication might not be successful with 802.1X server-fail configuration [PR1705490](#)
- No network reachability when routing-service enabled for PPPOE subscriber over AE [PR1706446](#)
- The Inline Flow Monitoring is not working on Junos MX-VC platforms [PR1708485](#)
- Ports with QSA adapter are down [PR1709817](#)
- The interface does not come up or keeps flapping [PR1712007](#)
- FPC memory leak will cause FPC crash [PR1712076](#)

- The traffic is dropped while passing through VCP link on MX Series Virtual Chassis with MPC10 line card. [PR1712790](#)
- RPD core file is seen after the switchover. [PR1694773](#)

High Availability (HA) and Resiliency

- Traffic will be impacted if GR-ISSU fails. [PR1694669](#)
- The rpd crashes and generates a core file when any commit is performed. [PR1701146](#)

Interfaces and Chassis

- Management interface speed is incorrectly reported as 10G instead of 1G. [PR1636668](#)
- The Packet Forwarding Engine I/O chip setup failed for some interfaces and causes those interfaces missing in Packet Forwarding Engine after backup chassis upgraded via sequential upgrade. [PR1670345](#)
- VRRP master-master condition might occur when there are more than two devices in the VRRP group. [PR1680178](#)
- In a rare scenario, the FPC/SLC will get stuck in the ready state after a restart. [PR1682271](#)
- If VRRP authentication key is more than 16 characters it is ignoring remaining characters. [PR1683871](#)
- Traffic is getting impacted as interface hold-time is not working with wan-phy framing. [PR1684142](#)
- Subscribers will fail to negotiate the PPP session and be unable to login post-software upgrade. [PR1686940](#)
- Incompatible or unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. [PR1692404](#)
- VRRP master session on aggregated Ethernet logical interface having child links on satellite device stops transmission post GRES. [PR1697394](#)
- The backup Virtual Chassis router could become master after the system reboot. [PR1697630](#)
- FPC offline can be seen on the MX Series Virtual Chassis during the sequential upgrade. [PR1706268](#)

- MX304 :: Not getting the expected values while verifying ['linktrace_egress_mac_address', 'linktrace_flags', 'linktrace_ingress_mac_address', 'reply_ttl'] on devices. [PR1707126](#)
- MXVC - MPC7E firmware upgrade tftp timeout. [PR1713502](#)

Layer 2 Ethernet Services

- MX240: Verify VRRP statistics fails after deactivating the access interface. [PR1666943](#)
- DHCP packets sent to the client have the Option 82 suboption length set to 0. [PR1684521](#)
- The ethernet switching tables do not synchronize between two PE devices. [PR1686546](#)
- IPv4 ALQ does not work with authentication. [PR1688272](#)
- DHCP packets might not be sent to the clients when 'forward-only' is reconfigured under the routing instance. [PR1689005](#)
- A dcd process crash is observed continuously when the dhcp-service is restarted. [PR1698798](#)
- DHCPv6 client options missing in solicit message if they exceed a certain length. [PR1702831](#)

Junos Fusion Satellite Software

- The Junos Fusion Satellite device will be stuck in the SyncWait state. [PR1682680](#)

MPLS

- The rpd core is seen due to IGP database and BGP LS database out of sync. [PR1655031](#)
- Traffic loss will be seen in an LDP->BGP-LU stitching scenario. [PR1670334](#)
- VCCV BFD session will be down as the periodic ping will not work as expected in a seamless MPLS scenario. [PR1670711](#)
- In the RSVP-TE scenario, with Entropy label capability is enabled during MBB issues handling Resv messages. [PR1681403](#)
- The Routing Engine crashes when MPLS next-hop is created and deleted frequently. [PR1681892](#)

- LDP IPv6 session fails to come up in dual transport scenario. [PR1683410](#)
- After disabling and then enabling the MPLS, targeted LDP session do not get established. [PR1687834](#)
- On a controller based MPLS setup with container LSPs, rpd daemon crashes after LSP deletion occurs. [PR1690458](#)
- The rpd crash will be observed during the MPLS label block allocation. [PR1694648](#)
- Restarting FPC or router reboot might causes some CCC interfaces to go down due to a 'Remote CCC down'. [PR1694777](#)
- The rpd process crash is seen when PCCD is deactivated. [PR1694957](#)
- MFT: rpd cores
@rt_check_open,rsvp_adjust_route_traffic_engineering,rsvp_route_traffic_engineering_change_job
after enabling/disabling mpls-forwarding TE configuration statement. [PR1696017](#)
- RPD(LDP) cores with configurations like BGP static routes or SR-TE routes in INET.0. [PR1697498](#)
- [MX]L2VPN ping is failing when UHP rsvp LSP is used. [PR1697982](#)
- The rpd core and traffic loss is observed on Junos OS and Junos OS Evolved platforms. [PR1701420](#)
- Memory leak issue in TED. [PR1701800](#)
- LDP flaps will be observed having LT interface with VLAN and LDP running between the logical-system instance and global instance. [PR1702220](#)

Network Management and Monitoring

- Aggregated ethernet interface beyond 1099 are allotted 0 snmp index. [PR1683264](#)

Platform and Infrastructure

- The MPC hosting an aggregated Ethernet member interface with a shared bandwidth policer configured at the aggregated Ethernet might crash upon encountering an HMC fatal error. [PR1666966](#)
- Traffic drop observed with SP style configuration for the logical tunnel in layer2 domain. [PR1669478](#)

- Layer 2 packets other than IPv4/IPv6 (e.g. CFM) will get forwarded as out of order via MPC10 and MPC11 in the egress direction. [PR1670316](#)
- The interface on the device will go down when one or more interfaces are connected to the Advantech3260 device at another end. [PR1678506](#)
- The traffic loss duration increases during the LSP switchover. [PR1681250](#)
- The line card gets crashed during node/interface statistics reporting with resource monitoring. [PR1681533](#)
- Incorrect programming of next-hop based on RVT interface hosted on MPC10E/MPC11E, LC9600, MX304 leads to traffic drops. [PR1682383](#)
- BGP session flap with error BGP_IO_ERROR_CLOSE_SESSION. [PR1685113](#)
- Probes received counter is not correct when set "moving-average-size" > "history-size" under TWAMP client configuration. [PR1685952](#)
- Packet Forwarding Engine will be disabled whenever XQ_TOE CM error is being detected. [PR1692256](#)
- Packets received from type-5 tunnel are not sent out to local CE in EVPN-VxLAN scenario. [PR1696106](#)
- The egress rewrite-rule might not work as expected for traffic entering the AE interface. [PR1700860](#)
- The TWAMP test session packets are dropped when the payload is less than 52 bytes. [PR1703104](#)
- Severity reclassification of queuing ASIC XQSS and memory parity error auto recovery. [PR1706494](#)

Routing Policy and Firewall Filters

- Error messages are observed while configuring the firewall filter with family inet6 with next-header and no payload-protocol and committing them. [PR1674893](#)

Routing Protocols

- JDI-RCT : PPM crashed at ppm_destroy_distrib_proto_stats_group_entry () . [PR1660299](#)
- SSH access is possible without ssh setting. [PR1664512](#)
- RPD crash might be observed due to multiple sequences of flap events. [PR1669615](#)

- Source/Destination AS fields shows up as 0 in the flow record. [PR1670673](#)
- Traffic loss observed due to multicast routes exceeding the scale for OISM feature. [PR1671901](#)
- The routes with an independent resolution can trigger an rpd crash when the last BGP peer is down. [PR1673160](#)
- BGP or OSPF neighbors will not come up in Junos OS Evolved platforms if IPSEC Security Associations are used to Authenticate the peer. [PR1674802](#)
- KRT queue shows deferred operation while creating IFL after FPC offline/online event. [PR1675212](#)
- The AGGREGATOR attribute will not be set correctly when the independent-domain is configured. [PR1679646](#)
- InboundConvergencePending flag is set after Routing Engine switchover. [PR1680360](#)
- Telemetry for peer-as does not work. [PR1687369](#)
- On single Packet Forwarding Engine with Fusion satellite, LACP is not sending PDUs. [PR1687395](#)
- BGP LU Advertisements fail with the message "BGP label allocation failure: Need a gateway". [PR1689904](#)
- The rpd process crashes on a system running with IGP shortcuts. [PR1690231](#)
- The rpd crash is seen when using a BGP neighbor telemetry subscription in a sharding environment. [PR1692255](#)
- RPD core@task_job_run_common->bgp_rsync_rcv->task_commit_sync_standby_done_notify->task_commit_sync_standby_done->rt_primary_process_standby_done (). [PR1692320](#)
- Configuration check-out failed when applying "irb with inet and inet6" and "inet6.0 static route". [PR1692484](#)
- When Lsys is configured with 'family route-target', there is a certain corner case scenario where Lsys shutdown does not complete. [PR1695050](#)
- Traffic blackholing is observed when removing the BGP routes take a long time to get removed from RIB. [PR1695062](#)
- Commit error when trying to configure rib-group under BGP in no-forward (default) RI. [PR1696576](#)
- Wrong SRTE Secondary path weight makes the secondary path active in forwarding table. [PR1696598](#)
- The BGP Auto-discovered neighborship is not formed after a reboot. [PR1699233](#)

- The BGP graceful-shutdown community is not advertised on Junos OS and Junos OS Evolved platforms. [PR1699633](#)
- OSPF stuck in InitStrictBFD state for the neighbor which doesn't send LLS header. [PR1700966](#)
- Junos OS prefers SRMS advertised label over IS-IS/OSPF SID label advertised via opaque-AS extended-prefix. [PR1702456](#)
- Anycast PIM doesn't work when the peer has an authentication key configured for MSDP. [PR1703707](#)
- FORWARD_NULL:DEV_COMMON_BRANCH. [PR1704834](#)
- With lsp-max-lsp configured some routes are not getting leaked from IS-IS L1 to L2. [PR1704924](#)
- OSPF routes are not getting installed after the interface is flapped. [PR1705975](#)
- A crash can be observed for 'mcsnoopd' process when the VLAN name for igmp-snooping has certain characters. [PR1711153](#)
- On all Junos and Junos OS Evolved platforms with max-lsp-size configured some flex-algo routes are not getting leaked from IS-IS L1 to L2. [PR1711565](#)
- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. [PR1712406](#)

Subscriber Access Management

- The authd process might not report CoS shaping-rate in acct-stop message. [PR1641416](#)
- The authd process crashes during GRES recovery phase. [PR1687998](#)
- A few subscriber sessions will not be up post Routing Engine switchover. [PR1697392](#)

User Interface and Configuration

- The system will ask for password while saving configuration files on single Routing Engine platforms. [PR1665008](#)
- Test Configuration might fail even though the config file is having valid configurations. [PR1671112](#)
- Configuration filtering doesn't work when the logical system is present. [PR1679413](#)

- Show commands may not work after unified ISSU upgrade. [PR1692409](#)
- gNMI GET request fails when OpenConfig is present. [PR1697869](#)
- The mgd process might crash during commit synchronize. [PR1699245](#)

VPNs

- Traffic over IPSec tunnels may be dropped during unified ISSU. [PR1416334](#)
- Routes flapping when configuration changes are applied to custom routing instance. [PR1654516](#)
- Generates a core file when restarting multiple daemons. [PR1682573](#)
- Two-digit numbered interfaces cannot be used as protect-interfaces. [PR1695075](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 111

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

NOTE: Junos OS Release 22.4 is the last-supported release for the following SKUs:

- MS-MPC-128G-BB
- MS-MPC-128G-R
- MS-MPC-128G-SX

- MS-MIC-16G
- MS-MIC-16G-SX
- SCG-TM-BAS

We recommend upgrading to MX-SPC3 **only** for the following SKUS:

- MS-MPC-128G-BB
- MS-MPC-128G-R
- MS-MPC-128G-SX

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, 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](#).

Junos OS Release Notes for NFX Series

IN THIS SECTION

- [What's New | 112](#)
- [What's Changed | 113](#)
- [Known Limitations | 113](#)
- [Open Issues | 114](#)
- [Resolved Issues | 115](#)
- [Migration, Upgrade, and Downgrade Instructions | 115](#)

What's New

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

What's Changed

IN THIS SECTION

- [Software Installation and Upgrade](#) | 113

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

Software Installation and Upgrade

- **Two-step Downgrade (NFX150, NFX250 NextGen, and NFX350)**—You cannot downgrade Junos OS Release 23.1R1 directly to certain releases (listed in the **Target Release** column in [Table 9 on page 113](#)). As a workaround, you can perform downgrade as a two-step activity, in which you downgrade Junos OS Release 23.1R1 first to a corresponding intermediate release (listed in [Table 9 on page 113](#)), and then to the target release.

Table 9: Release Compatibility for Downgrading Junos OS 23.1R1 on NFX Series Devices

Target Release	Intermediate Release
Any 22.4x release earlier than 22.4R2	22.4R2
Any 22.3x release earlier than 22.3R2.	22.3R2
<ul style="list-style-type: none">• Any 22.2x release earlier than 22.2R3.• Any 22.1x release or earlier releases.	22.2R3

[PR1694074](#)

Known Limitations

There are no changes in behavior or syntax 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

- [Interfaces](#) | 114
- [Virtual Network Functions \(VNFs\)](#) | 114

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

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

Interfaces

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

Workaround Deactivate and then activate the aggregated Ethernet interface. [PR1583054](#)

- If you disable the xe ports on NFX350, the ports' admin state appears down but the link state is up. [PR1697877](#)
- On the NFX350 device, even though the ethernet cable is physically plugged in and the `show interface` command displays Front panel LED status as up, the front panel LED is not ON. [PR1702799](#)

Virtual Network Functions (VNFs)

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

Resolved Issues

IN THIS SECTION

- [Virtual Network Functions \(VNFs\) | 115](#)

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

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

Virtual Network Functions (VNFs)

- The NFX350 device stops responding after you delete a VNF with SRIOV interfaces. Also, JDM becomes unreachable. As a workaround, you can power cycle the device. [PR1664814](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 116](#)

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

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

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

We have two types of releases, 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 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
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 PTX Series

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

See the [Junos OS Evolved release notes](#) for PTX Series products that run Junos OS Evolved.

Junos OS Release Notes for QFX Series

IN THIS SECTION

- [What's New | 117](#)
- [What's Changed | 121](#)
- [Known Limitations | 123](#)
- [Open Issues | 124](#)
- [Resolved Issues | 126](#)
- [Migration, Upgrade, and Downgrade Instructions | 131](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 118](#)
- [Dynamic Host Configuration Protocol | 118](#)
- [EVPN | 119](#)
- [Licensing | 119](#)
- [Routing Policy and Firewall Filters | 120](#)
- [Routing Protocols | 120](#)

- Virtual Chassis | 120
- VPNs | 120
- Additional Features | 121

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

Authentication and Access Control

- **802.1X MAC RADIUS authentication with global password (EX Series except EX4300 and QFX Series that support 802.1X authentication)**—In earlier releases, you used the client's media access control (MAC) address as the username and the password for MAC RADIUS authentication. Starting in Junos OS Release 23.1R1, you can configure a global password for all the MAC RADIUS authentication sessions by using the `password password-string` configuration statement at the `[edit protocols dot1x authenticator mac-radius]` hierarchy level.

[See [Configuring MAC RADIUS Authentication \(CLI Procedure\)](#) and [password \(MAC RADIUS Authentication\)](#).]

Dynamic Host Configuration Protocol

- **Additional client options from DHCP snooping (EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-48P, EX4100-F-24P, EX4100-F-48T, EX4100-F-24T, EX4100-F-12P, EX4100-F-12T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, QFX5110, QFX5110-VC, QFX5110-VCF, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS Release 23.1R1, you can configure DHCP snooping to collect additional client options such as the hostname, server ID, and client ID. The additional client options can be used for analytics using Juniper Mist Cloud Services.

To configure DHCP snooping to collect additional client options, use the `mine-dhcp-client-options` and `mine-dhcpv6-client-options` (for DHCPv6) configuration statements at the `[edit vlans vlan-name forwarding-options dhcp-security]` hierarchy level.

To view the DHCP client options along with other binding information, use the `show dhcp-security binding detail` and `show dhcp-security ipv6 binding detail` (for DHCPv6) operational commands.

[See [dhcp-security](#), [mine-dhcp-client-options](#), [mine-dhcpv6-client-options](#), [show dhcp-security binding](#), and [show dhcp-security ipv6 binding](#).]

EVPN

- **Determine IRB interface state changes based on local and remote connectivity states in EVPN fabrics (EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX2010, MX2020, vMX, QFX5110, QFX5120-48T, QFX5120-48Y, QFX5210, QFX10002, QFX10002-60, and QFX10008)**—Starting in Junos OS Release 23.1R1, the provider edge (PE) devices in an EVPN fabric consider the following factors when determining the state (up or down) of an L3 integrated routing and bridging (IRB) interface. These factors apply to an L3 IRB interface that is associated with a bridge domain or a VLAN in an EVPN instance (EVI).

- Associated local L2 interface states

To customize the L2 interface name and other parameters that the device uses to compute the IRB interface state, configure the `interface-state` statement at the `[edit interfaces irb unit n]` hierarchy.

- Remote provider edge (PE) device reachability based on the network isolation state of the bridge domain or the EVI

The device includes the states of the associated EVPN overlay tunnel interfaces in the network isolation state evaluation.

To define the parameters that determine when an EVI or a bridge domain is in a network isolation state:

1. Configure the `network-isolation group group-name` statement at the `[edit protocols]` hierarchy level to define a network isolation profile using the available options.
2. Assign the network isolation group profile to a bridge domain or an EVI using the `network-isolation-profile group network-isolation-group-name` statement at these hierarchy levels:
 - Bridge domain—`[edit bridge-domain bd-name bridge-options]`
 - EVI—`[edit routing-instance instance-name switch-options]`

[See [Determine IRB Interface State Changes from Local and Remote Connectivity States in EVPN Fabrics](#), [interface-state](#), and [network-isolation](#).]

Licensing

- **Support to trigger license alarm at configured time interval (EX Series, MX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 23.1R1, you can set the time interval at which you want to trigger alarms for features or capacity that do not have licenses installed.

To set the alarm log frequency, use the command `log-frequency` in the `set system license` hierarchy.

[See [Managing Licenses](#).]

Routing Policy and Firewall Filters

- **Support for the IPv6 unicast address-specific BGP extended community attribute (JRR200, QFX Series, and vRR)**—Starting in Junos OS Release 23.1R1, we support the IPv6 unicast address-specific BGP extended community attribute. You can configure the VRF route target with the IPv6 extended community. You can encode each IPv6 unicast address-specific extended community as a 20-octet file.

To accommodate the IPv6 unicast address-specific extended community, set the IPv6 community configuration under the [edit policy-options] hierarchy and set the following configuration statements in the [edit policy-options community *community-name* members] hierarchy:

- `ipv6-target:<IPv6 unicast address>:operator-defined local values`
- `ipv6-origin:<IPv6 unicast address>:operator-defined local values`
- `ipv6-extended:type-and-subtype value:<IPv6 unicast address>:operator-defined local values`

[See [show route detail](#), [show route advertising-protocol](#), [Understanding BGP Communities, Extended Communities, and Large Communities as Routing Policy Match Conditions](#), [Understanding How to Define BGP Communities and Extended Communities](#), [ipv6-extended](#), [ipv6-origin](#), and [ipv6-target](#).]

Routing Protocols

- **Support for BGP-LS NLRI to carry confederation ID (ACX710, ACX5448, MX10003, QFX5120-48YM, QFX5200, and QFX5210, and vRR)**—Starting in Junos OS Release 23.1R1, Junos OS enables BGP Link State (BGP-LS) network layer reachability information (NLRI) to carry the confederation ID in TLV 512 when BGP confederation is enabled. The NLRI carries the confederation ID along with the member autonomous system number (AS number) in TLV 517 as defined in RFC 9086. In releases before Junos OS Release 23.1R1, BGP-LS NLRI carries only the member AS number in TLV 512 and the confederation ID is not encoded in the Isdist.0 routing table.

[See [Link-State Distribution Using BGP Overview](#).]

Virtual Chassis

- Starting in Junos OS Release 23.1R1, QFX5120-48YM Switches support Virtual Chassis using HiGig over Ethernet (HGoE). With the help of this functionality, HiGig protocol packets are first sent out over the Virtual Chassis interface and then enclosed in a regular ethernet frame.

[See [Understanding QFX Series Virtual Chassis](#).]

VPNs

- **Support for native IPv6 in carrier-of-carrier VPNs (ACX Series, MX Series, and QFX Series)**—Starting in Junos OS Release 23.1R1, you can configure LDP and IGPs using IPv6 addressing to support

carrier-of-carriers VPNs. Junos OS supports native IPv6 prefix exchanges in the carrier-of-carriers deployments.

[See [Carrier-of-Carriers VPNs](#), [LDP Native IPv6 Support Overview](#), and [LDP Configuration](#).]

Additional Features

Support for the following features has been extended to these platforms.

- **On-box monitoring support on the control plane (EX Series, QFX Series, and SRX Series)**—The memory monitoring system monitors the system memory and raises a major or minor alarm using the `set system monitor memory system alarm` command statement on the devices. The alarm is raised when the device is running low on memory.

[See [Memory \(System\)](#).]

What's Changed

IN THIS SECTION

- [General Routing](#) | 121
- [EVPN](#) | 122
- [Network Management and Monitoring](#) | 122
- [Routing Protocols](#) | 123

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

General Routing

- When subscribing to the resource path `/junos/system/linecard/environment`, the prefix for the streamed path at the collector side was displaying as `/junos/linecard/environment`. This issue is resolved in Junos OS 23.1R1 and Junos OS Evolved 23.1R1 and the subscription path and the streamed path match to display `/junos/system/linecard/environment`.

EVPN

- Flow-label configuration status for EVPN ELAN services. The output for the `show evpn instance extensive` command now displays the flow-label and flow-label-static operational status for a device and not for the routing instances. A device with `flow-label` enabled supports flow-aware transport (FAT) flow labels and advertises its support to its neighbors. A device with `flow-label-static` enabled supports FAT flow labels but does not advertise its capabilities.
- **Specify the UDP source port in a ping overlay or traceroute overlay operation** — In Junos OS releases prior to 22.4R1, you could not configure the `udp` source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other `hash-*` options that may be used to determine the source port value.

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the `get-system-yang-packages` RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `get-system-yang-packages` RPC reply replaces the `xmlproxy-yang-modules` tag with the `proxy-xml-yang-modules` tag in the XML output.
- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is `error` instead of `warning`, and the `<rpc-`

`error` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

Routing Protocols

- **Avoid multicast traffic loss on OISM server leaf and border leaf devices in scaled EVPN-VXLAN fabrics (QFX5130-32CD and QFX5700 switches)**—You can configure QFX5130-32CD and QFX5700 switches as optimized intersubnet multicast (OISM) server leaf or border leaf devices in an EVPN-VXLAN fabric. In scaled fabrics with many VLANs, EVPN instances, and multicast streams, you might see multicast traffic loss on these devices due to the limited size of the multicast snooping route tables in the PFE. To avoid this problem on QFX5130-32CD and QFX5700 switches with OISM in scaled environments, we require that you configure the `conserve-mcast-routes-in-pfe` option at the `edit multicast-snooping-options oism` hierarchy on these platforms. This option is available only on QFX5130-32CD and QFX5700 switches. Use this option when you configure these devices as server leaf or border leaf devices with OISM. Do not configure this option when you configure these devices as standalone assisted replication (AR) replicators with OISM.

[See [oism \(Multicast Snooping Options\)](#).]

Known Limitations

IN THIS SECTION

- [General Routing](#) | 124

Learn about known limitations in this release for QFX 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 QFX10008, statistics for multicast packets is not as expected as the packets has Layer 2 header stripped during replication in Packet Forwarding Engine because of which it is not forwarded to the next hop. [PR1678723](#)
- There is increase in memory footprint across different demons after an image upgrade resulting increase in the system memory. [PR1694522](#)

Open Issues

IN THIS SECTION

- [General Routing](#) | 124

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. [PR1462548](#)
- When launching a guest Virtual Machine (VM) to run a third party application on Junos OS 15.1R1 and above, the guest VM might be shown as "UNAVAILABLE" even after successfully installing the third party application. This is due to duplicated device ID assigned to different disks. [PR1529596](#)
- Pim Vxlan not working on TD3 chipsets enabling VxLAN flexflow after release 21.3R1. Customers Pim Vxlan or data plane VxLAN can use the version 21.3R1. [PR1597276](#)
- Configuring em0/em1 interface on a Virtual chassis will cause instability in a Virtual Chassis, causing the VC members to split. VME interface should be used instead of em0/em1 [PR1636050](#)

- On QFX platform, v6 ifl stats are being derived from the underlying ifd stats unlike on PTX where they are hardware assisted. Hence, they are not very reliable and are at best, guesstimate. [PR1653671](#)
- On all QFX platforms, Ethernet VPN (EVPN) Type-5 traffic drops are observed when the device is configured only with Type-5 Virtual Routing and Forwarding (VRF) and without an Integrated Routing and Bridging (IRB) interface. [PR1663804](#)
- When the remote end server/system reboots, QFX5100 platform ports with SFP-T 1G inserted may go into a hung state and remain in that state even after the reboot is complete. This may affect traffic after the remote end system comes online and resumes traffic transmission. [PR1665800](#)
- On QFX5100 platforms (both stand-alone and VC scenario) running Junos, occasionally during the normal operation of the device, PFE (Packet Forwarding Engine) can crash resulting in total loss of traffic. The PFE reboots itself following the crash. [PR1679919](#)
- Applying ERSPAN configuration along with the ERSPAN output/egress INET interface configuration sometimes leads to the analyzer not getting created in the HW. [PR1682610](#)
- On Junos OS QFX5000 Series platforms, configuration changes in Ethernet Virtual Private Network (EVPN) Virtual Extensible LAN (VXLAN) with Type 5 tunnel cause port and protocol flaps which cause traffic loss (Configuration change related to the underlay network). [PR1688323](#)
- On QFX5110 with Virtual Chassis configured, if any of the egress queues 3 or 4 is congested it causes buffer stuck error messages and traffic drop on the VCP (Virtual Chassis port) ports. [PR1696119](#)
- root show chassis hardware Hardware inventory: Item Version Part number Serial number
Description Chassis XXXXXXXXXXXX Virtual Chassis Pseudo CB 0 Routing Engine 0 BUILTIN
BUILTIN QFX Routing Engine FPC 0 REV 16 650-064380 XXXXXXXXXXXX QFX5100-48S-6Q CPU
BUILTIN BUILTIN FPC CPU PIC 0 BUILTIN BUILTIN 48x10G-6x40G Xcvr 0 REV 01 740-031980
XXXXXXXXXXXX SFP+-10G-SR Power Supply 0 REV 04 740-041741 1GA27194620 JPSU-650W-
AC-AFO Power Supply 1 REV 04 740-041741 1GA27194616 JPSU-650W-AC-AFO Fan Tray 0
QFX5100 Fan Tray 0, Front to Back Airflow - AFO Fan Tray 1 QFX5100 Fan Tray 1, Front to Back
Airflow - AFO Fan Tray 2 QFX5100 Fan Tray 2, Front to Back Airflow - AFO Fan Tray 3 QFX5100 Fan
Tray 3, Front to Back Airflow - AFO Fan Tray 4 QFX5100 Fan Tray 4, Front to Back Airflow - AFO
Power Supply 0 REV 04 740-041741 1GA27194620 JPSU-650W-AC-AFO <<<<<<<<<< Dup!!
Power Supply 1 REV 04 740-041741 1GA27194616 JPSU-650W-AC-AFO <<<<<<<<<< Dup!! Fan
Tray 0 QFX5100 Fan Tray 0, Front to Back Airflow - AFO <<<<<<<<<< Dup!! Fan Tray 1 QFX5100
Fan Tray 1, Front to Back Airflow - AFO <<<<<<<<<< Dup!! Fan Tray 2 QFX5100 Fan Tray 2, Front
to Back Airflow - AFO <<<<<<<<<< Dup!! Fan Tray 3 QFX5100 Fan Tray 3, Front to Back Airflow -
AFO <<<<<<<<<< Dup!! Fan Tray 4 QFX5100 Fan Tray 4, Front to Back Airflow - AFO
<<<<<<<<<< Dup!! {master:0} root>. [PR1704106](#)

- 1. VC members can split when em0 cable is removed and reinserted. 2. VC will automatically converge after the split(after point 1). [PR1709938](#)
- In QFX5000 devices, LACP flaps will be seen, when LACP BPDUs are received, VLAN tag is not processed causing system-id mismatch. [PR1711783](#)
- Whenever a new VLAN is added in between previously configured VLANs, existing context ID which is already assigned to existing VLAN context, will be assigned for that new VLAN. Due to this we might see incorrect system ID or bridge ID and this might create an issue.[PR1717267](#)

Resolved Issues

IN THIS SECTION

- [Class of Service \(CoS\) | 126](#)
- [EVPN | 127](#)
- [General Routing | 127](#)
- [Interfaces and Chassis | 130](#)
- [MPLS | 130](#)
- [Platform and Infrastructure | 130](#)
- [Routing Protocols | 131](#)

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 congestion details will be lost as ECN bits in DSCP are cleared after VXLAN decapsulation. [PR1683438](#)

EVPN

- The kernel crash would be observed in an EVPN multi-homed scenario. [PR1649234](#)
- In EVPN-MPLS multihoming scenario DF election will get stuck in the preference based state. [PR1662954](#)
- Traffic drop might be observed due to the VTEP tunnels not being established in the EVPN-VxLAN scenario. [PR1700196](#)
- In EVPN scenario, proxy-arp on IRB interfaces do not work as expected. [PR1709007](#)
- The generation of the VXLAN table appears to be lost after loading configuration. [PR1712805](#)

General Routing

- The port LEDs do not light up when 40G/100G physical interfaces are up. [PR1660532](#)
- The dc-pfe process crash is observed with PTP transparent clock on QFX platforms. [PR1661602](#)
- The DHCP offer packets will not be sent to the clients when the DHCP relay agent is configured over type-5 EVPN. [PR1664656](#)
- Shaping-rate is not taking 20bytes of overhead into account. [PR1667879](#)
- EVPN multicast traffic might get impacted because of routes getting stuck in the kernel routing table (krt) queue. [PR1670435](#)
- VC members are reloading randomly. [PR1671293](#)
- QFX5120-48YM :: QFX-EVPN_VXLAN: ECN bits not getting copied to VXLAN tunnel header at the encap node. [PR1672308](#)
- QFX5100 switches can report Packet Forwarding Engine syslog message **ACL Unresolve DOT1Q failed in setting udf settings on unit**. [PR1676220](#)
- Interfaces with QFX-10000-30C and QFX10000-30C-M line cards will not work properly. [PR1677325](#)
- BFD sessions will remain down in the EVPN-VxLAN scenario. [PR1680757](#)
- LLDP neighborship fails to come up with a private VLAN configuration. [PR1681614](#)
- System uptime display is shown in minutes instead of seconds. [PR1681656](#)

- The dcpfe crash seen with PTP configuration on Junos OS platforms supporting boundary clock. [PR1683308](#)
- Traffic loss is seen when MAC flaps between the MC-AE interface and the ICL interface. [PR1683771](#)
- Licenses on the device might become invalid when the device is upgraded from a legacy licensing-based release to an Agile licensing-based release. [PR1684842](#)
- The protocol MTU for the IRB interface is not rolled back when the MTU of the IRB or IFD interfaces is modified or deleted. [PR1685406](#)
- JUNOS:JDI_REGRESSION:PROTOCOLS:SWITCHING:EVPN: Traffic statistics verification fails as receiving packet count exceeds specified limit in EVPN VXLAN multicast scenario. [PR1685467](#)
- Traffic through the ICL link to MC-AE peer box gets looped back to the VTEP tunnel on QFX5000 platforms. [PR1687024](#)
- QFX5120 will drop ingress traffic on an l2circuit configured interface on continuous flapping. [PR1687257](#)
- VXLAN configured on access port breaks L2 connectivity with vxlan encapsulate-inner-vlan configuration statement. [PR1687565](#)
- OVSDB certificate files are not copied from the primary to the backup. [PR1687847](#)
- ARP resolution to the CE port having EP style aggregate Ethernet with multiple VLANs would get fail in the EVPN-VXLAN scenario. [PR1687861](#)
- The LLDP output packets are not transmitting on the em0 interface of Junos OS and Junos OS Evolved platforms. [PR1688023](#)
- The FPC crash would be observed when the same CoS configuration is applied with wildcard for all the physical interfaces and aggregate Ethernet. [PR1688455](#)
- On QFX10008 and QFX10016 platforms fails to detect flaps even though the remote device connected has observed flaps. [PR1688993](#)
- [Blocker:Test] QFX10008: While verifying show ethernet-switching global-mac-count | display xml command **global-mac-count** is not as expected. [PR1689127](#)
- The switch might not respond to router solicitation message in the EVPN-VXLAN scenario. [PR1689925](#)
- Packet loss seen on the EVPN-VXLAN spine router. [PR1691029](#)
- Traffic loss is observed when the ECMP path is IRB over AE (IPv4->MPLS). [PR1693424](#)

- Packet Forwarding Engine crash is seen on all Junos OS QFX5000 and EX4600 platforms with L2PT configuration. [PR1694076](#)
- dot1xd.core-tarball.0.tgz is observed in 22.1R3 at #0x009113f0 in __mem_assert(). [PR1694129](#)
- All members of the VCF will not reboot on QFX5000 platforms. [PR1694996](#)
- The l2cpd telemetry crash would be observed when the LLDP Netconf notification from external controllers along with Netconf services configuration is present on the device. [PR1695057](#)
- Intra VLAN communication breaks in SP style configuration using VXLAN. [PR1695058](#)
- BMP EOR is sent with wrong peer address causing BMP failure. [PR1695320](#)
- On QFX5110-VC-VCF platforms, traffic impact is seen when the firewall filter with DSCP action is enabled. [PR1695820](#)
- JUNOS_REG::QFX5110-32Q:VC::After upgrading to Junos OS Release 20.4R3-S5.3, the dcpfe core file generates and the device becomes unstable. [PR1695943](#)
- The BFD session might be stuck in init state on certain QFX5000 platforms. [PR1696113](#)
- Adding more than 256 VLANs as name tags on the same interface results in dcd crash. [PR1696428](#)
- VSTP will not work in the EVPN-VxLAN network. [PR1696979](#)
- Assigning VNI to VLAN will cause a small number of packets lost on other VLANs on the same interface. [PR1697244](#)
- Local multicast traffic forwarding issue can be seen on QFX5000 in EVPN-VXLAN OISM setup. [PR1697614](#)
- Traffic drop is observed after deleting or deactivating the logical interface. [PR1697827](#)
- PE device changes an outer tag-id in a local return environment. [PR1697835](#)
- On QFX5000 switch, VGA is not working when SP style configuration is mixed with EP style configuration. [PR1698491](#)
- Adaptive sampling will not work if the system clock is turned backward. [PR1699585](#)
- Dot1x memory is spiking up even after clearing the dot1x sessions. [PR1702388](#)
- DCPFE crashes which leads to FPC restart. [PR1706515](#)
- The FPC crash can be seen on QFX5000 platforms during simultaneous soft and hard OIR of SFP. [PR1707094](#)

- The spine does not reply to RS messages coming via the VXLAN tunnel in the CRB scenario. [PR1707679](#)
- Ports with QSA adapter are down. [PR1709817](#)
- FPC is down on QFX5000 after committing an IPv6 filter. [PR1710704](#)
- The message **fpc0 list_get_head, list has bad magic (0x0)** might be output after the commit operation is complete. [PR1710776](#)
- The qfx-5e (TVP) Junos image installation issue on certain Junos OS release on QFX5100. [PR1710855](#)
- Traffic drop is observed in the EVPN-VXLAN scenario with Type-2 ESI tunnel. [PR1711889](#)
- [EVPN-VXAN] L3 VLANs created with IPv4 bits disabled. [PR1712405](#)

Interfaces and Chassis

- Management interface speed is incorrectly reported as 10G instead of 1G. [PR1636668](#)
- The unicast traffic is dropped on QFX5100 platforms. [PR1695663](#)

MPLS

- Traffic loss might be seen in an LDP->BGP-LU stitching scenario. [PR1670334](#)
- RPD(LDP) cores with configurations like BGP static routes or SR-TE routes in INET.0. [PR1697498](#)

Platform and Infrastructure

- Incorrect programming of next-hop based on RVT interface hosted on MPC10E/MPC11E, LC9600, MX304 leads to traffic drops. [PR1682383](#)
- The vmcore crash observed in low memory conditions. [PR1694463](#)

Routing Protocols

- The InboundConvergencePending flag is set after Routing Engine switchover. [PR1680360](#)
- The BGP auto-discovered neighborship is not formed after a reboot. [PR1699233](#)
- The BGP graceful-shutdown community is not advertised on Junos OS and Junos OS Evolved platforms. [PR1699633](#)
- IPv4 routes learnt over a link-local BGP session not advertised ahead to other BGP peers. [PR1712406](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 144

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

Upgrading Software on QFX Series Switches

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

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

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

The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.
3. Select **20.3** in the Release pull-down list to the right of the Software tab on the Download Software page.
4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.3 release.

An Alert box appears.

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

A login screen appears.

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

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-23.1-R1.n-secure-signed.tgz reboot
```

Replace *source* with one of the following values:

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 20.3 jinstall package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-23.1R1.9.tgz
```

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

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-
x86-64-23.1R1.9.tgz
```

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

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

Installing the Software on QFX10002 Switches

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

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

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

For example:

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

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

For example:

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

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

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

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

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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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

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



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

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

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

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

```
user@switch# exit
```

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

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

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

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

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

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-  
x86-64-23.1R1.n-secure-signed.tgz
```

For more information about the `request system software add` command, see the [CLI Explorer](#).

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

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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

For more information about the `request chassis routing-engine master` command, see the [CLI Explorer](#).

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

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

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

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

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-23.1R1.n-secure-signed.tgz
```

For more information about the `request system software add` command, see the [CLI Explorer](#).

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

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

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

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

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

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

16. Log in and issue the `show version` command to verify the version of the software installed.
17. Transfer routing control back to the master Routing Engine:

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

For more information about the `request chassis routing-engine master` command, see the [CLI Explorer](#).

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

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

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

Performing a Unified ISSU

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

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

Perform the following tasks:

- ["Preparing the Switch for Software Installation" on page 141](#)
- ["Upgrading the Software Using Unified ISSU" on page 142](#)

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

To verify that nonstop active routing is enabled:

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

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

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

- Enable nonstop bridging (NSB). See [Configuring Nonstop Bridging on EX Series Switches](#) for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the `request system snapshot` command.

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in [Installing Software Packages on QFX Series Devices](#).
2. Copy the software package or packages to the switch. We recommend that you copy the file to the `/var/tmp` directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
 - On the switch, enter:

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

where *package-name.tgz* is, for example, *jinstall-host-qfx-10-f-x86-64-23.1R1.n-secure-signed.tgz*.

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

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

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
```

```

Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

```

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

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

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

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

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

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


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

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

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

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

For both standard EOL and EEOL releases, you can upgrade to the next three subsequent releases or downgrade to the previous three releases. For example, you can upgrade from 20.4 to the next three releases – 21.1, 21.2 and 21.3 or downgrade to the previous three releases – 20.3, 20.2 and 20.1.

For EEOL releases only, you have an additional option - you can upgrade directly from one EEOL release to the next two subsequent EEOL releases, even if the target release is beyond the next three releases. Likewise, you can downgrade directly from one EEOL release to the previous two EEOL releases, even if the target release is beyond the previous three releases. For example, 20.4 is an EEOL release. Hence, you can upgrade from 20.4 to the next two EEOL releases – 21.2 and 21.4 or downgrade to the previous two EEOL releases – 20.2 and 19.4.

Table 11: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for SRX Series

IN THIS SECTION

- [What's New | 145](#)
- [What's Changed | 153](#)
- [Known Limitations | 160](#)
- [Open Issues | 161](#)
- [Resolved Issues | 162](#)
- [Migration, Upgrade, and Downgrade Instructions | 166](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 146](#)
- [Chassis Cluster-specific | 146](#)
- [Flow-based and Packet-based Processing | 146](#)
- [Intrusion Detection and Prevention | 146](#)
- [J-Web | 147](#)
- [Licensing | 149](#)
- [Network Address Translation \(NAT\) | 149](#)
- [Network Management and Monitoring | 149](#)
- [Securing GTP and SCTP Traffic | 151](#)
- [Software Installation and Upgrade | 151](#)
- [Content Security | 151](#)
- [VPNs | 152](#)

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

Authentication and Access Control

- **Support for multiple certificates and multiple domains (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we support multiple certificates with multiple domains and a single certificate with multiple domains for J-Web sessions. You can enter a new configuration statement `virtual-domain` in the `[edit system services web-management https]` hierarchy level to use this feature. This helps in having multiple sessions without any certificate warning.

[See [https \(Web Management\)](#).]

Chassis Cluster-specific

- **Support for IPv4 and IPv6 unicast IP-over-IP tunneling (SRX Series and vSRX)**—Starting in Junos OS Release 23.1R1, we support IP-over-IP tunneling for IPv4 and IPv6 traffic.

[See [IP-over-IP Tunneling](#).]

Flow-based and Packet-based Processing

- **Debug improvement of policy PFE control thread (SRX300, SRX320, SRX340, SRX345, SRX380, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can configure `services-offload` and `no-services-offload` in a mutually exclusive way. If you configure `services-offload`, then `no-services-offload` is automatically disabled. If you configure `no-services-offload`, then `services-offload` is automatically disabled. You cannot configure and commit both options simultaneously.

[See [show security policies](#).]

Intrusion Detection and Prevention

- **Support for on-box IDP Control Plane Packet Capture (SRX380, SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600, SRX550HM, SRX5400, SRX5600, SRX5800, vSRX 2.0, vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can store the packets captured by intrusion detection and prevention (IDP) locally on the SRX device. You can view the details on the UI or J-Web. The captured traffic is stored on the device at `/var/log/pcap/idp/`. You can limit the number of local packet capture files that are created using a configuration and the log rotation facility.

To support this new feature, we've:

- Added new counters to the existing packet-log counters.
- Provided a command to clear all the captured files.

[See <https://www.juniper.net/documentation/us/en/software/junos/idp-policy/topics/topic-map/security-idp-packet-capture.html>]

J-Web

- **Enhanced search and filter options for the Logs pages (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550HM, and vSRX3.0)**—Starting in Junos OS Release 23.1R1, J-Web supports additional operators in **Monitor > Logs** (Sessions, Threats, Web-filtering, ATP, VPN, and All Events) pages for better search and filter functionality. J-Web also supports Netmask when searching for IP addresses.

[See [Monitor Session](#), [Monitor Threats](#), [Monitor Web Filtering](#), [Monitor ATP](#), [Monitor VPN](#), and [Monitor All Events](#).]

- **Support for packet capture (SRX300, SRX320, RX1500, SRX4100, SRX4600, SRX5600, and vSRX3.0)**—Starting in Junos OS Release 23.1R1, you can:
 - Store the packet capture files locally on the SRX device. To do this task, enable Packet Capture from **Security Services > IPS > Packet Capture** and then enable **Local Storage** to configure the local storage parameters.
 - Download the packet capture files that record IDP attacks. Choose **Monitor > Logs > Threats** to see the packet capture data.
 - Download packet capture file that record session-close logs. Choose **Monitor > Logs > All Events** to view the packet capture data.

[See [About the Sensor Page](#), [Monitor Threats](#), and [Monitor All Events](#).]

- **Enhanced Certificate Management page (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.1R1, we've revamped the Certificate Management page. From this page, you can now:
 - Create device certificates by using the options:
 - Let's Encrypt
 - Local self-signed
 - SCEP
 - ACME
 - Certificate Management Protocol version 2 (CMPv2)
 - Certificate signing request (CSR)
 - Add a certificate authority (CA Certificate and Juniper Bundle).
 - Enroll the device certificates with the Let's Encrypt server and the ACME protocol.
 - Re-enroll a device certificate.

- Renew a Local Self-Signed device certificate.

[See [About the Certificates page](#).]

- **Support for virtual domain certificates (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.1R1, you can create virtual domain certificates from **Basic Settings > System Services** for secured J-Web access.

[See [Configure Basic Settings](#).]

- **Support for device certificates in the IPsec VPN page (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.1R1, you can select the device certificate (including Let's Encrypt or ACME) from the list of local certificates when you configure the IPsec VPN local gateway.

[See [Create a Remote Access VPN—Juniper Secure Connect](#).]

- **Support for authentication method (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550HM, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS 23.1R1 Release, you can:

- Configure the following authentication methods in Juniper Secure Connect:

- EAP-MSCHAPv2 (Username & Password)
- EAP-TLS (Certificate)
- Pre-shared Key (Username & Password)

- Configure the following authentication method in NCP Exclusive Client:

- EAP Based
- Pre-shared Key (Username & Password)

[See [Create a Remote Access VPN—Juniper Secure Connect](#).]

- **Support for connection profile and IKE ID (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, SRX550HM, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS 23.1R1 Release:

- We've renamed the Remote Access column to connection profile in the landing pages of **Network > VPN > IPsec VPN** and **Monitor > Network > IPsec VPN**.
- You can configure the connection profile in the fully qualified domain name (FQDN) or FQDN/Realm format. Using this connection profile, the SRX device automatically gets the IKE ID. If you change the input for the connection profile, the SRX device automatically gets the updated IKE ID.

[See [Create a Remote Access VPN—NCP Exclusive Client](#).]

- **Enhancement for the Tenant and LSYS menu (SRX1500, SRX4100, SRX4200, SRX4600, and SRX5000 line of devices)**—Starting in Junos OS 23.1R1 Release, after you enter as a tenant or a logical systems user, you can view the name and the number of available tenants or logical system. The **Tenant and LSYS** menu is available to the right of the feedback icon on the J-Web landing page.

[See [Explore J-Web](#).]

- **Support for data plane packet capture (SRX4600, and SRX5000 line of devices)**—Starting in Junos OS 23.1R1 Release, we've added the new **Data Plane Packet Capture** sub-menu under the **Device Administration** menu. You can use this page to capture and analyze data plane traffic on a router.

[See [About the Data Plane Packet Capture Page](#).]

Licensing

- **Support to trigger license alarm at configured time interval (EX Series, MX Series, QFX Series, and SRX Series)**—Starting in Junos OS Release 23.1R1, you can set the time interval at which you want to trigger alarms for features or capacity that do not have licenses installed.

To set the alarm log frequency, use the command `log-frequency` in the `set system license` hierarchy.

[See [Managing Licenses](#).]

Network Address Translation (NAT)

- **Support to retain existing NAT session with destination NAT (SRX Series)**—Starting in Junos OS release 23.1R1, with FQDN based Destination NAT, we support to retain existing NAT sessions even when the DNS resolved IP address changes for the Destination NAT Pool. To retain the existing NAT sessions, you can enable `session-retain` at `[security nat destination pool pool-name]` hierarchy. When `session-retain` is enabled, FQDN based destination NAT sessions remain in the session table, and cleared only upon connection termination from clients, or timeout due to sessions being inactive, or when sessions are explicitly cleared by the user through CLI.

Common DNS cache for NAT and Policy: The NAT and configured policy FQDNs use a single cache. The use of the single cache helps avoid packet drops if you've configured the same FQDN in the policy and NAT.

[See [pool \(Security Destination NAT\)](#).]

Network Management and Monitoring

- **On-box logging modernization (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can use the following operational commands to optimize the database query performance:
 - `show security log report in-detail`

- `show security log report in-interval`
- `show security log report summary`

[See [Understanding On-Box Logging and Reporting](#), [show security log report in-detail](#), [show security log report in-interval](#), and [show security log report summary](#).]

- **Improved filtering and search using new expression option for on-box reporting (SRX4600)**—Starting in Junos OS Release 23.1R1, we've enhanced the filtering options and search mechanism to generate optimized log reports. Use the expression option in the `show security log report in-detail all` and `show security log report summary all` commands with the following operators to generate optimized reports:
 - not equal to
 - greater than or equal to
 - less than or equal to
 - IP Addresses with netmask awareness

The total length of the expression is limited to 256 bytes including the brackets.

[See [Understanding On-Box Logging and Reporting](#), [show security log report in-detail](#), and [show security log report summary](#).]

- **Support for DNS logging in on-box reporting (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've added support for DNS logging in on-box reporting. You can now use on-box reporting with:
 - New logging database for DNS.
 - `in-detail` and `summary` CLI query options for DNS.
 - DNS as part of the threat category.

[See [Understanding On-Box Logging and Reporting](#), [show security log report in-detail](#), and [show security log report summary](#).]

- **Increased database file size capacity for on-box reporting (SRX4600)**—Starting in Junos OS Release 23.1R1, we've increased the on-box logging database file size capacity to 216 million entries. With this enhancement, you can customize the database sizing for each database table.

[See [report \(Security Log\)](#).]

- **Dedicated CPU resource for on-box reporting (SRX4600)**—Starting in Junos OS Release 23.1R1, you can assign a dedicated CPU resource for the on-box logging. The use of the dedicated resource

improves the query performance. To assign the dedicated resource, configure the new enhanced-logging statement at the [edit security forwarding-options resource-manager] hierarchy level.

[See [show security forward-options resource-manager](#) and [resource-manager](#).]

Securing GTP and SCTP Traffic

- **GTP: Filtering/masking ULI IE message parameters**—In Junos OS Release 23.1R1, we've introduced the `mask-uli` configuration statement. You can use this statement to configure a GPRS tunneling protocol (GTP) profile that masks the User Location Information (ULI) element in GTPv1 and GTPv2. You can also control the mask value for the ULI, which can range from 1 through 65,535 (in hexadecimal, 00 01 to FF FF). The GTP profile is attached to a policy to meet the necessary conditions for masking the ULI, as determined by the operator.

[See [mask-uli](#).]

RELATED DOCUMENTATION

https://www.juniper.net/documentation/us/en/software/junos/gtp-sctp/topics/ref/statement/mask_uli.html

<https://www.juniper.net/documentation/us/en/software/junos/agf-user-guide/agf/topics/concept/agf-sctp-amf.html>

Software Installation and Upgrade

- **ZTP enhancements to support both DHCP options and PHC (SRX4600)**—Starting with Junos OS Release 23.1R1, you can use either the legacy DHCP-options-based zero-touch provisioning (ZTP) or the phone-home client (PHC) to provision software for your device. If the device boots and receives DHCP options from the DHCP server for ZTP, ZTP resumes. If DHCP options are not present, PHC is attempted. PHC enables the device to securely obtain bootstrapping data, such as a configuration or software image, with no user intervention other than having to physically connect the device to the network. When the device first boots, PHC connects to the preconfigured Juniper redirect server (redirect.juniper.net), which will redirect to a phone-home server (PHS) to get the configuration or software image.

To initiate either DHCP-options-based ZTP or PHC, the device must either be in a factory-default state, or you can issue the `request system zeroize` command.

[See [Understanding the Phone-Home Client](#).]

Content Security

- **Sophos Live Protection version 2.0 support for content security (SRX Series and vSRX)**—Starting in Junos OS Release 23.1R1, content security supports antivirus Sophos Live Protection version 2.0. The new version of Sophos antivirus uses an HTTPS connection for the device-to-server

communication. For the HTTPS connection, you must create an SSL initiation profile and add the profile to the default configuration of the Sophos engine.

We've introduced the `host`, `port`, and `ssl-profile` statements at the `[edit security utm default-configuration anti-virus sophos-engine server]` hierarchy level. In addition, we've deprecated the `sxl-retry` and `sxl-timeout` statements at the `[edit security utm default-configuration anti-virus sophos-engine]` and `[security utm feature-profile anti-virus sophos-engine]` hierarchy levels.

[See [server \(Security Sophos Engine Antivirus\)](#), [Sophos Antivirus Protection Overview](#), and [show security utm anti-virus status](#)].

VPNs

- **Introduction of prelogon compliance checks (SRX Series and vSRX 3.0)**—In Junos OS Release 23.1R1, we introduce prelogon compliance for Juniper Secure Connect. This functionality validates the current status of a connecting client device prior to the authentication (that is, before user's login). You can configure different match criteria on the SRX Series firewall to allow or reject client devices.

You can configure this feature using the statement `compliance pre-logon name` at:

- `[edit security remote-access]` hierarchy level to configure prelogon compliance rules.
- `[edit security remote-access profile realm-name]` hierarchy level to associate a prelogon compliance rule to the remote-access profile.

[See [prelogon compliance checks](#).]

- **Support for application bypass in Juniper Secure Connect (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can use Juniper Secure Connect to send specific application traffic directly to its destination instead of passing it through the VPN tunnel. You can accomplish this functionality by specifying domain names and protocols for the specified applications that would bypass the VPN tunnel. The bypass feature simplifies the administrator and end-user experience.

When you configure the application bypass feature and establish a remote-access VPN tunnel, the configuration automatically enables a stateful firewall rule rejecting incoming connections on other adapters, which prevents the device from becoming a bastion host.

You can configure this feature on SRX Series firewalls and on vSRX 3.0 virtual firewalls by using `application-bypass` at the `[edit security remote-access client-config name]` hierarchy level.

[See [Application Bypass](#).]

- **Support for multiple certificates and multiple domains (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, with support for multiple certificates and multiple domains, we now allow Juniper Secure Connect connection profiles with different URLs without any certificate warning.

[See [Multiple certificates and domains support](#).]

What's Changed

IN THIS SECTION

- [EVPN | 153](#)
- [Flow-Based and Packet-Based Processing | 153](#)
- [General Routing | 154](#)
- [J-Web | 154](#)
- [Network Management and Monitoring | 154](#)
- [PKI | 155](#)
- [VPNs | 157](#)

Learn about what changed in this release for SRX Series.

EVPN

- Flow-label configuration status for EVPN ELAN services The output for the `show evpn instance extensive` command now displays the flow-label and flow-label-static operational status for a device and not for the routing instances. A device with `flow-label` enabled supports flow-aware transport (FAT) flow labels and advertises its support to its neighbors. A device with `flow-label-static` enabled supports FAT flow labels but does not advertise its capabilities.
- Specify the UDP source port in a ping overlay or traceroute overlay operation — In Junos OS releases prior to 22.4R1, you could not configure the `udp` source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other `hash-*` options that may be used to determine the source port value.

Flow-Based and Packet-Based Processing

- PMI Mode Passthrough ESP traffic: Starting in Junos OS Release 22.1R3, we support the PMI express path processing for passthrough ESP traffic on the SRX4100, SRX4200, and vSRX.

- **Flow session operational command support for content security (SRX Series and vSRX)**—We've extended the `show security flow session` operational command support to view the details of the content filtering and Web filtering content security features.

[See [show security flow session](#).]

General Routing

- When subscribing to the resource path `/junos/system/linecard/environment`, the prefix for the streamed path at the collector side was displaying as `/junos/linecard/environment`. This issue is resolved in Junos OS 23.1R1 and Junos OS Evolved 23.1R1 and the subscription path and the streamed path match to display `/junos/system/linecard/environment`.
- **Time zone support for local certificate verification (SRX1500 and SRX5600)**—Starting in this release, when the local certificate verification fails, you can see the time zone for the failed local certificate in the command output and system log messages.

J-Web

- **Packet Capture is now called Control Plane Packet Capture (SRX Series)**— Starting in Junos OS 23.1R1 Release, we've renamed **Packet Capture** to **Control Plane Packet Capture** under **Device Administration** menu. You can use this page to capture and analyze control plane traffic on a router.

[See [Control Plane Packet Capture](#).]

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas

emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the get-system-yang-packages RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The get-system-yang-packages RPC reply replaces the xmlproxy-yang-modules tag with the proxy-xml-yang-modules tag in the XML output.
- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

PKI

- **Deprecating options related to certificate enrollment (Junos)**—Starting in Junos OS Release 23.2R1, we're deprecating earlier CLI options related to Public Key Infrastructure (PKI) to enroll and reenroll local certificate through Simple Certificate Enrolment Protocol (SCEP). The table below shows the Junos CLI commands and configuration statements with the options being deprecated. You can find the same CLI options now available under scep option in these commands and statements.

Table 12: Deprecated Junos CLI Options

Junos CLI Commands and Statements	Deprecated Options
set security pki auto-re-enrollment	certificate-id

Table 12: Deprecated Junos CLI Options *(Continued)*

Junos CLI Commands and Statements	Deprecated Options
request security pki local-certificate enroll	ca-profile certificate-id challenge-password digest domain-name email ip-address ipv6-address logical-system scep-digest-algorithm scep-encryption-algorithm subject

Table 12: Deprecated Junos CLI Options (*Continued*)

Junos CLI Commands and Statements	Deprecated Options
request security pki node-local local-certificate enroll	ca-profile certificate-id challenge-password digest domain-name email ip-address ipv6-address logical-system scep-digest-algorithm scep-encryption-algorithm subject

[See [auto-re-enrollment \(Security\)](#), [request security pki local-certificate enroll scep](#), and [request security pki node-local local-certificate enroll](#).]

VPNs

- **Change format of remote-access profile names (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've changed the format of remote-access profile names to enhance end-user experience using Juniper Secure Connect. In releases before Junos OS Release 23.1R1, you configure the remote-access profile name using the realm name at the [edit security remote-access profile *realm-name*] hierarchy level. But with organizations connecting to several gateways, using the remote-access profile names, such as **hr**, multiple times in the remote-access connection profile becomes unmanageable.

To address this issue, we introduce a new convention for configuring remote-access profile names. You can now configure profile names with URLs using any of the following formats at the [edit

security remote-access profile *realm-name*] hierarchy level, so that end users can connect to the relevant gateway:

- *FQDN/RealmName*
- *FQDN*
- *IP address/RealmName*
- *IP address*

For example, you can now use **ra.example.com/hr**, **ra1.example.com/hr** and **ra.example.com** as realm names.

With the introduction of this convention, we need to deprecate the existing default-profile option at the [edit security remote-access] hierarchy level. Your remote-access profiles names will refer to URLs either with an FQDN or with an IP address, depending on how the end users would connect—for example, **ra.example.com/hr**, **ra.example.com**, **192.168.1.10/hr** or **192.168.1.10**. With this change, the end user will now see the connection profile name in the Juniper Secure Connect application as **ra.example.com/hr** instead of **hr**, as was the case in earlier releases.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name **hr** in the current configuration to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the follow commands -

- ```
user@host# rename security remote-access profile hr to profile ra.example.net/hr
```
- ```
user@host# rename security remote-access profile hr to profile 192.168.1.10/hr
```

[See [profile \(Juniper Secure Connect\)](#).]

- **Enhancements to automatic reenrollment of a local end-entity (EE) certificate (SRX300, SRX320, SRX550HM, SRX1500, SRX4100, SRX4600, SRX5400, SRX5600, SRX5800)**—Starting in Junos OS Release 23.2R1, the option `re-enroll-trigger-time-percentage` is made optional. But you must configure either `re-enroll-time` or `re-enroll-trigger-time-percentage` for the `commit-check` to be successful.

[See [auto-re-enrollment \(Security\)](#).]

- **Removal of power mode IPsec Intel QAT option in IPsec VPN (SRX Series)**—We have removed the option `power-mode-ipsec-qat` at [edit security flow] hierarchy level from Junos CLI for display. This option is now hidden as it is not recommended to be configured with multiple IPsec VPN tunnels. We continue to use AES-NI in PMI mode for better performance than QAT.

[See [Improving IPsec Performance with PowerMode IPsec](#).]

- **Unavailability of default-profile option for remote-access VPN solution (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've hidden the default-profile option at the [edit security remote-access] hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the default-profile option.

We've deprecated the default-profile option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However, modifying the current configuration does not affect existing deployments.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name in the current configuration **hr** to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the following commands -

- ```
user@host# rename security remote-access profile hr to profile ra.example.net/hr
```
- ```
user@host# rename security remote-access profile hr to profile 192.168.1.10/hr
```

For new configurations, consider the following scenarios to create a new remote-access profile based on how your end users connect using the Juniper Secure Connect application:

- If your end users connect using an IP address, specify the IP address in the profile name.
- If your end users connect using an FQDN, specify the FQDN in the profile name.
- If you need to separate users with different realm values such as **hr**, append **/hr** to the IP address or FQDN as follows:
 - [edit security remote-access profile *ra.example.net/hr*]
 - [edit security remote-access profile *192.168.1.10/hr*]

[See [default-profile \(Juniper Secure Connect\)](#) .

- **Remote-access VPN solution doesn't support hexadecimal pre-shared (SRX Series and vSRX 3.0)**—With remote-access VPN solution, for pre-shared-key based authentication method, we support ascii-text format. This means, do not use hexadecimal format for the pre-shared keys in your configuration for remote-access VPN solution. Therefore, configure the statement ascii-text with ascii text format at [edit security ike policy *policy-name* pre-shared-key] hierarchy level for use with Juniper Secure Connect.

- **Enhancement to SCEP PKI Certificate Enrollment**—Logical-system option is added to SCEP PKI certificate enrollment.

[See [request security pki local-certificate enroll scep](#).]

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

Known Limitations

Learn about known limitations in this release for 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.

Network Address Translation (NAT)

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

User Interface and Configuration

- The configured with persist-group-inheritance, which is enabled by default from Junos OS release 19.4R3 onwards might lead to mustd process stop in highly scaled configuration. [PR1638847](#)

Open Issues

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

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

Flow-Based and Packet-Based Processing

- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. [PR1546430](#)

General Routing

- FIPS mode is not supported in this release for SRX Series devices. [PR1697999](#)
- On all SRX Series devices, when firewall web-authentication and Juniper secure connect are configured on the same interface, the firewall web-authentication feature will not work. This might give "page not found" error to the user. [PR1714845](#)

Interfaces and Chassis

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

Resolved Issues

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

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

Application Layer Gateways (ALGs)

- Junos OS: SRX 5000 Series: Upon processing of a specific SIP packet an FPC can crash (CVE-2023-22408). [PR1658604](#)
- SIP 200 OK (INVITE) response packets are dropped leading to SIP call failure. [PR1677554](#)
- SIP calls are getting dropped due to NAT failure and SIP ALG is enabled. [PR1686613](#)
- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed. [PR1688986](#)

Chassis Clustering

- New secondary node to go into a disabled state after ISSU and failover RG0 because of fabric link failure. [PR1678772](#)
- Policy configured with condition route-active-on import is not working properly after RG0 failover. [PR1686648](#)
- Chassis cluster IP monitoring on the secondary node failed after the system reboot on the SRX Series devices. [PR1691071](#)
- The secure tunnel interface does not work properly in SRX Series devices standalone mode. [PR1702763](#)
- GTPv2 message filtering is not working. [PR1704472](#)

Flow-Based and Packet-Based Processing

- To track Routing Engine and Packet Forwarding Engine sync issue with NAT configuration and closed scan session counter issue. [PR1661796](#)
- The non-fragmented packets might get dropped on the SRX5000 line of devices with SPC3 card. [PR1683835](#)
- The flow sessions traversing the IOC2 card would time out early when Express Path is enabled. [PR1688658](#)

- SOF was incorrectly offloading short-lived flows leading to early exhaustion of NP memory, reducing overall device performance. [PR1692100](#)
- Application traffic drop seen on all SRX Series devices due to TCP window size issue. [PR1699578](#)
- Core files gets generated when user is changing interface configuration. [PR1704623](#)
- A flowd process stops on SRX4100, SRX4200, SRX4600, vSRX, and SRX5000 line of devices with SPC3 card when a route is changed frequently. [PR1705996](#)
- The IPv6 source-level fragmented SCTP packets passing through an IPsec tunnel will be dropped. [PR1708876](#)

General Routing

- Unexpected behavior when web-proxy is configured with ssl-proxy. [PR1580526](#)
- HA active/passive mode on-box logging in logical systems and tenant systems, Intermittently Security log contents of binary log file in logical systems are not as expected. [PR1587360](#)
- During reboot, "warning: requires 'idp-sig' license" can be seen on the screen even when the device has valid license. [PR1594014](#)
- On SRX4600 devices packet drop or srpxfe core dump might be observed. [PR1620773](#)
- On SRX5600 and SRX5800 devices, the SNMP mib queries might result in occasional response timeouts. [PR1631149](#)
- IMAP/IMAPS email permitted counter is not incremented in AAMW email statistics while testing whole email block. [PR1646661](#)
- Split tunneling feature might not work. [PR1655202](#)
- SRX4600 device in split-brain scenario post ISSU. [PR1658148](#)
- The show fwauth user details is not displaying group information. [PR1659115](#)
- Traffic loss might be seen due to SPC3 packets getting stuck. [PR1671649](#)
- VPN tunnel might not be established in exclusive client scenario. [PR1674522](#)
- NetBIOS traffic (IRB broadcast) is getting dropped post upgrade on the SRX Series devices. [PR1675853](#)
- Dial-on-demand mode on the dialer interface is not working as expected. [PR1680405](#)
- SRX4600 HA might not failover properly due to a hardware failure. [PR1683213](#)
- The cluster fabric link will be down post reboot of node or power cycle. [PR1684756](#)

- The user authentication page is not rendering on the client browser. [PR1685116](#)
- Unexpected default event-rate value for event mode logging. [PR1687244](#)
- The chassis cluster will not respond to DNS queries when configured with DNS proxy service. [PR1688481](#)
- The system might stoop when Jflow inactive timeout is configured to be less than 'previous flow-inactive-timeout + 180' seconds. [PR1688627](#)
- SNMP MIB walk for jnxBoxDescr OID returns incorrect value. [PR1689705](#)
- SRX1500 chassis cluster port ge-0/0/1 does not work in switching mode. [PR1690621](#)
- SRX cluster might fail in a rare scenario when node status changes to disabled state without going through the ineligible state. [PR1692611](#)
- The process srxpfd or flowd might stop on SRX Series devices. [PR1694449](#)
- TCP packet drops are seen when services-offload is enabled. [PR1702138](#)
- The flowd process generates core files when TLS 1.3 session ticket is received on SSL-I. [PR1705044](#)
- Log streaming to the security director cloud fails on TLS when DNS re-query is performed. [PR1708116](#)
- Setting the security log profile without a category or stream will lead to srxpfe process stops. [PR1708777](#)
- On SRX Series devices with ECDSA certificate based websites are not accessible when the SSL proxy is enabled from Junos OS release 22.1R1 onwards. [PR1709386](#)
- SRX4600 doesn't support aggregated Ethernet interfaces. [PR1711467](#)
- Continuous vmcores observed on the secondary node when committing set system management-instance command [PR1712727](#)
- Continuous vmcores observed on the secondary node when committing set system management-instance command. [PR1713759](#)
- The SSL session drops because of the wrong SNI value. [PR1716893](#)

Interfaces and Chassis

- Incompatible or unsupported configuration is not getting validated correctly during ISSU/normal upgrade causing the traffic loss. [PR1692404](#)

Intrusion Detection and Prevention (IDP)

- Network outage caused during change in IDP policy. [PR1705491](#)

J-Web

- The "address-book address-book name attach zone" is unexpectedly removed when address-book entry is added or removed by J-Web. [PR1712454](#)

Layer 2 Ethernet Services

- DHCPv6 client options missing in solicit message if they exceed a certain length. [PR1702831](#)

Network Address Translation (NAT)

- Incorrectly a warning is thrown at commit check for source NAT configuration when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0. [PR1699407](#)

Network Management and Monitoring

- The source-address on syslog at custom routing-instance not applied right after rebooting. [PR1689661](#)

Platform and Infrastructure

- Syslog message CHASSISD_IPC_WRITE_ERR_NULL_ARGS at commit. [PR1663839](#)
- The "%DAEMON-4: Set system alarm failed: Operation not supported by device" message is seen on SRX5000 line of devices. [PR1681701](#)
- Fabric monitoring suspension and control link failure might cause HA cluster outage. [PR1698797](#)
- The vmcores can be seen on SRX5000 line of devices when the fxp0 interface is configured under management-instance. [PR1714002](#)

Routing Policy and Firewall Filters

- Packet drops are seen for SRX Series devices destined traffic with self-traffic-policy. [PR1698021](#)
- Security policies go out of sync during ISSU. [PR1698508](#)

User Interface and Configuration

- Configuration filtering does not work when the logical system is present. [PR1679413](#)

VPNs

- Traffic over IPsec tunnels might be dropped during ISSU. [PR1416334](#)
- While verifying show security ipsec next-hop-tunnels output in device the IPsec SA and NHTB entry is not getting cleared after configuring firewall filter. [PR1432925](#)
- Routes flapping when configuration changes are applied to custom routing instance. [PR1654516](#)
- The kmd process pause is seen if the external-interface is empty in the IKE gateway configuration. [PR1664910](#)
- VPN traffic loss is seen after HA node reboot while using traffic selectors. [PR1667223](#)
- With active/active Multi SRGs, the address pools used by SRGs in the access profile must not overlap. [PR1687654](#)
- The IKE cookies didn't change in rekey lifetime expire cases after manual failover. [PR1690921](#)
- IPsec tunnel is not getting established back after the execution of clear security ike sa command. [PR1694604](#)
- Mismatch in configured and negotiated proxy-identity parameters might generate kmd process core files. [PR1699691](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 167](#)

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

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

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

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

We have two types of releases, 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 13: 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 vMX

IN THIS SECTION

- [What's New | 168](#)
- [What's Changed | 171](#)
- [Known Limitations | 172](#)
- [Open Issues | 172](#)
- [Resolved Issues | 173](#)
- [Upgrade Instructions | 173](#)

What's New

IN THIS SECTION

- [EVPN | 168](#)
- [Interfaces | 169](#)
- [Junos Telemetry Interface | 170](#)
- [MPLS | 170](#)

Learn about new features introduced in this release for vMX.

EVPN

- **Determine IRB interface state changes based on local and remote connectivity states in EVPN fabrics (EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX2010, MX2020, vMX, QFX5110, QFX5120-48T, QFX5120-48Y, QFX5210, QFX10002, QFX10002-60, and QFX10008)—** Starting in Junos OS Release 23.1R1, the provider edge (PE) devices in an EVPN fabric consider the following factors when determining the state (up or down) of an L3 integrated routing and bridging (IRB) interface. These factors apply to an L3 IRB interface that is associated with a bridge domain or a VLAN in an EVPN instance (EVI).

- Associated local L2 interface states

To customize the L2 interface name and other parameters that the device uses to compute the IRB interface state, configure the `interface-state` statement at the `[edit interfaces irb unit n]` hierarchy.

- Remote provider edge (PE) device reachability based on the network isolation state of the bridge domain or the EVI

The device includes the states of the associated EVPN overlay tunnel interfaces in the network isolation state evaluation.

To define the parameters that determine when an EVI or a bridge domain is in a network isolation state:

1. Configure the network-isolation group `group-name` statement at the `[edit protocols]` hierarchy level to define a network isolation profile using the available options.
2. Assign the network isolation group profile to a bridge domain or an EVI using the `network-isolation-profile group network-isolation-group-name` statement at these hierarchy levels:
 - Bridge domain—`[edit bridge-domain bd-name bridge-options]`
 - EVI—`[edit routing-instance instance-name switch-options]`

[See [Determine IRB Interface State Changes from Local and Remote Connectivity States in EVPN Fabrics](#), [interface-state](#), and [network-isolation](#).]

Interfaces

- **Permanent MAC address for aggregated Ethernet interface (MX240, MX480, MX960, MX2008, MX2010, MX2020, and VMX)**—Starting in Junos OS Release 23.1R1, the number of static MAC addresses increases for:
 - VMX, MX240, MX480, and MX960 from 16 to 80.
 - MX2008, MX2010, and MX2020 from 0 to 80.

The `chassid` process (`chassisd`) now allocates MAC addresses to aggregated Ethernet interfaces in this pattern:

- First 16 interfaces receive addresses from a private MAC pool.
- Next 64 ae interfaces receive addresses from a reserved public MAC pool.
- Rest of the ae interfaces receive addresses from a public MAC pool.

[See [static-mac](#).]

Junos Telemetry Interface

- **Number of configurable BMP monitoring stations increases to a maximum of eight (MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10004, MX10008, and vMX)**—Starting in Junos OS Release 23.1R1, Junos telemetry interface (JTI) delivers initial sync and ON_CHANGE BGP routing information base (also known as routing table) statistics by using remote procedure calls (gRPC) or the gRPC network management interface (gNMI) from a device to an outside collector for a maximum of eight BMP monitoring stations.
- **Segment routing telemetry for OSPFv2 (MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and VMX)**—Starting in Junos OS Release 23.1R1, we support collection and streaming of telemetry data for segment routing with the OSPFv2 protocol. You can record statistics for the Source Packet Routing in Networking (SPRING) traffic per interface, per link aggregation group, and per segment identifier. Support includes OpenConfig and native Junos sensors. To enable collection and export of SR statistics, include the sensor-based-stats statement at the [edit protocol ospf source-packet-routing] hierarchy level.

[See [Telemetry Sensor Explorer](#) for OpenConfig sensors and [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#) for native Junos sensors.]

MPLS

- **Enable TLS for PCEP sessions (ACX5448, ACX5448-D, ACX5448-M, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, you can enable Transport Layer Security (TLS) in a Path Computation Client (PCC) to establish a TCP connection with the Path Computation Element (PCE). This connection creates a secure Path Computation Element Protocol (PCEP) session to transport PCEP messages.

To enable TLS in a PCC process (PCCD) and to establish a PCEP session, set the `tls-strict` configuration statement at the [edit protocols pcep] hierarchy level.

[See [Enabling Transport Layer Security for PCEP Sessions](#).]

- **Support to report path optimization and computed metrics in PCEP (ACX710, ACX5448, ACX5448-M, ACX5448-D, MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 23.1R1, we report PCEP path optimization metrics (IGP, TE, and delay) for RSVP and segment routing-traffic engineering (SR-TE) label-switched paths (LSPs).

To configure the interior gateway protocol (IGP), traffic engineering, and path delay optimization metrics for RSVP LSPs, include the `metric-type igp/te/delay/delay minimum` CLI statement at the [edit protocols mpls label-switched-path *lsp-name*] hierarchy level.

To configure the optimization metrics for SR-TE LSPs, include the `metric-type igp/te/delay/delay minimum` CLI statement at the `[edit protocols source-packet-routing compute-profile compute-profile-name]` hierarchy level.

[See [Reporting Path Optimization Metrics in PCEP](#).]

What's Changed

IN THIS SECTION

- [Network Management and Monitoring](#) | 171

Learn about what changed in this release for vMX.

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the `get-system-yang-packages` RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `get-system-yang-packages` RPC reply replaces the `xmlproxy-yang-modules` tag with the `proxy-xml-yang-modules` tag in the XML output.
- **Changes to the NETCONF server's `<rpc-error>` element when the `operation="delete"` operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX,**

and vSRX)—We've changed the `<rpc-error>` response that the NETCONF server returns when the `<edit-config>` or `<load-configuration>` operation uses `operation="delete"` to delete a configuration element that is absent in the target configuration. The error severity is `error` instead of `warning`, and the `<rpc-error>` element includes the `<error-tag>data-missing</error-tag>` and `<error-type>application</error-type>` elements.

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](#) | 172

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

- The input fifo errors drops reported under Packet Forwarding Engine shell show ifd but not seen in show interface extensive output. [PR1642426](#)

Resolved Issues

There are no resolved 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.

Upgrade Instructions

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

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

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

Junos OS Release Notes for vRR

IN THIS SECTION

- [What's New | 174](#)
- [What's Changed | 175](#)
- [Known Limitations | 175](#)
- [Open Issues | 175](#)
- [Resolved Issues | 175](#)

What's New

IN THIS SECTION

- [Routing Policy and Firewall Filters | 174](#)
- [Routing Protocols | 174](#)

Learn about new features introduced in this release for vRR.

Routing Policy and Firewall Filters

- **Support for the IPv6 unicast address-specific BGP extended community attribute (JRR200, QFX Series, and vRR)**—Starting in Junos OS Release 23.1R1, we support the IPv6 unicast address-specific BGP extended community attribute. You can configure the VRF route target with the IPv6 extended community. You can encode each IPv6 unicast address-specific extended community as a 20-octet file.

To accommodate the IPv6 unicast address-specific extended community, set the IPv6 community configuration under the [edit policy-options] hierarchy and set the following configuration statements in the [edit policy-options community *community-name* members] hierarchy:

- `ipv6-target:<IPv6 unicast address>:operator-defined local values`
- `ipv6-origin:<IPv6 unicast address>:operator-defined local values`
- `ipv6-extended:type-and-subtype value:<IPv6 unicast address>:operator-defined local values`

[See [show route detail](#), [show route advertising-protocol](#), [Understanding BGP Communities, Extended Communities, and Large Communities as Routing Policy Match Conditions](#), [Understanding How to Define BGP Communities and Extended Communities](#), [ipv6-extended](#), [ipv6-origin](#), and [ipv6-target](#).]

Routing Protocols

- **Support for BGP-LS NLRI to carry confederation ID (ACX710, ACX5448, MX10003, QFX5120-48YM, QFX5200, and QFX5210, and vRR)**—Starting in Junos OS Release 23.1R1, Junos OS enables BGP Link State (BGP-LS) network layer reachability information (NLRI) to carry the confederation ID in TLV 512 when BGP confederation is enabled. The NLRI carries the confederation ID along with the member autonomous system number (AS number) in TLV 517 as defined in RFC 9086. In releases before Junos OS Release 23.1R1, BGP-LS NLRI carries only the member AS number in TLV 512 and the confederation ID is not encoded in the Isdist.0 routing table.

[See [Link-State Distribution Using BGP Overview](#).]

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 23.1R1, see "[Known Limitations](#)" on page 84 for MX Series routers.

Open Issues

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

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

Resolved Issues

Learn about the issues fixed in this release for vRR.

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

Platform and Infrastructure

- With BMP RIB-IN and BMP RIB-OUT configured on MX or PTX platforms, large number of BGP routes remain in hold-down state after route churn. [PR1685510](#)

- A 802.1Q tagged Ethernet traffic with an expected VLAN ID and with a nonzero 802.1P value ingressing a JRR200 VLAN enabled interface is dropped. [PR1691694](#)
- The rpd process stops when rib-sharding configured. [PR1699557](#)

Junos OS Release Notes for vSRX

IN THIS SECTION

- [What's New | 176](#)
- [What's Changed | 180](#)
- [Known Limitations | 187](#)
- [Open Issues | 187](#)
- [Resolved Issues | 188](#)
- [Migration, Upgrade, and Downgrade Instructions | 189](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 177](#)
- [Chassis Cluster-specific | 177](#)
- [Flow-based and Packet-based Processing | 177](#)
- [Intrusion Detection and Prevention | 177](#)
- [Network Management and Monitoring | 178](#)
- [Platform and Infrastructure | 178](#)
- [Content Security | 179](#)
- [VPNs | 179](#)

Learn about new features introduced in this release for vSRX.

Authentication and Access Control

- **Support for multiple certificates and multiple domains (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we support multiple certificates with multiple domains and a single certificate with multiple domains for J-Web sessions. You can enter a new configuration statement `virtual-domain` in the `[edit system services web-management https]` hierarchy level to use this feature. This helps in having multiple sessions without any certificate warning.

[See [https \(Web Management\)](#).]

Chassis Cluster-specific

- **Support for IPv4 and IPv6 unicast IP-over-IP tunneling (SRX Series and vSRX)**—Starting in Junos OS Release 23.1R1, we support IP-over-IP tunneling for IPv4 and IPv6 traffic.

[See [IP-over-IP Tunneling](#).]

Flow-based and Packet-based Processing

- **Debug improvement of policy PFE control thread (SRX300, SRX320, SRX340, SRX345, SRX380, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can configure `services-offload` and `no-services-offload` in a mutually exclusive way. If you configure `services-offload`, then `no-services-offload` is automatically disabled. If you configure `no-services-offload`, then `services-offload` is automatically disabled. You cannot configure and commit both options simultaneously.

[See [show security policies](#).]

Intrusion Detection and Prevention

- **Support for on-box IDP Control Plane Packet Capture (SRX380, SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600, SRX550HM, SRX5400, SRX5600, SRX5800, vSRX 2.0, vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can store the packets captured by intrusion detection and prevention (IDP) locally on the SRX device. You can view the details on the UI or J-Web. The captured traffic is stored on the device at `/var/log/pcap/idp/`. You can limit the number of local packet capture files that are created using a configuration and the log rotation facility.

To support this new feature, we've:

- Added new counters to the existing packet-log counters.
- Provided a command to clear all the captured files.

[See <https://www.juniper.net/documentation/us/en/software/junos/idp-policy/topics/topic-map/security-idp-packet-capture.html>]

Network Management and Monitoring

- **On-box logging modernization (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can use the following operational commands to optimize the database query performance:

- `show security log report in-detail`
- `show security log report in-interval`
- `show security log report summary`

[See [Understanding On-Box Logging and Reporting](#), [show security log report in-detail](#), [show security log report in-interval](#), and [show security log report summary](#).]

- **Support for DNS logging in on-box reporting (SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, vSRX, and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've added support for DNS logging in on-box reporting. You can now use on-box reporting with:

- New logging database for DNS.
- in-detail and summary CLI query options for DNS.
- DNS as part of the threat category.

[See [Understanding On-Box Logging and Reporting](#), [show security log report in-detail](#), and [show security log report summary](#).]

Platform and Infrastructure

- **Geneve flow infrastructure support (vSRX 3.0)** —Starting in Junos OS Release 23.1R1, vSRX 3.0 supports Geneve flow infrastructure for Geneve tunnel packet processing. With this support, you can use vSRX 3.0 as a transit router or a tunnel endpoint device in various cloud deployments. For example, you can integrate vSRX 3.0 with Amazon Web Services (AWS) Gateway Load Balancer (GWLB) service that uses the Geneve protocol encapsulation for transparent routing of packets between GWLB and virtual appliances.

With this support, vSRX 3.0 can:

- De-encapsulate the received Geneve tunnel packets.
- Analyze Geneve header and option fields.
- Inspect the inner packet with security services.
- Encapsulate the original inner packet and forward the packet to the destination.

[See [Geneve Flow Infrastructure on vSRX 3.0](#) and [AWS Gateway Load Balancing with Geneve](#).]

Content Security

- **Sophos Live Protection version 2.0 support for content security (SRX Series and vSRX)**—Starting in Junos OS Release 23.1R1, content security supports antivirus Sophos Live Protection version 2.0. The new version of Sophos antivirus uses an HTTPS connection for the device-to-server communication. For the HTTPS connection, you must create an SSL initiation profile and add the profile to the default configuration of the Sophos engine.

We've introduced the `host`, `port`, and `ssl-profile` statements at the `[edit security utm default-configuration anti-virus sophos-engine server]` hierarchy level. In addition, we've deprecated the `sxl-retry` and `sxl-timeout` statements at the `[edit security utm default-configuration anti-virus sophos-engine]` and `[security utm feature-profile anti-virus sophos-engine]` hierarchy levels.

[See [server \(Security Sophos Engine Antivirus\)](#), [Sophos Antivirus Protection Overview](#), and [show security utm anti-virus status](#)].

VPNs

- **Introduction of prelogon compliance checks (SRX Series and vSRX 3.0)**—In Junos OS Release 23.1R1, we introduce prelogon compliance for Juniper Secure Connect. This functionality validates the current status of a connecting client device prior to the authentication (that is, before user's login). You can configure different match criteria on the SRX Series firewall to allow or reject client devices.

You can configure this feature using the statement `compliance pre-logon name` at:

- `[edit security remote-access]` hierarchy level to configure prelogon compliance rules.
- `[edit security remote-access profile realm-name]` hierarchy level to associate a prelogon compliance rule to the remote-access profile.

[See [prelogon compliance checks](#).]

- **Support for application bypass in Juniper Secure Connect (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, you can use Juniper Secure Connect to send specific application traffic directly to its destination instead of passing it through the VPN tunnel. You can accomplish this functionality by specifying domain names and protocols for the specified applications that would bypass the VPN tunnel. The bypass feature simplifies the administrator and end-user experience.

When you configure the application bypass feature and establish a remote-access VPN tunnel, the configuration automatically enables a stateful firewall rule rejecting incoming connections on other adapters, which prevents the device from becoming a bastion host.

You can configure this feature on SRX Series firewalls and on vSRX 3.0 virtual firewalls by using `application-bypass` at the `[edit security remote-access client-config name]` hierarchy level.

[See [Application Bypass](#).]

- **Support for multiple certificates and multiple domains (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, with support for multiple certificates and multiple domains, we now allow Juniper Secure Connect connection profiles with different URLs without any certificate warning.

[See [Multiple certificates and domains support](#).]

What's Changed

IN THIS SECTION

- [EVPN | 180](#)
- [Flow-Based and Packet-Based Processing | 181](#)
- [General Routing | 181](#)
- [Network Management and Monitoring | 181](#)
- [PKI | 182](#)
- [VPNs | 184](#)

Learn about what changed in this release for vSRX.

EVPN

- **Flow-label configuration status for EVPN ELAN services** The output for the `show evpn instance extensive` command now displays the flow-label and flow-label-static operational status for a device and not for the routing instances. A device with `flow-label` enabled supports flow-aware transport (FAT) flow labels and advertises its support to its neighbors. A device with `flow-label-static` enabled supports FAT flow labels but does not advertise its capabilities.
- **Specify the UDP source port in a ping overlay or traceroute overlay operation** — In Junos OS releases prior to 22.4R1, you could not configure the `udp` source port in a ping overlay or traceroute overlay operation. You may now configure this value in an EVPN-VXLAN environment using `hash`. The configuration option `hash` will override any other `hash-*` options that may be used to determine the source port value.

Flow-Based and Packet-Based Processing

- **PMI Mode Passthrough ESP traffic:** Starting in Junos OS Release 22.1R3, we support the PMI express path processing for passthrough ESP traffic on the SRX Series devices.
- **Flow session operational command support for UTM (SRX Series and vSRX)**—We've extended the `show security flow session` operational command support to view the details of the content filtering and Web filtering UTM features.

[See [show security flow session](#).]

General Routing

- When subscribing to the resource path `/junos/system/linecard/environment`, the prefix for the streamed path at the collector side was displaying as `/junos/linecard/environment`. This issue is resolved in Junos OS 23.1R1 and Junos OS Evolved 23.1R1 and the subscription path and the streamed path match to display `/junos/system/linecard/environment`.
- **Time zone support for local certificate verification (SRX1500 and SRX5600)**—Starting in this release, when the local certificate verification fails, you can see the time zone for the failed local certificate in the command output and system log messages.

Network Management and Monitoring

- **operator login class is restricted from viewing NETCONF trace files that are no-world-readable (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—When you configure NETCONF tracing options at the `[edit system services netconf traceoptions]` hierarchy level and you restrict file access to the file owner by setting or omitting the `no-world-readable` statement (the default), users assigned to the operator login class do not have permissions to view the trace file.
- **Support for the `junos:cli-feature` YANG extension (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The `cli-feature` YANG extension identifies certain CLI properties associated with some command options and configuration statements. The Junos YANG modules that define the configuration or RPCs include the `cli-feature` extension statement, where appropriate, in schemas emitted with extensions. This extension is beneficial when a client consumes YANG data models, but for certain workflows, the client needs to generate CLI-based tools.

[See [Understanding the Junos DDL Extensions YANG Module](#).]

- **XML tag in the get-system-yang-packages RPC reply changed (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—The get-system-yang-packages RPC reply replaces the xmlproxy-yang-modules tag with the proxy-xml-yang-modules tag in the XML output.
- **Changes to the NETCONF server's <rpc-error> element when the operation="delete" operation deletes a nonexistent configuration object (ACX Series, EX Series, MX Series, QFX Series, SRX Series, vMX, and vSRX)**—We've changed the <rpc-error> response that the NETCONF server returns when the <edit-config> or <load-configuration> operation uses operation="delete" to delete a configuration element that is absent in the target configuration. The error severity is error instead of warning, and the <rpc-error> element includes the <error-tag>data-missing</error-tag> and <error-type>application</error-type> elements.

PKI

- **Deprecating options related to certificate enrollment (Junos)**—Starting in Junos OS Release 23.2R1, we're deprecating earlier CLI options related to Public Key Infrastructure (PKI) to enroll and reenroll local certificate through Simple Certificate Enrolment Protocol (SCEP). The table below shows the Junos CLI commands and configuration statements with the options being deprecated. You can find the same CLI options now available under scep option in these commands and statements.

Table 14: Deprecated Junos CLI Options

Junos CLI Commands and Statements	Deprecated Options
set security pki auto-re-enrollment	certificate-id

Table 14: Deprecated Junos CLI Options *(Continued)*

Junos CLI Commands and Statements	Deprecated Options
request security pki local-certificate enroll	ca-profile certificate-id challenge-password digest domain-name email ip-address ipv6-address logical-system scep-digest-algorithm scep-encryption-algorithm subject

Table 14: Deprecated Junos CLI Options (*Continued*)

Junos CLI Commands and Statements	Deprecated Options
request security pki node-local local-certificate enroll	ca-profile certificate-id challenge-password digest domain-name email ip-address ipv6-address logical-system scep-digest-algorithm scep-encryption-algorithm subject

[See [auto-re-enrollment \(Security\)](#), [request security pki local-certificate enroll scep](#), and [request security pki node-local local-certificate enroll](#).]

VPNs

- **Change format of remote-access profile names (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 23.1R1, we've changed the format of remote-access profile names to enhance end-user experience using Juniper Secure Connect. In releases before Junos OS Release 23.1R1, you configure the remote-access profile name using the realm name at the `[edit security remote-access profile realm-name]` hierarchy level. But with organizations connecting to several gateways, using the remote-access profile names, such as `hr`, multiple times in the remote-access connection profile becomes unmanageable.

To address this issue, we introduce a new convention for configuring remote-access profile names. You can now configure profile names with URLs using any of the following formats at the `[edit`

security remote-access profile *realm-name*] hierarchy level, so that end users can connect to the relevant gateway:

- *FQDN/RealmName*
- *FQDN*
- *IP address/RealmName*
- *IP address*

For example, you can now use **ra.example.com/hr**, **ra1.example.com/hr** and **ra.example.com** as realm names.

With the introduction of this convention, we need to deprecate the existing default-profile option at the [edit security remote-access] hierarchy level. Your remote-access profiles names will refer to URLs either with an FQDN or with an IP address, depending on how the end users would connect—for example, **ra.example.com/hr**, **ra.example.com**, **192.168.1.10/hr** or **192.168.1.10**. With this change, the end user will now see the connection profile name in the Juniper Secure Connect application as **ra.example.com/hr** instead of **hr**, as was the case in earlier releases.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name **hr** in the current configuration to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the follow commands -

- ```
user@host# rename security remote-access profile hr to profile ra.example.net/hr
```
- ```
user@host# rename security remote-access profile hr to profile 192.168.1.10/hr
```

[See [profile \(Juniper Secure Connect\)](#).]

- **Unavailability of default-profile option for remote-access VPN solution (SRX Series and vSRX 3.0)—** Starting in Junos OS Release 23.1R1, we've hidden the default-profile option at the [edit security remote-access] hierarchy level. In releases before Junos OS Release 23.1R1, you use this option to specify one of the remote-access profiles as the default profile in Juniper Secure Connect. But with changes to the format of remote-access profile names, we no longer require the default-profile option.

We've deprecated the default-profile option—rather than immediately removing it—to provide backward compatibility and a chance to make your existing configuration conform to the changed configuration. You'll receive a warning message if you continue to use the default-profile option in your configuration. However, modifying the current configuration does not affect existing deployments.

In existing deployments, to ensure a smooth transition with this change, we recommend that you modify the profile name in the current configuration **hr** to **ra.example.com/hr** or **192.168.1.10/hr** at the [edit] hierarchy level using the following commands -

- ```
user@host# rename security remote-access profile hr to profile ra.example.net/hr
```
- ```
user@host# rename security remote-access profile hr to profile 192.168.1.10/hr
```

For new configurations, consider the following scenarios to create a new remote-access profile based on how your end users connect using the Juniper Secure Connect application:

- If your end users connect using an IP address, specify the IP address in the profile name.
- If your end users connect using an FQDN, specify the FQDN in the profile name.
- If you need to separate users with different realm values such as **hr**, append **/hr** to the IP address or FQDN as follows:
 - ```
[edit security remote-access profile ra.example.net/hr]
```
  - ```
[edit security remote-access profile 192.168.1.10/hr]
```

[See [default-profile \(Juniper Secure Connect\)](#) .

- **Remote-access VPN solution doesn't support hexadecimal pre-shared (SRX Series and vSRX 3.0)**—With remote-access VPN solution, for pre-shared-key based authentication method, we support ascii-text format. This means, do not use hexadecimal format for the pre-shared keys in your configuration for remote-access VPN solution. Therefore, configure the statement `ascii-text` with ascii text format at `[edit security ike policy policy-name pre-shared-key]` hierarchy level for use with Juniper Secure Connect.
- **Enhancement to SCEP PKI Certificate Enrollment**—Logical-system option is added to SCEP PKI certificate enrollment.
[See [request security pki local-certificate enroll scep.](#)]
- **Limited ECDSA Certificate Support with SSL Proxy (SRX Series and vSRX 3.0)**—With SSL proxy configured on SRX Series firewall and vSRX Virtual firewalls,
 - ECDSA based websites with P-384/P-521 server certificates are not accessible with any root-ca certificate as the security device has limitation to support only P-256 group.
 - When RSA based root-ca and P-384/P-521 ECDSA root-ca certificate is configured, all ECDSA websites will not be accessible as SSL-Terminator is negotiated with RSA, which is why the security device is sending only RSA ciphers and sigalgs to the destination web server while doing

the SSL handshake. To ensure both ECDSA and RSA-based websites are accessible along with the RSA root certificate, configure a 256-bits ECDSA root certificate.

- In some scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server does not support P-256 groups.
- In other scenarios, even if 256-bit ECDSA root certificate is used in the SSL proxy configuration, ECDSA based websites with P-256 server certificates are not accessible if the server supports sigalgs other than P-256. The issue is seen in hardware offload mode with failing signature verification. As hardware offload for ECDSA certificate is introduced in Junos OS release 22.1R1, this issue will not be observed if you use Junos OS released prior to 22.1R1. Also, the issue is not seen if the SSL-proxy for ECDSA certificate is handled in software.
- **Changes to IP address byte order (vSRX 3.0)**—In syslog messages for *KMD_VPN_DOWN_ALARM_USER* and *KMD_VPN_UP_ALARM_USER*, the IP address byte order now appears in the correct order as against the reverse byte order which was appearing in earlier releases.

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.

General Routing

- When APBR profile is configured as a policy and not attached to a security zone and a failover occurs in between a long-lived ALG (FTP-DATA) session, then the APBR info does not populated in the AppTrack session close log from the backup node. This issue will be seen only when the (FTP) control session and the ALG FTP-DATA) session are not active on the same node. [PR1688021](#)

Resolved Issues

IN THIS SECTION

- [Resolved Issues: 23.1R1 | 189](#)

Learn about the issues fixed in this release for vSRX.

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

Application Layer Gateways (ALGs)

- H.323 traffic failure caused by RAS packet drops when incorrect route lookup performed. [PR1688986](#)

Flow-Based and Packet-Based Processing

- Packet loss on GRE tunnel due to improper route look up for tunnel destination. [PR1683334](#)
- When PMI mode is enabled, uplink-incoming-interface-name not updated properly though link switch is successful by APBR as well as symmetric routing maintained. [PR1692062](#)
- TCP session timeout seen on GRE tunnel. [PR1708646](#)

General Routing

- Unexpected behavior when web-proxy is configured with ssl-proxy. [PR1580526](#)
- Split tunneling feature might not work. [PR1655202](#)
- Change in few fields of IKE_VPN_UP_ALARM_USER and IKE_VPN_DOWN_ALARM_USER syslogs of IKED. [PR1657704](#)
- ARP might not get learned if redundant Ethernet interface is configured with VLAN. [PR1681042](#)
- The jnxOperatingDescr.1.1.0.0 returns blank, but jnxOperatingState.1.1.0.0 returns value. [PR1683753](#)
- GeoIP cloud feed update is failing. [PR1698589](#)

- Log streaming to the security director cloud fails on TLS when DNS re-query is performed. [PR1708116](#)
- VLAN tagging does not work for vSRX3.0 on HyperV Windows Server 2019 data center. [PR1711440](#)

Network Address Translation (NAT)

- Incorrectly a warning is thrown at commit check for source NAT configure when the source-address or destination-address of the NAT rule is set as 0.0.0.0/0. [PR1699407](#)

Services Applications

- The srpxfe generates core file when the EVPN and XLAN configured. [PR1704061](#)

Resolved Issues: 23.1R1

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 195](#)

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 23.1R1 for vSRX using J-Web (see [J-Web](#)) or the Junos Space Network Management Platform (see [Junos Space](#)).

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

The following limitations apply:

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

Check this using the following command:

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

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

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

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

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 23.1R1 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 23.1R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz /var/crash/corefiles/
```

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

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING: This package will load JUNOS 20.4 software.
WARNING: It will save JUNOS configuration files, and SSH keys
WARNING: (if configured), but erase all other files and information
WARNING: stored on this machine. It will attempt to preserve dumps
WARNING: and log files, but this can not be guaranteed. This is the
WARNING: pre-installation stage and all the software is loaded when
WARNING: you reboot the system.
Saving the config files ...
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
=====
Host OS upgrade is FORCED
```

```

Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
=====
Installing Host OS ...
upgrade_platform: -----
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-
linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -----
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz..
./
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...

```

```

upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software rollback'
WARNING:      command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07

```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 23.1R1 for vSRX.

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

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

```

--- JUNOS 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE
JUNOS OS Kernel 64-bit [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]

```

```

JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]

```

Validating the OVA Image

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

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

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

We have two types of releases, 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 15: 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](#).

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 | 198
- Creating a Service Request with JTAC | 199

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net/>

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

Creating a Service Request with JTAC

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

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

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

Revision History

8 August 2024—Revision 17, Junos OS Release 23.1R1.

11 July 2024—Revision 16, Junos OS Release 23.1R1.

16 November 2023—Revision 15, Junos OS Release 23.1R1.

14 September 2023—Revision 14, Junos OS Release 23.1R1.

20 July 2023—Revision 13, Junos OS Release 23.1R1.

6 July 2023—Revision 12, Junos OS Release 23.1R1.

1 June 2023—Revision 11, Junos OS Release 23.1R1.

25 May 2023—Revision 10, Junos OS Release 23.1R1.

11 May 2023—Revision 9, Junos OS Release 23.1R1.

4 May 2023—Revision 8, Junos OS Release 23.1R1.

19 April 2023—Revision 7, Junos OS Release 23.1R1.

13 April 2023—Revision 6, Junos OS Release 23.1R1.

6 April 2023—Revision 5, Junos OS Release 23.1R1.

31 March 2023—Revision 4, Junos OS Release 23.1R1.

23 March 2023—Revision 3, Junos OS Release 23.1R1.

17 March 2023—Revision 2, Junos OS Release 23.1R1.

16 March 2023—Revision 1, Junos OS Release 23.1R1.

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 © 2024 Juniper Networks, Inc. All rights reserved.