

Release Notes

Published
2025-01-17

Junos OS Release 23.4R1®

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewalls, vRR, and vSRX Virtual Firewall. These release notes accompany Junos OS Release 23.4R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

Table of Contents

Introduction | 1

Junos OS Release Notes for ACX Series

What's New | 1

What's Changed | 2

Known Limitations | 4

Open Issues | 4

Resolved Issues | 5

Migration, Upgrade, and Downgrade Instructions | 7

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 7

Junos OS Release Notes for cRPD

What's New | 9

Licensing | 9

Additional Features | 9

Known Limitations | 9

Open Issues | 10

Resolved Issues | 10

Junos OS Release Notes for cSRX

What's New | 11

Authentication and Access Control | 11

Content Security | 12

Device Security | 12

Flow-based and Packet-based Processing | 12

Public Key Infrastructure (PKI) | 13

VPNs | 13

What's Changed | 14

Known Limitations | 14

Open Issues | 14

Resolved Issues | 15

Junos OS Release Notes for EX Series

What's New | 16

Authentication and Access Control | 17

Chassis | 18

Dynamic Host Configuration Protocol | 18

Ethernet Switching and Bridging | 19

EVPN | 20

Interfaces | 26

Junos Telemetry Interface | 27

Layer 2 Features | 28

Network Management and Monitoring | 29

MC-LAG | 29

Routing Protocols | 30

Additional Features | 30

What's Changed | 31

Known Limitations | 33

Open Issues | 34

Resolved Issues | 37

Migration, Upgrade, and Downgrade Instructions | 43

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 43

Junos OS Release Notes for JRR Series

What's New | 45

What's Changed | 45

Known Limitations | 45

Open Issues | 46

Resolved Issues | 46

Migration, Upgrade, and Downgrade Instructions | 46

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 47

Junos OS Release Notes for Juniper Secure Connect

What's New | 48

What's Changed | 49

Known Limitations | 49

Open Issues | 49

Resolved Issues | 49

Junos OS Release Notes for MX Series

What's New | 50

Hardware | 51

Authentication and Access Control | 51

Chassis | 52

Class of Service | 52

EVPN | 52

High Availability | 55

Interfaces | 56

IPv6 | 56

Juniper Extension Toolkit (JET) | 58

Junos Telemetry Interface | 58

MPLS | 65

Multicast | 70

Network Address Translation (NAT) | 71

Network Management and Monitoring | 72

Platform and Infrastructure | 72

Precision Time Protocol (PTP) | 74

Routing Options | 74

Routing Protocols | 74

Public Key Infrastructure (PKI) | 76

Services Applications | 76

Software Defined Networking (SDN) | 76

Source Packet Routing in Networking (SPRING) or Segment Routing | 76

Subscriber Management and Services | 78

System Logging | 80

VPNs | 80

Additional Features | 81

What's Changed | 82

Known Limitations | 85

Open Issues | 86

Resolved Issues | 92

Migration, Upgrade, and Downgrade Instructions | 110

Junos OS Release Notes for NFX Series

What's New | 118

Authentication and Access Control | 118

Class of Service | 119

Flow-based and Packet-based Processing | 119

Software Installation and Upgrade | 119

What's Changed | 120

Known Limitations | 120

Open Issues | 121

Resolved Issues | 122

Migration, Upgrade, and Downgrade Instructions | 123

Junos OS Release Notes for QFX Series

What's New | 126

Authentication and Access Control | 127

EVPN | 127

Interfaces | 129

Junos Telemetry Interface | 130

Network Management and Monitoring | 130

Additional Features | 131

What's Changed | 131

Known Limitations | 134

Open Issues | 134

Resolved Issues | 136

Migration, Upgrade, and Downgrade Instructions | 141

Junos OS Release Notes for SRX Series Firewalls

What's New | 155

Hardware | 156

Application Identification (AppID) | 174

Authentication and Access Control | 175

Chassis | 175

Class of Service	176
Content Security	176
Device Security	176
Flow-based and Packet-based Processing	177
High Availability	178
Interfaces	180
J-Web	180
Juniper Advanced Threat Prevention Cloud (ATP Cloud)	184
Junos Telemetry Interface	185
Network Address Translation (NAT)	186
Network Management and Monitoring	187
Public Key Infrastructure (PKI)	187
VPNs	188
Additional Features	189

What's Changed | 190

Known Limitations | 194

Open Issues | 195

Resolved Issues | 196

Migration, Upgrade, and Downgrade Instructions | 202

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases	202
--	-----

Documentation Updates | 203

Junos OS Release Notes for vRR

What's New | 205

Junos Telemetry Interface	205
---------------------------	-----

What's Changed | 207

Known Limitations | 207

Open Issues | 207

Resolved Issues | 207

Junos OS Release Notes for vSRX Virtual Firewall

What's New | 208

Application Identification (AppID) | 209

Authentication and Access Control | 209

Content Security | 210

Device Security | 210

Flow-based and Packet-based Processing | 211

J-Web | 212

Juniper Advanced Threat Prevention Cloud (ATP Cloud) | 216

Network Address Translation (NAT) | 216

Platform and Infrastructure | 217

Public Key Infrastructure (PKI) | 218

VPNs | 218

What's Changed | 220

Known Limitations | 224

Open Issues | 224

Resolved Issues | 224

Migration, Upgrade, and Downgrade Instructions | 226

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life
Releases | 232

Licensing | 233

Finding More Information | 234

Requesting Technical Support | 235

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, MX Series, NFX Series, QFX Series, SRX Series Firewall, vRR, and vSRX Virtual Firewall. These release notes accompany Junos OS Release 23.4R1. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for ACX Series

IN THIS SECTION

- [What's New | 1](#)
- [What's Changed | 2](#)
- [Known Limitations | 4](#)
- [Open Issues | 4](#)
- [Resolved Issues | 5](#)
- [Migration, Upgrade, and Downgrade Instructions | 7](#)

What's New

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

To view features supported on the ACX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R1, click the Group by Release link. You can collapse and expand the list as needed.

- [ACX710](#)
- [ACX5448-D](#)
- [ACX5448-M](#)
- [ACX5448](#)

What's Changed

IN THIS SECTION

- [General Routing | 2](#)
- [Junos XML API and Scripting | 3](#)
- [Network Management and Monitoring | 3](#)

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

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.
- **Deprecated license revoke information**—Starting in Junos OS Release 23.4R1, we've deprecated the `show system license revoked-info` command. You can use the `show system license` and `show system license usage` commands to know the license information.
- **Change in the XML tags displayed for the `show virtual-network-functions` command in JDM (Junos node slicing)**— To align the XML tags displayed for the `show virtual-network-functions gnf-name | display xml` with the new XML validation logic, we have replaced the underscores (`_`) in the output with hyphens (`-`) as shown below:

Old output: `user@jdm> show virtual-network-functions mgb-gnf-d | display xml` `<rpc-reply xmlns:junos=http://xml.juniper.net/junos/23.4I0/junos> <vnf-information xmlns=http://xml.juniper.net/junos/23.4I0/junos-jdmd junos:style="detail"> <vnf-instance> <id>1</id> <name>mgb-gnf-d</name> <state>Running</state> <liveliness>down</liveliness> <ip_addr>192.168.2.1</ip_addr> <<< The tag includes _. <vcpus>2</vcpus> <max_mem>16GiB</max_mem> <<< The tag includes _. <resource_template>2core-16g</resource_template> <<< The tag includes _. <qemu_process_id>614702</qemu_process_id> <<< The tag includes _. <smbios_version>v2</smbios_version> <<< The tag includes _. <vnf-blk-dev-list> </vnf-blk-dev-list> </vnf-instance> </vnf-information> <cli> <banner></banner> </cli> </rpc-reply>`

New output: `user@jdm> show virtual-network-functions mgb-gnf-d | display xml` `<rpc-reply xmlns:junos=http://xml.juniper.net/junos/23.4I0/junos> <vnf-information xmlns=http://xml.juniper.net/junos/23.4I0/junos-jdmd`

```
junos:style="detail"> <vnf-instance> <id>1</id> <name>mgb-gnf-d</name> <state>Running</state>
<liveliness>down</liveliness> <ip-addr>192.168.2.1</ip-addr> <<< The tag changes to ip-addr. <vcpus>2</vcpus>
<max-mem>16GiB</max-mem> <<< The tag changes to max-mem. <resource-template>2core-16g</resource-template> <<<
The tag changes to resource-template. <qemu-process-id>614702</qemu-process-id> <<< The tag changes to qemu-
process-id. <smbios-version>v2</smbios-version> <<< The tag changes to smbios-version. <vnf-blk-dev-list> </
vnf-blk-dev-list> </vnf-instance> </vnf-information> <cli> <banner></banner> </cli> </rpc-reply>
```

This change is applicable to any RPC that previously had underscores in the XML tag name.

- In the CLI using the command `request chassis feb slot slot-number offline` if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is rejected. If offline/restart is still intended for primary FEB, use `force` option in addition to the command. WARNING message displayed in the CLI: "warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using `request chassis routing-engine master switch` CLI. If offline/restart is still intended, use `force` option in addition to this CLI."

Junos XML API and Scripting

- **Ability to commit extension-service file configuration when application file is unavailable**—When you set the optional option at the `edit system extension extension-service application file file-name` hierarchy level, the operating system can commit the configuration even if the file is not available at the `/var/db/scripts/jet` file path.

[See [file \(JET\)](#).]

- **XML output tags changed for `request-commit-server-pause` and `request-commit-server-start` (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the `request system commit server pause` command (`request-commit-server-pause` RPC) and the `request system commit server start` command (`request-commit-server-start` RPC). The root element is `<commit-server-operation>` instead of `<commit-server-information>`, and the `<output>` tag is renamed to `<message>`.

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

[See [<copy-config>](#).]

- **ephemeral-db-support statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the ephemeral-db-support statement at the [edit protocols layer2-control] hierarchy level in the static configuration database.

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

Known Limitations

IN THIS SECTION

- [Infrastructure | 4](#)

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

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

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and later, validation and upgrade might fail. The upgrade requires using the no-validate option to complete successfully. [PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 5](#)
- [MPLS | 5](#)

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 ACX1K/2K platforms, when a lo0.x filter is configured under a vrf type routing-instance, any IPv4 transit traffic that makes ARP request to generate to the CE-facing interfaces will fail in ARP resolution due to the ARP request packets are discard by lo0.x filter if no specific term to accept the IPv4 packets. [PR1737999](#)
- Due to software issue with initialization sequence, the PTP encapsulation does not get applied with PTP configuration on ge interfaces. Because of this, PTP feature is impacted on ge interfaces. [PR1755852](#)
- Some Junos OS Releases from 21.4R3 to 22.4R3, might display the Remote fault state as 'Offline' in show interface by default. [PR1764243](#)

MPLS

- The default behavior of local reversion has changed from Junos OS Release 16.1 and that impacts the LSPs for which the ingress does not perform make-before-break. Junos OS does not perform make-before-break for no-cspf LSPs. [PR1401800](#)

Resolved Issues

IN THIS SECTION

- [Platform and Infrastructure](#) | 6

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.

Platform and Infrastructure

- TCP window scaling may be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. [PR1761242](#)
- Delegated BFD sessions configured on routing-instance may fail to come up. [PR1633395](#)
- Interface queues display incorrect values of default reserved buffers [PR1689183](#)
- dc-pfe: HEAP malloc(0) detected! when a VPLS instance is deactivated in ACX5048. [PR1692400](#)
- Link is not going down physically while disabling the l2circuit configured interface on Junos based ACX5448 platform [PR1703935](#)
- L3VPN traffic loss and PFE errors can be seen after an LSP Flap. [PR1719507](#)
- [ACX5048] L2circuit might drop forwarding traffic after flaps although it's in UP state; acx_rt_ccc_eth_vpws_vpn_uni_port_add:UNI VPWS port_add failed AC-IFL: VPN: (-15:Invalid configuration) [PR1726711](#)
- A panic reboot will be observed due to deadlock on VMhost platforms. [PR1727985](#)
- Traffic drops on certain ACX platforms after it is upgraded. [PR1731081](#)
- EVPN instance traffic will be dropped when hierarchical-scheduler is enabled on the CE interface. [PR1732124](#)
- The IPv4 classification and EXP remarking might not work as expected in the IP-MPLS scenario. [PR1732509](#)
- Crash on all Junos VMhost platforms due to deadlock panic. [PR1735843](#)
- Traffic loss in ACX710 and ACX5448 on any-mpls unicast nexthop protocol configuration [PR1742960](#)
- [TWM Clocking Solution] - chassis clock status should not move to "holdover" while switching between PTP path alone. [PR1745604](#)
- QSFP interfaces show additional flap during PFE bringup. [PR1747140](#)
- The memory consumption increases due to memory leak. [PR1747992](#)
- Interfaces fail to come online post upgrade. [PR1750814](#)

- Default ieee-8021p classifier not working for UNI interface for Layer 2 services. [PR1756150](#)
- Interface flaps leading to PFE crash due to FPC heap corruption. [PR1764083](#)
- On ACX710 and ACX5448 devices with hierarchical-scheduler on CE interfaces, the EVPN ETREE Leaf to LEAF communication is allowed. [PR1765486](#)
- On ACX5448 and ACX710 with hierarchical-scheduler LACP packets are not being sent after chassis reboot. [PR1765478](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 7](#)

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

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

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

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 1: EOL and EEOL Releases

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

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

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

Junos OS Release Notes for cRPD

IN THIS SECTION

- [What's New | 9](#)
- [Known Limitations | 9](#)
- [Open Issues | 10](#)
- [Resolved Issues | 10](#)

What's New

IN THIS SECTION

- [Licensing | 9](#)
- [Additional Features | 9](#)

Learn about new features introduced in this release for cRPD.

Licensing

- **New license keys (cRPD)**—Starting in Junos OS Release 23.4R1, cRPD uses a different licensing management system from earlier releases. You must regenerate your license keys before you upgrade cRPD to Junos OS Release 23.4R1 or later. License keys generated through the older licensing management system will not work. See [Activate Junos OS Licenses](#) for instructions to generate your new license keys.

Additional Features

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

- **Support for logging using eventd and time zone**

[See [Configure Time Zones](#), [time-zone](#), and [No Link Title](#).]

- **Support for RADIUS server (cRPD)**. We provide RADIUS server support to use authentication, authorization, and accounting (AAA) features on cRPD.

[See [RADIUS Authentication](#), [radius \(System\)](#), and [radius-server \(System\)](#).]

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

IN THIS SECTION

- [General Routing](#) | 10

Learn about the issues fixed in this release for cRPD 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

- Rpd process generates core files when you delete protocols MPLS in `krt_fc_table_destroy` on cRPD container. [PR1703415](#)
- BGP sessions flap due to license updates. [PR1737035](#)
- Deprecated the unsupported `route-record` option from `routing-options`. [PR1754845](#)
- With the BGP RIB sharding enabled, you might observe high CPU utilization. [PR1765417](#)

Junos OS Release Notes for cSRX

IN THIS SECTION

- [What's New | 11](#)
- [What's Changed | 14](#)
- [Known Limitations | 14](#)
- [Open Issues | 14](#)
- [Resolved Issues | 15](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 11](#)
- [Content Security | 12](#)
- [Device Security | 12](#)
- [Flow-based and Packet-based Processing | 12](#)
- [Public Key Infrastructure \(PKI\) | 13](#)
- [VPNs | 13](#)

Learn about new features introduced in this release for cSRX.

Authentication and Access Control

- **User Firewall and JIMS integration (cSRX)**—Starting in Junos OS Release 23.4R1, cSRX supports User Firewall active directory and Juniper® Identity Management Service (JIMS) integration.

The cSRX instances can now create, manage, and refine firewall rules based on user identity rather than IP address and query JIMS.

JIMS then communicates with Active Directory to retrieve the username-to-group mapping information. The cSRX instances use the username-to-group mapping information to identify the group to which each user belongs and then enforces appropriate security policy decisions.

[See [Authentication and Integrated User Firewalls User Guide](#)[Juniper Identity Management Service User Guide](#)].

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

Content Security

- **Juniper NextGen Web Filtering (SRX Series and cSRX)**—Starting in Junos OS Release 23.4R1, Juniper NextGen Web Filtering (NGWF) is available as the URL filtering infrastructure in the Juniper cloud. It uses the OEM Cloud for URL reputation and category. NGWF enables the SRX Series Firewall and cSRX Container Firewall to permit or deny access to specific URLs based on the reputation and category to which the URLs belong. It intercepts, scans, and acts upon HTTP or HTTPS traffic to prevent inappropriate Web content access. It also provides better visibility into the URL traffic.

[See [Juniper Web Filtering](#).]

Device Security

- **Security Services support (cSRX)**—Starting in Junos OS Release 23.4R1, Juniper Networks® cSRX Container Firewall (cSRX) supports the following security services for roaming and on-premises users:
 - Content Security (UTM)—Configure, monitor, and manage the Content Security features to secure the network from viruses, malware, or malicious attachments and protect the users from security threats.
 - Intrusion Detection and Prevention (IDP)—Monitor the events occurring in your network, and selectively enforce various attack detection and prevention techniques on the network traffic that passes through the cSRX instances.
 - Juniper Networks Deep Packet Inspection (JDPI)—For deep packet inspection and classification of applications and associated protocol attributes.

See [[Content Security User Guide](#) , [Intrusion Detection and Prevention User Guide](#) , and [Juniper Networks JDPI](#)].

Flow-based and Packet-based Processing

- **Support drop-flow to prevent security attack - (SRX Series Firewall, vSRX3.0, cSRX, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, we support a new feature drop-flow to prevent security attack. You can control and limit the number of max-session for the drop-flow. The

session in the drop-flow is valid for 4 seconds by default. During a drop-flow, the session state displays as Drop, but in the flow, the state remains as Valid.

The drop-flow feature is enabled by default. To disable the feature, use the `set security flow drop-flow max-sessions 0` command. To delete only the drop-flow feature, use the `run clear security flow session drop-flow` command.

To view the current drop-flow configuration, use the `show security flow drop-flow` command, and the view all the available drop-flow, use the `show security flow session drop-flow` command.

[See [Flow Based Session](#).]

Public Key Infrastructure (PKI)

- **Support for dynamic update of trusted CA bundle for SSL proxy (SRX Series, cSRX, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support dynamic update of default trusted CA certificates for SSL proxy. Earlier in Junos OS Release 23.2R1, we introduced dynamic update of default trusted CA certificates for Junos OS devices. In the current release, we've made the following enhancements:
 - The Juniper content delivery network (CDN) server (<http://signatures.juniper.net/cacert>) is up to date with the latest copy of trusted CA certificates.
 - The SSL proxy on your SRX Series Firewall uses the latest trusted CA certificate from the default trusted CA bundle downloaded to your device from the CDN server.

With this feature, we ensure authenticity, confidentiality, and integrity of SSL proxy-based communication.

[See [Configuring a Trusted CA Profile Group](#).]

VPNs

- **Certificate-based IPsec VPN tunnels (cSRX)**—Starting in Junos OS Release 23.4R1, the cSRX Container Firewall (cSRX) supports certificate-based IPsec tunnels to enable secure communications across a public WAN such as the Internet.

[See [IPsec VPN User Guide](#).]

What's Changed

IN THIS SECTION

- [Platform and Infrastructure](#) | 14

Learn about what changed in this release for cSRX.

Platform and Infrastructure

- On cSRX instances, the trust and the untrust zones are not created by default. You must configure the trust and the untrust security zones using Junos configurations if needed.
- Advanced Policy-Based Routing Policies (APBR) is not supported on cSRX instances. So, when you run the APBR related CLI commands such as `show security advance-policy-based-routing count`, then you will receive an error message as `error: Unrecognized command (network-security)`.

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

IN THIS SECTION

- [Platform and Infrastructure | 15](#)
- [VPNs | 15](#)

Learn about the issues fixed 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.

Platform and Infrastructure

- The Packet Forwarding Engine stopped in CSRX-L model due to kernel_heap memory is not allocated for ukern allocations. [PR1725126](#)

VPNs

- Traffic loss will be observed on cSRX in an IPsec scenario. [PR1735358](#)

Junos OS Release Notes for EX Series

IN THIS SECTION

- [What's New | 16](#)
- [What's Changed | 31](#)
- [Known Limitations | 33](#)
- [Open Issues | 34](#)

- [Resolved Issues | 37](#)
- [Migration, Upgrade, and Downgrade Instructions | 43](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 17](#)
- [Chassis | 18](#)
- [Dynamic Host Configuration Protocol | 18](#)
- [Ethernet Switching and Bridging | 19](#)
- [EVPN | 20](#)
- [Interfaces | 26](#)
- [Junos Telemetry Interface | 27](#)
- [Layer 2 Features | 28](#)
- [Network Management and Monitoring | 29](#)
- [MC-LAG | 29](#)
- [Routing Protocols | 30](#)
- [Additional Features | 30](#)

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

To view features supported on the EX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R1, click the Group by Release link. You can collapse and expand the list as needed.

- [EX2300](#)
- [EX2300-VC](#)
- [EX2300 Multigigabit](#)
- [EX3400](#)

- [EX3400-VC](#)
- [EX4100](#)
- [EX4100-F](#)
- [EX4300 Multigigabit](#)
- [EX4400](#)
- [EX4400 Multigigabit](#)
- [EX4400-24X](#)
- [EX4650-48Y](#)
- [EX9200](#)

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Support for VLAN group on EX series switches (EX Series)**—Starting in Junos OS Release 23.4R1, you can configure VLAN group on EX series switches. The 802.1X VLAN group maps a single WLAN to a single VLAN or multiple VLANs. In this feature, the VLAN group name is added within the Tunnel-Private-Group-ID (defined as RADIUS attribute type 81, RFC 2868) and sent in the RADIUS response instead of a regular VLAN ID or VLAN Name. It helps to reduce the number of broadcast domains and reduce the need for administrators to load balance your network.

To configure VLAN groups, you can use the `set vlans vlan-groups vlan_group_name vlan-id-list vlan-id-list` configuration statement at the `[edit vlans]` hierarchy level.

[See [Configuring VLAN Groups on EX Series Switches](#).]

- **Support for micro and macro segmentation with GBP using Mist Access Assurance (EX4100, EX4400, and EX4650)**—Starting in Junos OS Release 23.4R1, we support micro and macro segmentation in a VXLAN (Virtual extensible Local Area Network) architecture using Group Based Policy (GBP) through Juniper Mist Access Assurance. GBP tags are assigned dynamically to clients as part of RADIUS transaction by Mist Cloud NAC.

[See [802.1X for Switches Overview](#).]

- **Control device access privileges with exact match configuration (ACX5448, ACX5448-M, ACX5448-D, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP,**

EX4100-H-12P, EX4100-H-12P-DC, EX4100-H-24P, EX4100-H-24P-DC, EX4100-H-24F, EX4100-H-24F-DC, 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, EX9214, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, QFX10002-60C, QFX10002, QFX10008, and QFX10016)—Starting in Junos OS Release 23.4R1, you can configure access privileges for login classes by allowing or denying full hierarchy strings with the `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration options. The exact match configuration enables you to set separate permissions for set, delete, activate, or deactivate operators for any hierarchy.

The `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration options support full hierarchy strings as well as wildcard characters and regular expressions.

[See [Understanding Exact Match Access Privileges for Login Classes](#).]

Chassis

- **Platform resiliency support (EX-Series)** – Starting in Junos OS release version 23.4R1, platform resiliency support is provided for EX-Series devices with relevant and appropriate alarms, logs, SNMP management for fan, PEM, CPU, FPGA, PFE Storage, I2C controller, and external USB.

[See [High Availability User Guide](#).]

Dynamic Host Configuration Protocol

- **Support for Q-in-Q tunneling with L2 swap-push/pop-swap configuration and DHCP security (EX2300, EX4100, EX3400, EX4300-MP, EX4400, and EX4400-MP)**—Starting in Junos OS Release 23.4R1, you can configure Q-in-Q tunneling with L2 swap-push/pop-swap in which the customer VLAN (C-VLAN) tag is swapped with the `inner-vlan-id` tag, and the service-provider-defined service VLAN (S-VLAN) tag is pushed on it (for traffic flowing from customer to service provider site). For the traffic flowing from the service provider network to the customer network, we've removed the S-VLAN tag, and replaced the C-VLAN tag with the VLAN ID configured on the UNI logical interface. To support DHCP security along with Q-in-Q tunneling, you can configure the following DHCP security features:
 - DHCP snooping (DHCPv4 and DHCPv6)
 - Dynamic ARP inspection
 - Neighbor discovery inspection
 - IP source guard
 - DHCP option 82 and DHCPv6 option 37

[See [DHCP Security in Q-in-Q with Service Provider Configuration](#).]

Ethernet Switching and Bridging

- **Limit and track MAC address movement for all VLANs in a routing instance (EX2300, EX2300-MP, EX2300-C, EX3400, EX3400-VC, EX4100-24MP, EX4300-MP, EX4400-24P, EX4650, EX4650-48Y-VC, EX9204, EX9208, and EX9214)**-Starting in Junos OS Release 23.4R1, you can limit and track the number of times a MAC address moves to a new interface within a second by configuring MAC move limiting feature. If the MAC address movement exceeds the configured limit then an action can be configured, where the incoming packets can be ignored, dropped, logged, or can also be configured to shut down the interface.

If you configure MAC move limit and packet-action at the routing-instance level, then the configuration also applies to all the VLANs within that routing instance.

To configure MAC move limits at the default routing-instance level, use the following configuration:

```
user@host# set switch-options mac-move-limit limit packet-action action
```

To configure MAC move limits at a user-defined routing-instance level, use the following configuration:

```
user@host# set routing-instances routing-instance switch-options mac-move-limit limit packet-action action
```

If you configure MAC move limit at the VLAN level, then the VLAN's MAC move limit and its packet action takes precedence over the routing-instance's MAC move limit and packet-action. If a packet action is not configured at the VLAN level, then the VLAN uses the packet-action as None rather than inheriting the one configured at the routing-instance level.

If you do not want the VLAN to inherit the routing instance's MAC move limit properties and actions, then you need to disable MAC move limit at the VLAN level. This ensures the VLAN does not inherit the routing-instance's configured MAC move limits and all the MAC address movements will be ignored.

To disable MAC move limit for a VLAN in the default routing-instance level, use the following configuration:

```
user@host# set vlan vlan-name switch-options mac-move-limit none
```

To disable MAC move limit for a VLAN in a user-defined routing-instance level, use the following configuration:

```
user@host# set routing-instances routing-instance vlan vlan-name switch-options mac-move-limit none
```

You can track the MAC address movement limits applicable for each VLAN by using the following commands:

```
user@host> show vlans extensive
user@host> show vlans <vlan-name> extensive
```

EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 23.4R1, you can configure an Ethernet VPN–Virtual Extensible LAN (EVPN-VXLAN) fabric with an IPv6 underlay. You can use this feature only with MAC-VRF routing instances (all service types). You must configure either an IPv4 or an IPv6 underlay across the EVPN instances in the fabric; you can't mix IPv4 and IPv6 underlays in the same fabric.

To enable this feature, include these steps when you configure the EVPN underlay:

- Configure the underlay VXLAN tunnel endpoint (VTEP) source interface as an IPv6 address:

```
set routing-instances mac-vrf-instance-name vtep-source-interface lo0.0 inet6
```

- Configure a router ID in the routing instance as a 32-bit unsigned integer value in dotted quad decimal notation. You must configure this for BGP handshaking to work in the underlay even though the underlay uses the IPv6 address family.

```
set routing-instances mac-vrf-instance-name routing-options router-id router-ID
```

- Enable the Broadcom VXLAN flexible flow feature, which is required in Junos OS Release 21.2R2 where the feature is not enabled by default:

```
set forwarding-options vxlan-flexflow
```

We support the following EVPN-VXLAN features with an IPv6 underlay:

- EVPN Type 1, Type 2, Type 3, Type 4, and Type 5 routes. [See [EVPN Type-5 Route with VXLAN Encapsulation for EVPN-VXLAN](#).]
- Shared VTEP tunnels (required with MAC-VRF instances).

- All-active multihoming. [See [EVPN Multihoming Overview](#).]
- EVPN core isolation. [See [Understanding When to Disable EVPN-VXLAN Core Isolation](#).]
- Bridged overlays. [See [Bridged Overlay Design and Implementation](#).]
- Layer 3 gateway functions in edge-routed bridging (ERB) and centrally-routed bridging (CRB) overlays with IPv4 or IPv6 traffic.
- Underlay and overlay load balancing.

Layer 3 protocols over IRB interfaces—BFD, BGP, OSPF. [See [Supported Protocols on an IRB Interface in EVPN-VXLAN](#).]

- Data center interconnect (DCI)—over-the-top (OTT) full mesh only. [See [Over-the-Top Data Center Interconnect in an EVPN Network](#).]
- EVPN proxy ARP and ARP suppression, and proxy NDP and NDP suppression. [See [EVPN Proxy ARP and ARP Suppression, and Proxy NDP and NDP Suppression](#).]

[See [EVPN-VXLAN with an IPv6 Underlay](#).]

- **Backup liveness detection on EVPN dual homed peers (EX4100-48MP, EX4100-H-12P-DC, EX4100-H-24P, EX4100-H-24F-DC, 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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, and EX4650)**—Starting in Junos OS Release 23.4R1, we've added support for backup liveness detection for EVPN peers. This feature addresses a gap in the core isolation feature that halts traffic within a data center with two spine devices when the BGP session between those devices goes down. You can configure backup liveness detection to track the state of the adjacent peer in conjunction with core isolation to ensure that the links to one of the spine devices stay up even during a BGP session failure. This configuration allows traffic within the data center to continue.

[See [Backup Liveness Detection on EVPN Dual Homed Peers](#)]

- **Enhanced OISM with IGMPv2, IGMPv3, and IGMP snooping for IPv4 multicast traffic in EVPN-VXLAN fabrics (EX4100-24MP, EX4100-48MP, EX4100-24P, EX4100-48P, EX4100-24T, EX4100-48T, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, and EX4650)**—Starting in Junos OS Release 23.4R1, we support an enhanced optimized intersubnet multicast (OISM) model with IGMPv2, IGMPv3, and IGMP snooping for IPv4 multicast traffic in EVPN-VXLAN edge-routed bridging (ERB) overlay fabrics. With enhanced OISM, on each device, you have the option to configure only the revenue VLANs that device hosts. You don't need to configure all revenue VLANs in the fabric on all OISM leaf devices as you do with the regular OISM symmetric bridge domains model. This asymmetric bridge domains model enables OISM to scale well when your network has leaf devices that host a large number of different VLANs.

Enhanced OISM operates similarly to the OISM symmetric bridge domains model, but with differences to account for the asymmetric bridge domains model, such as the following:

- The source devices forward east-west multicast traffic:
 - On the source VLAN to multihoming peer leaf devices.
 - On the OISM supplemental bridge domain (SBD) for all other destinations (whether they host the source VLAN or not).
- For north-south multicast traffic from external sources and to external receivers:
 - The border leaf PIM EVPN gateway (PEG) devices exchange EVPN Type 10 Selective P-Multicast Service Interface (S-PMSI) Auto-Discovery (A-D) routes.
 - With the S-PMSI A-D routes, the PEG devices can reliably signal multicast (S,G) PIM registration to the external multicast rendezvous point (RP) only for sources within the fabric.
- You must configure:
 - The enhanced-oism option instead of the oism option (both options are at the [edit forwarding-options multicast-replication evpn irb] hierarchy level).
 - Matching revenue VLANs on any OISM leaf devices that are multihoming peer devices.

[See [Optimized Intersubnet Multicast in EVPN Networks.](#)]

- **Enhanced OISM with MLDv1, MLDv2, and MLD snooping for IPv6 multicast traffic in EVPN-VXLAN fabrics (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, and EX4650)**—Starting in Junos OS Release 23.4R1, we support the enhanced optimized intersubnet multicast (OISM) model with MLDv1, MLDv2, and MLD snooping for IPv6 multicast traffic in EVPN-VXLAN edge-routed bridging (ERB) overlay fabrics. Enhanced OISM uses an asymmetric bridge domains model that enables OISM to scale well when your network has leaf devices that host a large number of different VLANs.

[See [Optimized Intersubnet Multicast in EVPN Networks.](#)]

- **Support for static VXLAN with MC-LAG using service provider interface configuration (EX4650)**—Starting in Junos OS Release 23.4R1, you can use service provider style interface to configure static VXLAN in a spine-and-leaf network where the leaf devices support MC-LAG and Q-in-Q VLAN tunnels (VLAN translation). Junos OS supports Q-in-Q VLAN tunnels only when you use service provider interface configurations.

[See [Q-in-Q Tunneling in Leaf-Spine Network with Static VXLAN Tunnels.](#)]

- **Support for 802.1X assignment of GBP tags using the RADIUS server (EX4100, EX4400, and EX4650)** —Starting in Junos OS Release 23.4R1, we've added these enhancements to the group-based policy (GBP) micro segmentation feature:

- Support for a new VSA "Juniper-Group-Based-Policy-Id" to assign GBP tags dynamically from RADIUS.

- Support for these new CLI statements:

- `set protocols dot1x authenticator interface [interface-name] server-fail gbp-tag gbp-tag`

Specify the GBP tag to apply on the interface when the server is inaccessible.

- `set protocols dot1x authenticator interface [interface-name] server-reject-vlan gbp-tag gbp-tag`

Specify the GBP tag to apply when RADIUS rejects the client authentication.

- `set protocols dot1x authenticator interface [interface-name] guest-gbp-tag gbp-tag`

Specify the GBP tag to apply, when an interface is moved to a guest VLAN when no 802.1X supplicants are connected on the interface.

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

- **Range and list support for VLAN, port, and port+VLAN GBP filter matches (EX4100, EX4400, and EX4650)**—Starting in Junos OS Release 23.4R1, the EX4400, EX4100, and EX4650 switches support multiple entries in the VLAN, port, and port+VLAN type GBP filters of same type in a term. The EX4100 switches do not support the VLAN and port+VLAN GBP filter match options.

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

- **EVPN-VXLAN pure T5 host-route auto-generated community (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, EX4650, and MX960)**—Starting in Junos OS Release 23.4R1, we added support for EVPN-VXLAN pure T5 host-route auto-generated community. This feature adds a community to MAC-IP ARP/NDP based pure Type 5 host routes. Border leaf devices in ERB topologies with Type 5 connectivity to other leaf devices in the data center and Type 5 connections to external networks need to advertise aggregate routes to the external network instead of individual Type 5 routes. Border leaf devices can use this community to identify these routes and create an aggregate route to advertise to external EVPN networks.

[See [EVPN-VXLAN Pure T5 Host-Route Auto-Generated Community](#)]

- **Static configuration of MAC-IP bindings with EVPN-VXLAN (EX4100-24MP, EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX10004, MX10008, MX2010, and QFX10002-60C)**—Starting in Junos OS Release 23.4R1, we've added the functionality to allow static configuration of MAC-IP bindings on an interface, similar to configuring static MACs on an interface. This feature enables the static configuration of IP and MAC entries for crucial services provided by management and infrastructure hosts. It proves particularly advantageous in Internet Exchange Point (IXP) networks where participant Customer Edge routers (CEs) remain well-known and static, not transitioning to different Provider Edge (PE) devices.

You can now utilize a new feature that establishes a static link between an IP address and a MAC for a logical interface within a bridge domain or VLAN. When you provision a static MAC-IP entry on a PE, the PE will initiate a probe following an exponential backoff pattern. The probe will use an all-zero sender IP address on the associated interface. If the entity owning the IP to MAC entry responds to the probe, the system will learn the IP to MAC binding as static. Subsequently, it will be propagated to remote PEs through the BGP/EVPN Type 2 MAC advertisement route. The corresponding MAC will be recognized as a dynamic entry. If you want to deactivate the probing mechanism for learning the IP to MAC binding, you can do so by configuring a new configuration option [arp-nd-probe-disable]. Without probing, both the MAC and IP to MAC binding will be acquired from network traffic and communicated using EVPN.

We've introduced the following commands and configuration statements:

- Configuration of static IP to MAC bindings



NOTE: A maximum of 8 MACs can be configured per static IP address.

- QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface
interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn interface interface-name static-mac-ip ip-
address [MAC1 MAC2 ... MACn]
```

The aforementioned commands provide an option to configure router and override bits for IPV6 entries. For example:

QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
<router | override>
```

- Disable probing on configuration of static IP to MAC entries:

To turn off the default probing on configuration of static IP to MAC entries, you can use the global configuration statement `arp-nd-probe-disable`.

```
set protocols l2-learning arp-nd-probe-disable
```

- Enable logging for failed probing of static IP to MAC entries:

To turn on the logging, configure the global configuration statement `arp-nd-probe-failed-log`.

```
set protocols l2-learning arp-nd-probe-failed-log
```

- Enable GARP/unsolicited-NA for local and remote static entries

If this feature is required, you must configure the global configuration statement `garp-na-enable`.

```
set protocols l2-learning garp-na-enable
```

- Disable dynamic learning [all static provisioning]

If dynamic learning of MAC-IP entries is not required, configure the statement `drop-unknown-macip` under BD/VLAN.

- QFX:

```
set vlans vlan-name switch-options drop-unknown-macip
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options drop-unknown-macip
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn drop-unknown-macip
```

- Drop unicast ARP request

To drop unicast address resolution requests (for instance, NUD NS messages), you can configure the statement `block-unicast-arp` at global level for QFX and per BD level for MX.

- QFX:

```
set protocols l2-learning block-unicast-arp
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options block-unicast-arp
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn block-unicast-arp
```

[See [EVPN Proxy ARP and ARP Suppression](#), and [Proxy NDP and NDP Suppression](#) and [interface-mac-ip-limit](#).]

- **Access security support in EVPN-VXLAN overlay networks (EX4400-48T, and EX4650)**—Starting in Junos OS Release 23.4R1, we support access security features on switches that function as Layer 2

VXLAN gateways in an EVPN-VXLAN centrally-routed overlay network (two-layer IP fabric). We support the following features on Layer 2 server-facing interfaces that are associated with VXLAN-mapped VLANs:

- DHCPv4 and DHCPv6 snooping. [See [DHCP Snooping](#).]
- Dynamic ARP inspection (DAI). [See [Understanding and Using Dynamic ARP Inspection \(DAI\)](#).]
- Neighbor discovery inspection (NDI). [See [IPv6 Neighbor Discovery Inspection](#).]
- IPv4 and IPv6 source guard. [See [Understanding IP Source Guard for Port Security on Switches](#).]
- Router advertisement (RA) guard. [See [Understanding IPv6 Router Advertisement Guard](#).]

The access security features function the same and you configure them in the same way in an EVPN-VXLAN environment as you do in a non-EVPN-VXLAN environment. However, keep these differences in mind:

- We do not support these features on multihomed servers.

These features do not influence the VXLAN tunneling and encapsulation process.

- **Loop detection for EVPN-VXLAN fabrics (EX4100-48MP, EX4100-H-12P, EX4100-H-12P-DC, EX4100-H-24P, EX4100-H-24P-DC, EX4100-H-24F-DC, 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)**—Starting in Junos OS Release 23.4R1, you can configure loop detection on the server-facing Layer 2 interfaces of the leaf devices in an EVPN-VXLAN fabric. This feature can detect the following types of Ethernet loops:
 - A loop between two interfaces with different Ethernet segment identifiers (ESIs), usually caused if you miswire fabric components.
 - A loop between two interfaces with the same ESI, usually caused if you miswire a third-party switch to the fabric.

After you enable loop detection, the interfaces periodically send multicast loop-detection protocol data units (PDUs). If a loop detection-enabled interface receives a PDU, the device detects a loop, which triggers the configured action to break the loop. For example, if you configure the `interface-down` action, the device brings down the interface. After the `revert-interval` timer expires, the device reverts the action and brings the interface back up again.

[See [loop-detect \(EVPN\)](#).]

Interfaces

- **Support for port bounce (EX Series, MX Series, QFX Series, and PTX Series)**—Starting in Junos OS Release 23.4R1, you can shut down the interface for a given time by using the request `interface bounce interface_name interval seconds`. The interface goes up at the end of the configured time.

[See [request interface bounce](#).]

Junos Telemetry Interface

- **Native sensor support for 802.1x telemetry (EX2300-VC, EX3400-VC, EX4100-MP, EX4100, EX4300-MP, EX4400-MP, and EX4400)**—Starting in Junos OS Release 23.4R1, we support telemetry streaming of operational state data for the 802.1x protocol based on the native Junos data model `junos-state-dot1x.yang`.

[See [Junos YANG Data Model Explorer](#).]

- **802.1X configuration and operational state sensors using OpenConfig (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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and QFX10002-60C)**—Starting in Junos OS Release 23.4R1, we support configuration and telemetry streaming of operational state data based on the OpenConfig data model `openconfig-if-8021x.yang`.

[For state sensors, see [Junos YANG Data Model Explorer](#). For OpenConfig configuration, see [Mapping OpenConfig 802.1X Commands to Junos Configuration](#).]

- **Firewall filter OpenConfig configuration support (EX9204, EX9208, EX9214, MX204, MX240, MX480, MX960, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Junos OS Release 23.4R1 supports OpenConfig firewall filter (also known as access control list) configurations based on the OpenConfig data models `openconfig-acl.yang` (version 1.2.2) and `openconfig-network-instance.yang` (version 1.4.0).

[See [Mapping OpenConfig Firewall Filter Commands to Junos Configuration](#).]

- **VLAN telemetry support for VLAN group name (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, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 23.4R1, we now support the new leaf `vlan-group-name`. Use the sensor `/state/protocols/dot1x/interfaces/interface/authenticated-sessions/authenticated-session/<vlan-group-name>` in a subscription to stream this value from a Juniper device to a collector.

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **Per-group TCAM utilization telemetry, CLI, and syslog support (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, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)—Starting in Junos OS Release 23.4R1, we now support per-group TCAM utilization statistics. In network environments with high throughput and low latency, Packet Forwarding Engine errors, statistics, and status are critical. This feature provides per-group TCAM statistics and also triggers a system log when TCAM consumption reaches approximately 90% for a group.

To stream statistics to a collector, subscribe with the sensor `/junos/system/linecard/npu/memory/`. To specify groups to export, use the existing Junos configuration statement `set forwarding-options pfe-sensor npu-memory resource-list resource-list`. If you do not specify groups, the default action exports all active groups in the system.

You can use the Junos operational mode command `show pfe filter hw summary` to see group information, too.

[See [Junos YANG Data Model Explorer](#) for sensors and `show pfe filter hw summary` and `resource-list`].

- **New native data model supporting DHCP security (EX2300-VC, EX3400-VC, EX4100-48MP, EX4100-24MP, EX4100-48P, EX4100-48T, EX4100-24P, EX4100-24T, EX4100-F-12P, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 23.4R1, we support the new native data model `junos-state-dhcp-security`.

[For state sensors, see [Junos YANG Data Model Explorer](#).]

- **STP OpenConfig and operational state sensor support (ACX710, ACX5448, ACX5448-M, ACX5448-D, 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, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, we support OpenConfig STP configurations and sensors based on the OpenConfig data model `openconfig-spanning-tree` (Version 1, Revision 0.3.1).

[For OpenConfig configuration, see [Mapping OpenConfig STP Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

Layer 2 Features

- **Support for Q-in-Q tunneling with L2 swap-push/pop-swap configuration (EX2300, EX4100, EX4300, EX4300-MP, EX4400, EX4400-MP)**—Starting in Junos OS Release 23.4R1, you can configure Q-in-Q tunneling with L2 swap-push/pop-swap in which the customer VLAN (C-VLAN) tag is swapped with the inner-vlan-id tag, and the service-provider-defined service VLAN (S-VLAN) tag is pushed on it (for traffic flowing from customer to service provider site). For the traffic flowing from

the service provider network to the customer network, we've removed the S-VLAN tag, and replaced the C-VLAN tag with the VLAN ID configured on the UNI logical interface.

[See [Configuring Q-in-Q Tunneling and VLAN Q-in-Q Tunneling and VLAN Translation](#).]

- **Q-in-Q support on redundant trunk links using LAGs with link protection (EX4100-48MP and EX4400-48F)**—Starting in Junos OS Release 23.4R1, we now support Q-in-Q on redundant trunk links (also called “RTGs”) using LAGs with link protection. Redundant trunk links provide a simple solution for network recovery when a trunk port on a switch goes down. In this case, traffic is routed to another trunk port, keeping network convergence time to a minimum.

Q-in-Q support on redundant trunk links on a LAG with link protection also includes support for the following items:

- Configuration of flexible VLAN tagging on the same LAG that supports the redundant links configurations.
- Multiple redundant links configurations on one physical interface.
- Multicast convergence.

[See [Q-in-Q Support on Redundant Trunk Links Using LAGs with Link Protection](#).]

Network Management and Monitoring

- **Support for synchronizing the ephemeral configuration database on EX Series Virtual Chassis (EX2300-VC, EX4400-48F, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 23.4R1, NETCONF and Junos XML protocol client applications can synchronize the ephemeral configuration database across EX Series Virtual Chassis members.

[See [Understanding the Ephemeral Configuration Database](#).]

- **System logging support to capture the layer 2 error conditions on ports (EX-Series, MX-Series, and QFX-series)**—Starting in Junos OS Release 23.4R1, Junos OS generates system log messages for MAC Limiting, MAC Move Limiting, MAC learning, Storm control, and redundant trunk groups (RTGs) to record the error conditions on ports.

[See [Overview of System Logging](#).]

MC-LAG

- **Service Provider (SP) style configuration for MC-LAG (EX4650 switches)**—Starting in Junos OS Release 23.4R1, Service Provider (SP) style configuration for MC-LAG is available.

[See [Understanding Multichassis Link Aggregation Groups](#) and [show interfaces mc-ae](#).]

Routing Protocols

- Support for OSPFv2 HMAC SHA-1 keychain authentication and optimization for multi-active MD5 keys (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, MX204, MX240, MX304, MX480, MX960)—Starting in Junos OS Release 23.4R1, you can enable OSPFv2 HMAC-SHA1 authentication with keychain to authenticate packets reaching or originating from an OSPF interface. This feature ensures smooth transition from one key to another for OSPFv2 with enhanced security.

You can enable OSPFv2 to send packets authenticated with only the latest MD5 key after all the neighbors switch to the latest configured key. In Junos OS releases earlier than Release 23.4R1, we support advertising authenticated OSPF packets always with multiple active MD5 keys with a maximum limit of two keys per interface.

To enable OSPFv2 HMAC-SHA1 authentication, configure the authentication keychain *<keychain name>* option at the [edit protocols ospf area *area-id* interface *interface_name* hierarchy level. To enable optimization of multiple active MD5 keys, configure the delete-if-not-inuse option at the [edit protocols ospf area *area-id* interface *interface_name* authentication multi-active-md5] hierarchy level.

[See [Understanding OSPFv2 Authentication](#).]

Additional Features

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

- MAC limiting and MAC move limiting with EVPN-VXLAN (EX4650)
[See [Understanding MAC Limiting and MAC Move Limiting](#).]
- **MACsec with GRES** (EX2300, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4100-MP, EX4100, EX4300-MP, EX4400-MP, EX4400 and EX4650)
[See [Configuring Advanced MACsec Features](#).]
- **MLD snooping** (EX4650-48Y-VC)
[See [Understanding MLD Snooping](#).]
- Overlay and CE-IP ping and traceroute support for EVPN-VXLAN (EX9204 and EX9208).
[See [ping overlay](#), [traceroute overlay](#), [ping ce-ip](#), and [traceroute ce-ip](#).]
- **Support for forwarding-class policer action** (EX4100 and EX4400)
[See [then \(Policer Action\)](#).]

- **Support for MACsec VLAN tag in the clear support** (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48T, and MX304)

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

- **Support for physical interface policer** (EX4650)

[See [physical-interface-policer](#).]

- **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 HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- [EVPN | 31](#)
- [Junos XML API and Scripting | 32](#)
- [Network Management and Monitoring | 33](#)

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

EVPN

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature**—The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:
 - Peer PE device `peer-id` value can only be 1 or 2.
 - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback-subnet peer1-subnet` and `loopback peer2-subnet` options at the `edit services evpn device-attribute hierarchy` level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. The `loopback-subnet` option at the `edit services evpn device-attribute hierarchy` level has been deprecated.

- If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called `EXPORT-LOO` that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
- The commit script generates "notice" messages instead of "error" messages for configuration errors so you can better handle `edit services evpn` configuration issues.
- The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.

This feature also now includes a few new options so you have more flexibility to customize the generated configuration:

- `no-underlay-config` at the `edit services evpn` hierarchy level—To provide your own underlay peering configuration.
- `mtu overlay-mtu` and `mtu underlay-mtu` options at the `edit services evpn global-parameters` hierarchy level—To change the default assigned MTU size for underlay or overlay packets.

[See [Easy EVPN LAG Configuration](#).]

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement**—With the `EZ-LAG subnet-address inet` or `subnet-address inet6` options at the `edit services evpn evpn-vxlan irb irb-instance` hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ?`. Also, in the generated configuration for IRB interfaces, the commit script now includes default `router-advertisement` statements at the `edit protocols` hierarchy level for that IRB interface.

[See [subnet-address \(Easy EVPN LAG Configuration\)](#).]

Junos XML API and Scripting

- **Ability to commit extension-service file configuration when application file is unavailable**—When you set the `optional` option at the `edit system extension extension-service application file file-name` hierarchy level, the operating system can commit the configuration even if the file is not available at the `/var/db/scripts/jet` file path.

See [file \(JET\)](#).

- **XML output tags changed for request-commit-server-pause and request-commit-server-start (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the `request system commit server pause` command (`request-commit-server-pause` RPC) and the `request system commit server start` command (`request-commit-server-start` RPC). The root element is `<commit-server-operation>` instead of `<commit-server-information>`, and the `<output>` tag is renamed to `<message>`.

Network Management and Monitoring

- **NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.
[See [<copy-config>](#).]
- **ephemeral-db-support statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the ephemeral-db-support statement at the [edit protocols layer2-control] hierarchy level in the static configuration database.
[See [Enable and Configure Instances of the Ephemeral Configuration Database](#).]

Known Limitations

IN THIS SECTION

- [General Routing | 33](#)
- [Infrastructure | 34](#)

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

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

General Routing

- In EX2300, transit ARP requests entering a port can get trapped to the CPU even if no IRB is configured on the VLAN. This can result in unnecessary ARP requests to the CPU and in extreme cases result in drops of genuine ARP requests in the ARP queue to CPU. [PR1365642](#)
- This is a Broadcom limitation and Day 1 issue affecting broadcom chipsets such as EX4650's, EX4300. One VLAN can be mapped to only on ERPS ring. For example, VLAN 100 can be mapped to

only one ERPS ring. This same VLAN 100 cannot be part of another ERPS ring on the same switch.[PR1732885](#)

- [interface] [all] EX4400-48F :: JUNOS_REG: EX4400 : input-vlan-tagged-frames are not in the expected range while verifying Vlan Tagged Frames[PR1749391](#)

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. <https://kb.juniper.net/TSB18251>[PR1568757](#)

Open Issues

IN THIS SECTION

- [General Routing | 34](#)
- [Interfaces and Chassis | 35](#)
- [Layer 2 Ethernet Services | 36](#)
- [Platform and Infrastructure | 36](#)
- [Virtual Chassis | 36](#)

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](#)
- On EX4300-48MP platform, if POE is enabled, a master RE reconnect might be seen which could cause traffic impact. [PR1499771](#)

- On EX2300, EX3400, EX4300-48MP and EX4300, Pause frames counters does not get incremented when pause frames are sent. [PR1580560](#)
- On all EX platforms, whenever beacon LED functionality is enabled, there is a mismatch between the physical LED status and the output of the CLI command ?show chassis led? showing incorrect port LED status for interfaces as LED up instead of off. [PR1697678](#)
- On EX4650, the SFP-LX interface will not be UP when different Small Form-factor Pluggable(SFP-10GBASE-T and SFP-LX) are plugged in within the same 4 port group. The presence of the 10GE-T SFP resets the speed of the quad back to 10G even if the quad port speed is set to 1G. Normally 10G interface by itself will be up when set to 1G if no other SFP is plugged in. [PR1714833](#)
- On EX4400, a "BCM Error: API bcm_plp_mode_config_set" error msg may be seen in the syslog when converting a VCP to network port. There is no functionality impact. [PR1738410](#)
- Disable the vme interfaces or have the default route added properly from the shell script for the connectivity with the ztp server to work [PR1743222](#)
- EX-hardening: EX4400: set chassis config-button no-clear is not working [PR1758042](#)
- EX2300 VC: Dot1x authentication flapping in multiple supplicant mode with 100 user scale [PR1767706](#)
- On EX2300/EX3400 series with SFP-SX/LX interface is not coming up due to auto-negotiation failure. [PR1789617](#)

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the [edit forwarding-options family inet6] hierarchy level: [edit forwarding-options family inet6] route-accounting; By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the show interface statistics operational mode command. Can be found here: http://www.juniper.net/techpubs/en_US/junos10.4/topics/usage-guidelines/policy-configuring-ipv6-accounting.html [PR717316](#)

Layer 2 Ethernet Services

- If name-server information is changed via CLI after the DHCP subscribers are up, DNS obtained from DHCP server is overwritten by local config. This may result in DNS look up failures in some cases. [PR1743611](#)

Platform and Infrastructure

- On Junos OS EX4300 and EX4300-VC platforms, if zeroize or interface configuration deletion performed, PFEX process crash will be seen when interface/device comes up and there will be traffic loss during the PFE restart. [PR1714117](#)
- In a rare scenario, due to timing issues, the Packet Forwarding Engine (PFE) crash is observed on Junos EX4300 platforms. This causes traffic loss until the PFE comes up. [PR1720219](#)
- On EX4300-VC, the Online Insertion and Removal (OIR) of Quad Small Form-factor Pluggable (QSFP) may result in a PFE crash under near-zero idle CPU conditions. [PR1733339](#)
- On EX4300 VC setup, "qsfp_tk_read_mem_page: Rear QSFP+ PIC failed to select addr 127 err 1000" messages may be seen intermittently. There is no functionality impact for these error messages [PR1747126](#)
- On all EX4300 platforms, traffic is sent on an AE interface and sent to the removed child interface from AE (Aggregated Ethernet) where the traffic is lost. [PR1749406](#)

Virtual Chassis

- On EX4600-VC, when "request system reboot all members" is executed, post-reboot one of the VC member/Flexible PIC Concentrator(FPC) might disconnect and join the VC back due to Packet Forwarding Engine (PFE) restart. Traffic loss is seen when FPC is disconnected. [PR1700133](#)

Resolved Issues

IN THIS SECTION

- [EVPN | 37](#)
- [General Routing | 37](#)
- [Interfaces and Chassis | 41](#)
- [J-Web | 42](#)
- [Junos Fusion Satellite Software | 42](#)
- [Layer 2 Ethernet Services | 42](#)
- [Platform and Infrastructure | 42](#)
- [Routing Protocols | 42](#)
- [User Interface and Configuration | 43](#)

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

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

EVPN

- After deactivating/activating GBP configuration in the MH AE scenario all tag entries not getting re-learned on leaf nodes in the ethernet-switching table resulting in traffic loss. [PR1739878](#)

General Routing

- Unable to onboard the VC members after performing ZTP due to the phone-home process sending a blank in the device serial number field while connecting to the redirect server. [PR1687926](#)
- EX4400: pps counter does not show correct values for jubmo frames. [PR1700309](#)
- With MAC limit and persistent MAC learning configuration l2ald process will crash when MAC is learned through remote peers. [PR1706364](#)

- Mac entry not ageout in RTG in EX4600-VC after VCP port reconnect. [PR1707878](#)
- On EX4400, "show chassis environment power-supply-unit" displays only master member's details. [PR1709483](#)
- The interface remains up and LED is still green when the cable is removed. [PR1711695](#)
- The dcpfe process will crash due to memory fragmentation. [PR1711860](#)
- IGMP/MLD queries may get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. [PR1716902](#)
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario. [PR1719868](#)
- Port will be down when "no-auto-negotiation" is configured on EX4400-48F platform. [PR1720074](#)
- Invalid "Power Class" value will be observed. [PR1722674](#)
- The entPhysicalSoftwareRev MIB object returns Junos OS version value for components which do not run Junos OS. [PR1725078](#)
- Memory leak is observed on all Junos platforms during ZTP. [PR1726603](#)
- Root user is unable to login using public key authentication after reboot or upgrade. [PR1726621](#)
- On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time. [PR1727954](#)
- Traffic loss will be observed due to CRC errors with QSFP+-40G-ACU10M plugged. [PR1729067](#)
- EX4400: While exporting telemetry data, transceiver data is also streamed when there is no transceiver in device itself. [PR1729464](#)
- On EX4400, PIC2 details may not be displayed for "show snmp mib walk entPhysicalVendorType" output. [PR1731146](#)
- Filter term dropping VRRP traffic when "then log" is configured. [PR1732271](#)
- The ppmdd proces crashes will be seen in EX-VC scenario. [PR1733134](#)
- Error logs are seen with a non-vxlan dot1x enabled port. [PR1733365](#)
- On EX2300-VC when VCP interfaces are disabled/enabled then tvp_status_led_set error messages are seen. [PR1733636](#)
- EX4300-48MP: Device did not come up with USB image when "request system reboot usb" is issued. [PR1734925](#)

- Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario. [PR1735685](#)
- Port LEDs are not working as expected when the mode is changed from default to EN. [PR1735786](#)
- EX4400 shaping rate not working as expected. [PR1736790](#)
- Junos OS: EX Series: A PHP vulnerability in J-Web allows an unauthenticated attacker to control important environment variables (CVE-2023-36844). [PR1736937](#)
- On EX4400, request system halt/power-off doesn't turn off FAN LED's. [PR1737500](#)
- VC on EX3400 platforms will not form with 40GBASE-BXSR optics. [PR1737524](#)
- The 'input-vlan-map push' operation will not work on double-tagged frames. [PR1738384](#)
- VC case not handled properly while calling `brcm_vxlan_port_discard_set` api. [PR1738404](#)
- On certain EX platforms when 25G DAC in 4x25G is plugged into PIC port does not come up when used as VC. [PR1738535](#)
- DHCP offer is dropped at MX and specific EX platforms when an It interface is used as the transport. [PR1738548](#)
- In EVPN-VXLAN scenario DHCP does not work for clients connected on the dot1x port. [PR1739730](#)
- Layer 2 traffic will be dropped on VSTP disabled interface. [PR1739975](#)
- EX4400 VC : Both mge and ge interfaces are getting created for all ports during master member-id and role swap with Linecard. [PR1740024](#)
- The interface speed is not updated during reboot on Junos EX platforms. [PR1740064](#)
- On EX4400-48F, After phc commit in VC, default storm control config has extra xe port config for 0-11 ports and extra ge port config for 37-48 ports. This has no functionality impact. [PR1740579](#)
- On EX4400 with pre existing configuration of 1g for the uplink interfaces, it might not come up after 4x10G module insertion event. [PR1741724](#)
- DOT1XD_USR_ATHNTICTD_GST_VLAN is not triggered. [PR1741867](#)
- Basic VLAN configuration on EX2300-24MP / EX2300-48MP / EX4400-24MP / EX4400-48MP is missing from factory default configuration. [PR1742114](#)
- Race condition where FLOOD ROUTE DEL event can cause I2ald crash. [PR1742613](#)
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. [PR1742763](#)

- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration. [PR1743282](#)
- EX Series: Removal of notice about the availability of new POE firmware and the prompt to upgrade the same. [PR1743547](#)
- On EX2300/EX3400, unexpected error message during oam boot. [PR1744141](#)
- On EX4100, VC formation will not happen automatically after zeroize. [PR1744190](#)
- Enhancement of PoE Controller Firmware upgrade procedure. [PR1744343](#)
- Enhancement of PoE controller firmware files into Junos Software. [PR1745088](#)
- VLAN traffic received over VTEP is being dropped. [PR1746998](#)
- LLDP will not work on HGoE VC mode with 40G VCP connections. [PR1747095](#)
- PoE ports stop working after the reboot. [PR1747128](#)
- Soft OIR of the link connected to 10GBASE-T SFP will not update the link state at the other end. [PR1747277](#)
- Connectivity fails intermittently on 802.1x enabled ports. [PR1749312](#)
- The Mixed PEM alarm should be generated against the corresponding Member on Junos EX4100 platforms. [PR1750158](#)
- The PFE process crashed while removing and applying the firewall filters. [PR1750828](#)
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on L2 ports. [PR1751700](#)
- POE Log "Thread 22 (PoE Periodic) ran for ms without yielding" may be seen. [PR1751868](#)
- L2ALD_IFBD_COUNT_EXCEED is not generated when exceeded max number of vmember. [PR1752756](#)
- Runt frames generate excessive traffic statistics on EX4100/EX4400 platforms. [PR1753576](#)
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN. [PR1754474](#)
- QFX: VC(virtual chassis) doesn't get formed when using 100G for vc port. [PR1754838](#)
- The transceiver fails to get detected after the system reboot. [PR1754931](#)
- The interface stats interrupt may be lost resulting in stats not getting updated. [PR1755161](#)
- Ports remain down on backup member switch of VC on certain EX4400 platforms after power outage in a rare scenario. [PR1755433](#)

- The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols. [PR1757329](#)
- Whenever IGMP leave request is initiated by receiver unicast traffic to the host IP on the switch port is non-responsive. [PR1757431](#)
- The ksyncd and vmcore core will be seen on backup RE when GRES is configured. [PR1757692](#)
- macsec license get cleared on master member post nssu/reboot. [PR1757835](#)
- EX4400:PSM is not detected in "show chassis hardware" until AC feed is connected to it. [PR1759351](#)
- The configuration was not applied correctly to set the transmit-rate to the same speed as the interface speed. [PR1759821](#)
- The fxpc process might crash and cause traffic loss when adding and deleting irb configuration. [PR1760229](#)
- The 'input-vlan-map push' operation will not work on double-tagged frames. [PR1761220](#)
- SNMP Insertion trap not seen while fan removal and insertion. [PR1762096](#)
- Telemetry data of subscription path of /junos/system/linecard/npu/memory/ for IPV6 LPM less than 64 allocated values are exported as IPV6 LPM greater than 128 sometimes. [PR1762535](#)
- LLDP neighborship will not be formed on all Junos devices. [PR1763053](#)
- VPLAG information not installed correctly in hardware results in traffic flooding. [PR1763116](#)
- LLDP neighborship is not forming in non-master members. [PR1764085](#)
- Memory leak is observed when dot1x authentication is used. [PR1766314](#)
- A warning message is seen while installing a license key with an unknown feature. [PR1766515](#)

Interfaces and Chassis

- DCD crash can be seen sometimes while pushing config using API. [PR1742124](#)
- Services using the management interface will be affected on all Junos platforms. [PR1757936](#)

J-Web

- Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845). [PR1736942](#)

Junos Fusion Satellite Software

- Junos Fusion Satellite device will be stuck in the SyncWait state. [PR1733558](#)

Layer 2 Ethernet Services

- Auto-image-upgrade knob is not present when EX-VC is zeroized and VC is formed. [PR1694952](#)
- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). [PR1722082](#)
- Address allocation for DHCP client will fail if 'force-discover' configuration is enabled on client. [PR1742696](#)
- Name-server resolution failure may be seen intermittently after zeroize or loading factory default config resulting in MIST on-boarding failure. [PR1747800](#)

Platform and Infrastructure

- CPU utilization increases and stays high due to pfex_junos process. [PR1640045](#)
- VRRP peers delay to sync when 'mac-move-limit' is configured on EX switch. [PR1725042](#)

Routing Protocols

- OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers. [PR1737978](#)
- BFD session for BGP remains down in a specific scenario. [PR1738074](#)
- Memory leak observed when reconfiguring the flow routes. [PR1742147](#)

- BGP multipath route is not correctly applied after changing the IGP metric. [PR1754935](#)

User Interface and Configuration

- After the device reboot BGP sessions configured with authentication will be down. [PR1726731](#)
- The mgd process crash is observed when 'show' is executed from the configuration mode. [PR1745565](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 43

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.

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

Table 2: EOL and EEOL Releases

Release Type	End of Engineering (EOE)	End of Support (EOS)	Upgrade/ Downgrade to subsequent 3 releases	Upgrade/ Downgrade to subsequent 2 EEOL releases
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 | 45](#)
- [What's Changed | 45](#)
- [Known Limitations | 45](#)
- [Open Issues | 46](#)
- [Resolved Issues | 46](#)



NOTE: Junos OS Release 23.4R1 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
JRR200	JRR200-AC	Junos OS Release 23.4R1
JRR200	JRR200-CHAS	Junos OS Release 23.4R1
JRR200	JRR200-DC	Junos OS Release 23.4R1

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

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

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

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 47](#)

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.



NOTE: Junos OS Release 23.4R1 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
JRR200	JRR200-AC	Junos OS Release 23.4R1

(Continued)

Product Line	SKUs	Junos OS Release
JRR200	JRR200-CHAS	Junos OS Release 23.4R1
JRR200	JRR200-DC	Junos OS Release 23.4R1

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.

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

Table 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 Juniper Secure Connect

IN THIS SECTION

- [What's New | 48](#)
- [What's Changed | 49](#)
- [Known Limitations | 49](#)
- [Open Issues | 49](#)
- [Resolved Issues | 49](#)

What's New

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

What's Changed

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

Known Limitations

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

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

Open Issues

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

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

Resolved Issues

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

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

Junos OS Release Notes for MX Series

IN THIS SECTION

● [What's New | 50](#)

● [What's Changed | 82](#)

- [Known Limitations | 85](#)
- [Open Issues | 86](#)
- [Resolved Issues | 92](#)
- [Migration, Upgrade, and Downgrade Instructions | 110](#)

What's New

IN THIS SECTION

- [Hardware | 51](#)
- [Authentication and Access Control | 51](#)
- [Chassis | 52](#)
- [Class of Service | 52](#)
- [EVPN | 52](#)
- [High Availability | 55](#)
- [Interfaces | 56](#)
- [IPv6 | 56](#)
- [Juniper Extension Toolkit \(JET\) | 58](#)
- [Junos Telemetry Interface | 58](#)
- [MPLS | 65](#)
- [Multicast | 70](#)
- [Network Address Translation \(NAT\) | 71](#)
- [Network Management and Monitoring | 72](#)
- [Platform and Infrastructure | 72](#)
- [Precision Time Protocol \(PTP\) | 74](#)
- [Routing Options | 74](#)
- [Routing Protocols | 74](#)
- [Public Key Infrastructure \(PKI\) | 76](#)
- [Services Applications | 76](#)
- [Software Defined Networking \(SDN\) | 76](#)

- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 76](#)
- [Subscriber Management and Services | 78](#)
- [System Logging | 80](#)
- [VPNs | 80](#)
- [Additional Features | 81](#)

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

Hardware

- **New AC PSU and Active Blank for MX Series Routers**—Starting in Junos OS Release 23.4R1, we introduce a new AC Power Supply Unit or PSU (JNP10K-PWR-AC3), and active blank (JNP10K-PWR-BLN3) for MX10004 and MX10008 routers.

The new JNP10K-PWR-AC3 power supply is a high capacity model that is designed to support AC systems in a 15-A and 20-A mode.

The JNP10K-PWR-BLN3 active blank, as part of the power supply, helps in airflow and cooling in the MX router.

[See [MX10004 Power System](#) and [MX10008 Power System](#).]

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Control device access privileges with exact match configuration (ACX5448, ACX5448-M, ACX5448-D, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-H-12P, EX4100-H-12P-DC, EX4100-H-24P, EX4100-H-24P-DC, EX4100-H-24F, EX4100-H-24F-DC, 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, EX9214, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, QFX10002-60C, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, you can configure access privileges for login classes by allowing or denying full hierarchy strings with the `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration

options. The exact match configuration enables you to set separate permissions for set, delete, activate, or deactivate operators for any hierarchy.

The `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration options support full hierarchy strings as well as wildcard characters and regular expressions.

[See [Understanding Exact Match Access Privileges for Login Classes.](#)]

Chassis

- **Source Redundancy and Feed Redundancy support on MX10004 and MX10008** – Starting in Junos OS Release 23.4R1, N+1 power redundancy is supported on MX10004 and MX10008 routers with JNP10K-PWR-AC3 power supply modules (PSMs). You can enable either source redundancy or feed redundancy for the PSM.

[See [Managing Power.](#)]

- **Resiliency support (MX10004 and MX10008)** – Starting in Junos OS Release 23.4R1, the FRU resiliency support is provided on the MX10004 and MX10008 platforms with JNP10K-PWR-AC3 PSMs.

[See [Fabric Resiliency.](#)]

Class of Service

- **Replicate mode support for PWHT All-Active Mode (MX240, MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, we support replicate mode for pseudowire headend termination (PWHT) configurations in all-active mode. You use existing CoS interface commands to set the redundant logical tunnel (RLT) interface to replicate mode. This ensures accurate QoS in your PWHT all-active configuration.

[See [member-link-scheduler](#), [Configuring Hierarchical Schedulers for COS](#), and [Configuring PWHT Active-Active Mode with Targeting.](#)]

EVPN

- **Support for EVPN route advertisements in EVPN-MPLS Inter-AS Option-C networks (MX204, MX304, MX960, MX10004, MX10008, and MX2020)**—Starting in Junos OS Release 23.4R1, we have added support for EVPN route advertisements through an Inter-AS Option-C network. Configure the `inet` or `inet6` statement at the `[edit routing-options forwarding-table chained-composite-next-hop ingress labeled-bgp]` hierarchy to enable a label-switched path (LSP) from ingress PE to egress PE.
[See [labeled-bgp.](#)]
- **EVPN-VXLAN pure T5 host-route auto-generated community (EX4100-24T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-48F, EX4400-48MP, EX4650, and MX960)**—Starting in Junos OS Release 23.4R1, we added support for EVPN-VXLAN pure T5 host-route auto-generated community. This feature adds a community to MAC-IP ARP/NDP based pure Type 5 host routes.

Border leaf devices in ERB topologies with Type 5 connectivity to other leaf devices in the data center and Type 5 connections to external networks need to advertise aggregate routes to the external network instead of individual Type 5 routes. Border leaf devices can use this community to identify these routes and create an aggregate route to advertise to external EVPN networks.

[See [EVPN-VXLAN Pure T5 Host-Route Auto-Generated Community](#)]

- **EVPN E-LAN over SRv6 underlay (MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, and MX10008)**—EVPN E-LAN is a framework for delivering multipoint-to-multipoint VPN service with the EVPN signaling mechanisms. E-LAN service allows service providers to offer services that manage the L2 learning very efficiently. Starting in Junos OS Release 23.4R1, you can configure all-active multi-homed EVPN-ELAN service using segment routing over IPv6 (SRv6). To provide SRv6 service, the egress PE signals an SRv6 Service SID with the VPN route. The ingress PE encapsulates the Service SID in the VPN packet in an outer IPv6 header where the destination address is the SRv6 SID advertised by the egress PE and is routable in the underlay. The nodes between the PEs only need to support plain IPv6 forwarding. We support SRv6 micro-SID & Segment Routing Header (SRH) based control planes and forwarding. Different endpoint behaviors are defined for SRv6 services on the egress node.

[See [Configuring EVPN E-LAN over SRv6](#) .]

- **Static configuration of MAC-IP bindings with EVPN-VXLAN (EX4100-24MP, EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX10004, MX10008, MX2010, and QFX10002-60C)**—Starting in Junos OS Release 23.4R1, we've added the functionality to allow static configuration of MAC-IP bindings on an interface, similar to configuring static MACs on an interface. This feature enables the static configuration of IP and MAC entries for crucial services provided by management and infrastructure hosts. It proves particularly advantageous in Internet Exchange Point (IXP) networks where participant Customer Edge routers (CEs) remain well-known and static, not transitioning to different Provider Edge (PE) devices.

You can now utilize a new feature that establishes a static link between an IP address and a MAC for a logical interface within a bridge domain or VLAN. When you provision a static MAC-IP entry on a PE, the PE will initiate a probe following an exponential backoff pattern. The probe will use an all-zero sender IP address on the associated interface. If the entity owning the IP to MAC entry responds to the probe, the system will learn the IP to MAC binding as static. Subsequently, it will be propagated to remote PEs through the BGP/EVPN Type 2 MAC advertisement route. The corresponding MAC will be recognized as a dynamic entry. If you want to deactivate the probing mechanism for learning the IP to MAC binding, you can do so by configuring a new configuration option [arp-nd-probe-disable]. Without probing, both the MAC and IP to MAC binding will be acquired from network traffic and communicated using EVPN.

We've introduced the following commands and configuration statements:

- Configuration of static IP to MAC bindings



NOTE: A maximum of 8 MACs can be configured per static IP address.

- QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface
interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn interface interface-name static-mac-ip ip-
address [MAC1 MAC2 ... MACn]
```

The aforementioned commands provide an option to configure router and override bits for IPV6 entries. For example:

QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
<router | override>
```

- Disable probing on configuration of static IP to MAC entries:

To turn off the default probing on configuration of static IP to MAC entries, you can use the global configuration statement `arp-nd-probe-disable`.

```
set protocols l2-learning arp-nd-probe-disable
```

- Enable logging for failed probing of static IP to MAC entries:

To turn on the logging, configure the global configuration statement `arp-nd-probe-failed-log`.

```
set protocols l2-learning arp-nd-probe-failed-log
```

- Enable GARP/unsolicited-NA for local and remote static entries

If this feature is required, you must configure the global configuration statement `garp-na-enable`.

```
set protocols l2-learning garp-na-enable
```

- Disable dynamic learning [all static provisioning]

If dynamic learning of MAC-IP entries is not required, configure the statement `drop-unknown-macip` under BD/VLAN.

- QFX:

```
set vlans vlan-name switch-options drop-unknown-macip
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options drop-unknown-macip
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn drop-unknown-macip
```

- Drop unicast ARP request

To drop unicast address resolution requests (for instance, NUD NS messages), you can configure the statement `block-unicast-arp` at global level for QFX and per BD level for MX.

- QFX:

```
set protocols l2-learning block-unicast-arp
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options block-unicast-arp
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn block-unicast-arp
```

[See [EVPN Proxy ARP and ARP Suppression](#), and [Proxy NDP and NDP Suppression](#) and [interface-mac-ip-limit](#).]

High Availability

- **Multihop BFD support in inline mode (MX304, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, multihop BFD sessions will operate using inline mode by default instead of distributed mode. Inline mode allows for a higher number of programmable RPD (PRPD) programmed multihop BFD sessions. We support multihop sessions only in inline mode when you configure enhanced IP mode.

You can globally disable multihop BFD using inline mode with the `set protocols bfd mhop-inline-disable` configuration statement.

To disable multihop BFD using inline mode on a per BFD session basis, use the `set protocols bgp group group bfd-liveness-detection inline-disable` configuration statement.

[See [Understanding How BFD Detects Network Failures](#).]

- **BFD Session Dampening for LACP Interfaces (MX240, MX480, MX960, MX10003)**—Starting in Junos OS Release 23.4R1, you can use BFD session damping on LACP interfaces to suppress BFD session state change notifications for a configured time period when thresholds for session flapping are exceeded. Session damping helps reduce potential instability from excessive BFD notifications.

Use the `set bfd-liveness-detection damping` configuration statement at the `[edit dynamic-profiles name interfaces name aggregated-ether-option]` hierarchy level to configure BFD session damping.

[See [BFD Session Damping Overview](#).]

- **Support for running unified ISSU on MPC10 line cards on MX240, MX480, and MX960 routers**—Starting in Junos OS Release 23.4R1, we support in-service software upgrade (ISSU) for subscriber services functionality on MPC10 line cards on MX240, MX480, and MX960.

[See [request system software in-service-upgrade](#) and [Unified ISSU System Requirements](#)]

- **Configure BFD size to support large packets on AFT-enabled devices (MX304, MX10003, MX10004, MX10008, MX10016, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, on AFT-enabled devices, you can adjust the size of the BFD protocol data units (PDUs) with the `pdu-size` configuration statement at the `[edit protocols ospf area area interface interface bfd-liveness-detection]` hierarchy level. You can configure the BFD PDU size from the default of 24 bytes up to a maximum of 9000 bytes.

[See [Understanding How BFD Detects Network Failures](#).]

Interfaces

- **Support for port bounce (EX Series, MX Series, QFX Series, and PTX Series)**—Starting in Junos OS Release 23.4R1, you can shut down the interface for a given time by using the `request interface bounce interface_name interval seconds`. The interface goes up at the end of the configured time.

[See [request interface bounce](#).]

IPv6

- **SRv6 TE micro SID support for transport and L3VPN (MX10004, MX10008, MX10016)**—Starting in Junos OS Release 23.4 R1, we extend the micro segment Identifier (uSID) support for SRv6 traffic engineering (TE). We support SR TE micro SID only with default block configurations across the whole network domain or if any block configs are present, then that config must be same throughout the whole network. The Packet Forwarding Engine supports bit shifting operation for both `<block>:<uN>:<uA>` and `<block>:<uA>` routes. You must configure the full SID, the way it is advertised in IS-IS IGP, that is `<block>:<uN>` or `<block>:<uN>:<uA>`.

We've introduced the following configuration statements:

- `micro-srv6-sid` statement under `protocols source-packet-routing segment-list <name> <hop-name>` hierarchy to configure micro-SID in SRTE SRv6 segment-list.

- `strict-adjacency` statement under `protocols source-packet-routing segment-list <name> <hop-name>` hierarchy to strictly follow the micro adjacency SID

You can configure the segment-list containing micro-SIDs with the existing SRv6 configuration statement like the traditional SRv6 configuration. The only difference between the traditional and micro-SID configuration is that in traditional SRv6 TE segment-list configuration, you must use the configuration statement `srv6-sid`. However, for micro-SID configuration, you must use the new configuration statement `micro-srv6-sid`.

[See [How to Enable SRv6 Network Programming in IS-IS Networks](#) and [micro-sid](#).]

- **Operations, Administration, and Maintenance (OAM) ping and traceroute support for SRv6 uSID (MX10004, MX10008, MX10016)**—Starting in Junos OS Release 23.4R1, we support pinging an SRv6 micro segment Identifier (uSID) to verify that the uSID is reachable and is locally programmed at the target node. We also support tracerouting to an SRv6 uSID for hop-by-hop fault localization as well as path tracing to a uSID.

As part of this feature, we support SRv6 uSID ping and traceroute for the following configurations:

- SRv6 IS-IS ping and traceroute for End behavior with NEXT-CSID (uN)/uN+End.X behavior with NEXT-CSID (uA)/uN+End.DT behavior with NEXT-CSID (uDT) SIDs.
- SRv6 IS-IS ping and traceroute for compressed SID (compressed SID to be provided by user) for uN/uA/uDT.
- SRv6 uSID-stack ping and traceroute for uN/uN+uA/nN+uDT SIDs.

We've introduced the following commands:

- `ping srv6 spring-te micro-sids-stack nexthop-address <nh-addr> nexthop-interface <if-name> usids [usid1 usid2 ...]`
- `traceroute srv6 spring-te micro-sids-stack nexthop-address <nh-addr> nexthop-interface <if-name> usids [usid1 usid2 ...]`
- `traceroute srv6 spring-te micro-sids-stack nexthop-address <nh-addr> nexthop-interface <if-name> usids [usid1 usid2 ...] probe-icmp`

[See [How to Enable SRv6 Network Programming in IS-IS Networks](#) and [micro-sid](#).]

- **Optimizing ARP, NDP and Default-Route handling in internal DB of DCD (MX480)**—Starting in Junos OS 23.4R1, DCD only deletes routing entries for addresses that are completely unlinked from all associated addresses. Additionally, we introduce checks to prevent configuring multiple static MAC addresses for a single ARP and NDP address, which helps improve system stability and avoid potential conflicts in network configurations.

Juniper Extension Toolkit (JET)

- **BGP routes can inherit flexible tunnel encapsulation information from associated static routes (MX10003)**—In some configurations, static routes resolve over flexible tunnels. Starting in Junos OS Release 23.4R1, BGP can inherit the encapsulation information for the flexible route from the associated static route. The device can then use the static route's indirect next hop to encapsulate traffic in the flexible tunnel without intermediate steps. This streamlines your network configuration.

To enable this feature, configure the `preserve-nexthop-hierarchy` option at the `[edit routing-instances routing-instance-name routing-options resolution rib routing-instance.inet.0]` hierarchy level.

To view the details of the ultimate next hop, use the `show route extensive route expanded-nh` command.

[See [rib \(Route Resolution\)](#) and [Configuring Recursive Resolution over BGP Multipath](#).]

Junos Telemetry Interface

- **Forwarding Information Base (FIB) sensor support (MX240, MX960, and MX2020)**—Starting in Junos OS Release 23.4R1, we support OpenConfig-Abstract Forwarding Table (oc-aft) model and forwarding information base (FIB), also known as forwarding table, to stream enhanced routing statistics. To deliver statistics to a collector, you add sensors to a subscription and also include the statement `set routing-options forwarding-table oc-tlv-support` at the `[edit]` hierarchy level to enable statistics collection. The Junos routing protocol process (rpd) sends the origin-protocol and origin-network-instance of a route, as well as the next-hop via an opaque type, length, and value (TLV) to the collector. Include the following sensors in your subscription:

- Next-hops:
 - `/network-instances/network-instance/afts/next-hops/next-hop/state/pop-top-label`
 - `/network-instances/network-instance/afts/next-hops/next-hop/state/vni-label`
 - `/network-instances/network-instance/afts/next-hops/next-hop/state/vni-label`
 - `/network-instances/network-instance/afts/next-hops/next-hop/ip-in-ip/state/dest-ip`
- State-synced:
 - `/network-instances/network-instance/afts/state-synced/state/ipv4-unicast`
 - `/network-instances/network-instance/afts/state-synced/state/ipv6-unicast`
- IPv4 and IPv6 unicast:
 - `/network-instances/network-instance/afts/ipv4-unicast/ipv4-entry/state/origin-network-instance`
 - `/network-instances/network-instance/afts/ipv6-unicast/ipv6-entry/state/origin-network-instance`

[For statement support, see [routing-options forwarding-table oc-tlv-support](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **IS-IS OpenConfig and operational state sensor support (ACX5448, ACX710, MX204, MX240, MX480, MX960, MX10003, MX10008, MX10016, and MX2008)**—Starting in Junos OS Release 23.4R1, we support OpenConfig ISIS configurations and sensors based on the OpenConfig data model `openconfig-isis.yang` (version 1.0.0). This feature closes some gaps in our OpenConfig configuration and sensor support in the IS-IS area.

[For OpenConfig configuration, see [Mapping OpenConfig ISIS Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **MPLS OpenConfig and operational state sensor support (MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we support OpenConfig MPLS configurations and sensors based on OpenConfig data models `openconfig-mpls.yang` (version 3.2.2), `openconfig-mpls-types.yang` (version 3.2.1), and `openconfig-mpls-te.yang` (version 3.2.2). We support the following OpenConfig configurations and state sensors.

- Configurations:
 - MPLS global TTL propagation (`/network-instances/network-instance/mpls/global/config/ttl-propagation`)
 - MPLS LSP PRI/SEC path-metric-bound-constraint (`/network-instances/network-instance/mpls/lsp/constrained-path/tunnels/tunnel/p2p-tunnel-attributes/p2p-primary-path/p2p-primary-path/path-metric-bound-constraints/path-metric-bound-constraint/config/`)
- Sensors:
 - MPLS global (`/network-instances/network-instance/mpls/global/state/`)
 - MPLS global interface-attributes (`/network-instances/network-instance/mpls/global/interface-attributes/`)
 - MPLS LSP autobandwidth (`/network-instances/network-instance/mpls/lsp/constrained-path/tunnels/tunnel/bandwidth/auto-bandwidth/state/`)
 - MPLS LSP PRI/SEC path-metric-bound-constraint (`/network-instances/network-instance/mpls/lsp/constrained-path/tunnels/tunnel/p2p-tunnel-attributes/p2p-primary-path/p2p-primary-path/path-metric-bound-constraints/path-metric-bound-constraint/state/`)
 - MPLS traffic engineering global attributes SRLG (`/network-instances/network-instance/mpls/te-global-attributes/srlgs/srlg/static-srlg-members/members-list/state/`)

[For OpenConfig configuration, see [Mapping MPLS OpenConfig MPLS Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **MPLS OpenConfig and operational state sensor support (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we support OpenConfig MPLS configurations and sensors based on the OpenConfig data models `openconfig-mpls-ldp.yang` (version 3.2.0) and `openconfig-mpls-rsvp.yang` (version 4.0.0). This feature closes some gaps in our OpenConfig configuration and sensor support in the MPLS RSVP-TE and MPLS LDP areas.

[For OpenConfig configuration, see [Mapping MPLS OpenConfig MPLS Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **Telemetry streaming of operational state data for syslog messages (ACX5448, ACX710, MX240, MX480, MX960, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, we support telemetry streaming of operational state data for syslog messages to an external gRPC Network Management Interface (gNMI) collector. Sensors are based on the native Junos data model under the hierarchy level `/state/system/syslog/messages`. You can stream data using `ON_CHANGE` and `TARGET_DEFINED` modes.

[See [Junos YANG Data Model Explorer](#).]

- **Segment Routing Traffic Engineering (SR-TE) Policy telemetry (MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we've introduced support for telemetry streaming of operational state data for segment routing traffic engineering (SR-TE) policy. State sensors are based on OpenConfig data model `openconfig-srte-policy.yang`. You can subscribe to SR-TE sensors using resource path `/network-instances/network-instance/segment-routing/te-policies`.

[See [Junos YANG Data Model Explorer](#).]

- **802.1X configuration and operational state sensors using OpenConfig (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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and QFX10002-60C)**—Starting in Junos OS Release 23.4R1, we support configuration and telemetry streaming of operational state data based on the OpenConfig data model `openconfig-if-8021x.yang`.

[For state sensors, see [Junos YANG Data Model Explorer](#). For OpenConfig configuration, see [Mapping OpenConfig 802.1X Commands to Junos Configuration](#).]

- **Telemetry support for QoS queue statistics on pseudowire interface sets (MX240, MX304, MX480, MX960, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020 with Trio chipset EA, ZT and YT-based line cards)**—Starting in Junos OS Release 23.4R1, we have introduced support for telemetry streaming of QoS queue statistics for pseudowire logical interface sets. You can stream operational state statistics using the native Junos resource path `/junos/system/linecard/cos/interface/interface-set/output/queue/`. The sensors stream queue statistics using gRPC Network Management

Interface (gNMI) or UDP. Suppression of zero values in statistics from streamed data is also supported.

[See [Junos YANG Data Model Explorer](#).]

- **Firewall filter OpenConfig configuration support (EX9204, EX9208, EX9214, MX204, MX240, MX480, MX960, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Junos OS Release 23.4R1 supports OpenConfig firewall filter (also known as access control list) configurations based on the OpenConfig data models `openconfig-acl.yang` (version 1.2.2) and `openconfig-network-instance.yang` (version 1.4.0).

[See [Mapping OpenConfig Firewall Filter Commands to Junos Configuration](#).]

- **ISIS operational state sensors and configuration using OpenConfig (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020 and vMX)**—Starting in Junos OS Release 23.4R1, we've introduced enhancements to IS-IS telemetry support based on OpenConfig data model `openconfig-isis.yang` (version 1.0.0). Support includes new operational state paths and configuration paths.

We've added a new configuration statement `no-lsp-authentication` at `[edit protocols isis level <level>]` hierarchy level.

[For OpenConfig configuration, see [Mapping OpenConfig ISIS Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **Interface counters on-box aggregation support (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, we now support on-board aggregation of interface counters. Off-box aggregation has limited insight into systemic events, such as line card resets or LAG membership changes. On-box aggregation support aggregates the counters at the source and generates a telemetry stream of aggregated PFE statistics and telemetry data that will reduce production errors at the collector.

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **CoS counter on-box aggregation support (MX204, MX480, MX960, MX10004, MX10008, MX10016, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, we now support on-board aggregation of CoS counters. Off-box aggregation has limited insight into systemic events, such as line card resets or LAG membership changes. On-box aggregation support aggregates the counters at the source and generates a telemetry stream of aggregated PFE statistics and telemetry data that will reduce production errors at the collector.

Use the following sensors:

- `/junos/system/linecard/interface/queue/` exports queue statistics on physical AE and RLT interfaces

- `/junos/system/linecard/interface/logical/usage/` exports queue statistics on physical AE and RLT interfaces
- `/qos/interfaces/interface/output/queues/queue/state/` exports queue statistics for AE and RLT physical interfaces and AE and PS logical interfaces
- `/junos/system/linecard/cos/interface/interface-set/output/queue/` exports queue statistics for logical AE and PS IFLsets

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **Mount point sensor support (ACX5448, ACX710, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we now support new sensors for mount points and memory usage. If a system has the concept of mounting physical or virtual resources to a mount point within the root file system (/), that mount point is included in the telemetry data stream using the sensor `/system/mount-points/`.

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **LACP telemetry support for new leaves (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, we now support the new LACP leaves `last-change` and `lacp-timeout` introduced in the OpenConfig data model `openconfig-lacp-yang` (version 1.2.0).

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **Multicast telemetry support with IGMP and PIM operational state sensors (ACX710, ACX5448, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we now support IGMP and PIM sensors based on the OpenConfig data models `openconfig-igmp.yang` (version 0.3.0) and `openconfig-pim.yang` (version 0.4.2).

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **New state data model for Juniper proprietary Remote Procedure (gRPC) service (ACX710, ACX5448, MX204, MX240, MX960, MX2008, MX2010, MX2020 and MX10004)**—Starting in Junos OS Release 23.4R1, we've included a restructured native state data model defining gRPC server instances. The new model includes common attributes and gRPC Network Management Interface (gNMI) service details.

The sensor `/state/system/services/http/servers/` and its leaves illustrate the new structure.

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **Resource Public Key Infrastructure (RPKI) enhanced streaming telemetry support (MX480 and vRR)**—Starting in Junos OS Release 23.4R1, we now support enhanced statistics for RPKI databases and RPKI sessions and validation-related statistics per route, per RIB and per BGP peer basis. Using these

statistics, you can perform operational debugging on your network and take appropriate mitigating actions.

These existing Junos operational mode commands contain new statistics:

- `show route [extensive|detail]` displays origin validation information for each route entry
- `show bgp neighbor validation statistics <peer>` displays BGP peer-RIB validation statistics
- `show route validation-statistics` displays local routing information base (RIB) specific validation statistics
- `show validation statistics` displays new counters for the Validated Route Payload (VRP) table

We now support the following telemetry sensors (with leaves):

- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/routes/route/origin-validation-state`
- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/routes/route/origin-validation-invalid-reason`
- `/state/routing-instances/routing-instance/protocols/bgp/groups/group/neighbors/neighbor/afi-safis/afi-safi[ipv4|ipv6]/validation-counters/`
- `/state/routing-instances/routing-instance/protocols/bgp/groups/group/neighbors/neighbor/afi-safis/afi-safi[ipv4|ipv6]/validation-counters`
- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/validation-counters/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/rpki-rtr/groups/group/sessions/session/rpki-session-counters/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/route-validation-databases/route-validation-database/[ipv4|ipv6]/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/rpki-rtr/groups/group/sessions/session/`

[For sensors, see [Junos YANG Data Model Explorer](#).] For operational mode commands, see [show route](#), [show bgp neighbor validation statistics](#), [show route validation-statistics](#), and [show validation statistics](#).

- **Segment routing sensors OpenConfig compliance support (MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, and MX10016)**—Starting in Junos OS Release 23.4R1, we now support OpenConfig compliant resource paths for the segment routing SID ingress

sensor. Use the new resource paths to export statistics using UDP, Juniper proprietary Remote Procedure Call (gRPC) or gRPC Network Management Interface (gNMI).

For example, the new OpenConfig compliant resource path `/network-instances/network-instance/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter/mpls-label` replaces `/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/aggregate-sid-counter/state/mpls-label`. If you are using UDP for export, the new OpenConfig compliant resource path `/network-instances/network-instance/mpls/signaling-protocols/segment-routing/aggregate-sid-counters/` replaces the resource path `/junos/services/segment-routing/sid/usage/`.

This feature also supports initial sync, a feature that samples all statistics for a subscription from a device, then only exports statistics that change.

[For sensors, see [Junos YANG Data Model Explorer](#).]

- **Routing policy and network instance OpenConfig configuration and sensor support (MX480)**—Starting in Junos OS Release 23.4R1, we support resource paths and OpenConfig configurations that have previously been unsupported or non-compliant with OpenConfig data models `openconfig-local-routing.yang` (version 2.0.0) and `openconfig-routing-policy.yang` (version 3.3.0).

[For OpenConfig configurations, see [Mapping OpenConfig Network Instance Commands to Junos Operation](#) and [Mapping OpenConfig Routing Policy Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **STP OpenConfig and operational state sensor support (ACX710, ACX5448, ACX5448-M, ACX5448-D, 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, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX10002, QFX10002-60C, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, we support OpenConfig STP configurations and sensors based on the OpenConfig data model `openconfig-spanning-tree` (Version 1, Revision 0.3.1).

[For OpenConfig configuration, see [Mapping OpenConfig STP Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

- **Upgrade of OpenConfig models for Routing Instances (ACX5448, ACX710, MX240, MX480, MX960, MX10003, MX10008, MX2008, MX2010 and MX2020)**—Starting in Junos OS Release 23.4R1, we support an upgrade for the following OpenConfig models:
 - `openconfig-local-routing.yang` to version 2.0.0.
 - `openconfig-routing-policy.yang` to version 3.3.0.

The upgraded models introduce new leaves for operational state sensors and configuration in the following areas:

- Inter-instance policies.
- Route limits.
- Router advertisement.
- Local aggregates.
- Static routes.

[For state sensors, see [Junos YANG Data Model Explorer](#).

For OpenConfig configuration, see [Mapping OpenConfig Network Instance Commands to Junos Configuration](#).]

- **Telemetry streaming of operational state data for syslog messages (ACX5448, ACX710, MX240, MX480, MX960, MX10004, MX10008, MX10016, MX2008, MX2010 and MX2020)**—Starting in Junos OS Release 23.4R1, we support telemetry streaming of operational state data for syslog messages to an external gNMI collector. Sensors are based on the native Junos data model under the hierarchy level `/state/system/syslog/messages/`. You can stream data using `ON_CHANGE` and `TARGET_DEFINED` modes.

[See [Junos YANG Data Model Explorer](#).]

MPLS

- **M-LDP Recursive FEC support (MX960, MX10004, MX10008)**—Starting in Junos OS Release 23.4R1, we partially support RFC 6512. We've introduced the recursive opaque value type for the MLDP forwarding equivalence class (FEC) element. The recursive opaque value helps to form Multipoint LDP (MLDP) point-to-multipoint (P2MP) tunnels between two autonomous systems (ASs), where the intermediate nodes do not have the route to reach the root node.

To enable the recursive opaque value, configure the `fec` statement at the `[edit protocols ldp p2mp recursive]` hierarchy level.

[See [Understanding Multipoint LDP Recursive FEC](#).]

- **Computation of unreserved bandwidth optimized RSVP dynamic bypass LSP (MX204, MX240, MX304, MX480, MX960, MX10003, MX10008, MX10016, MX2008, MX2010, MX2020, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, the Constrained Shortest Path First (CSPF) can optionally use a different approach to protect a link or a node by leveraging the computation based on unreserved bandwidths on traffic engineering (TE) links. To enable this feature, use the `optimize bandwidth` configuration statement at the `edit protocols rsvp interface interface link-protection` hierarchy level. While the default approach of RSVP bypass produces a bypass method that optimizes traffic engineering (TE) metric, enabling the new configuration statement maximizes the end-to-end unreserved bandwidth.

[See [Configuring Link Protection on Interfaces Used by LSPs](#).]

- **Capability to compute diverse paths between a set of LSPs (MX960, MX10004, and MX10008)**—Starting in Junos sOS Release 23.4R1, you can associate a group of LSPs (RSVP LSPs or SR MPLS LSPs) to the Path Computation Element Communication Protocol (PCEP) to compute diverse paths for the associated LSPs. The Junos PCC advertises to a Path Computation Element (PCE) that a particular LSP belongs to a diversity-association group. RFC 8800 defines PCEP protocol extensions to associate a set of LSPs that belong to the same association group. This enables a PCE to compute diverse paths for each of the LSPs in each diversity association group and then push the results to the PCC. A PCE can also associate set of LSPs across different PCCs.

You can enable diversity-association capability in the open message by configuring the following statement:

```
user@host# set protocol pcep diversity-association-capability
```

After enabling diversity-association capability, you need to also configure the diversity-association group using the following statement:

For RSVP LSPs:

```
user@host# set protocols mpls label-switched-path lsp-name lsp-external-controller pccd  
diversity-association group group-name
```

For SR LSPs:

```
user@host# set protocols source-packet-routing source-routing-path lsp-name diversity-  
association group group-name
```

You can provision and delegate the following LSPs:

- Provision PCE initiated RSVP LSPs with diverse paths
- Delegate RSVP LSPs with diverse association groups
- Provision PCE initiated SR MPLS uncolored LSPs with diverse paths
- Delegate SR MPLS uncolored LSPs with diverse association groups
- Provision PCE initiated SR MPLS colored LSPs with diverse paths
- Delegate SR MPLS colored LSPs with diverse association groups
- Provision PCE initiated SRv6 colored LSPs with diverse paths

- Delegate SRv6 colored LSPs with diverse association groups
- Provision PCE initiated SRv6 uncolored LSPs with diverse paths
- Delegate SRv6 uncolored LSPs with diverse association groups

[See [PCEP Configuration](#).

- **PCE requests to allocate binding SIDs for SR-TE Colored LSPs (MX480)**—Starting in Junos OS Release 23.4R1, a Path Computation Element (PCE) can request Path Computation Client (PCC) to allocate a binding SID from PCC's label space. PCE can request PCC to allocate a specific binding SID and can also allocate binding SID of PCC's choice.

The following PCEP operations are now supported:

- PCE requests PCC to allocate binding SID of PCC's choice for delegated LSPs
- PCE requests PCC to allocate binding SID of PCC's choice for PCE-Initiated LSPs
- PCE requests PCC to allocate a specific binding SID for delegated LSPs
- PCE requests PCC to allocate a specific binding SID for PCE-Initiated LSPs
- BGP LS for binding SID for colored SR LSP

The following SRTE binding SID database and label show commands has been introduced to display all binding SIDs with brief and detail outputs:

- `show spring-traffic-engineering binding-sid database brief`
- `show spring-traffic-engineering binding-sid database detail`
- `show spring-traffic-engineering binding-sid database label label brief`
- `show spring-traffic-engineering binding-sid database label label detail`
- `show spring-traffic-engineering binding-sid label label brief`
- `show spring-traffic-engineering binding-sid label label detail`

[See [PCEP Configuration](#).

- **Support for ICMP MTU exceed error message generation for labeled MPLS packets - Layer 3 VPN and static LSPs (MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2010, MX2020)**—Starting in Junos OS Release 23.4R1, we now support ICMP error message generation for MTU exceed errors in an MPLS environment. If a MPLS labeled packet failure occurs at the egress interface of the core or transit nodes due to MTU exceed errors, an ICMP error message is received at the source or Customer Edge devices.

To enable ICMP MTU exceed error message generation, you need to include the `icmp-tunnelling` configuration statement at the `[edit protocol mpls]` hierarchy on the core routers.

RFC3032 defines ICMP tunnel mechanism to handle ICMP error message generation for MPLS packets for TTL expiry and MTU exceeded exceptions.

- **Map static IPv6 route to next-hop using service label (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, virtual-chassis-fabric, QFX10002-60C, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 23.4R1, you can enable static IPv6 routes to be mapped to the next-hop over an IPv4 MPLS network. 6PE is a transitional IPv6 over IPv4 technology that uses MPLS tunnels to carry services.

You can use the `explicit-null` configuration statement under the `[edit routing-options rib inet6.0 static route ipv6-address]` hierarchy level to push ingress service label as part of the static next hop configuration for static IPv6 routes. The `explicit-null` configuration statement only supports configuring IPv4 mapped IPv6 address.

The static configuration statement under the `[edit routing-options forwarding-table chained-composite-next-hop ingress]` hierarchy provisions chained composite next-hop.



NOTE: The static configuration statement must be enabled before configuring the `explicit-null` configuration statement.

- **Distributed CSPF support for IPv6-based SR-TE (MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, we now support distributed CSPF path computation and auto-translation of IPv6 addresses through SR-TE configuration. A path's destination address family determines the address family of the SIDs used for the path. Configuring IPv6 addresses through SR-TE results in auto-translation of IPv6 addresses to the associated SIDs. IPv6 hops are defined in compute segment-lists.

Use the following CLI configurations to enable auto-translation of IPv6 addresses:

```
user@host# set protocols source-packet-routing segment-list name auto-translate
user@host# set protocols source-packet-routing segment-list name name ip-address IPv6-address
```

Use the following CLI configurations to define IPv6 hops in compute segment-lists:

```
user@host# set protocols source-packet-routing compute-profile name compute-segment-list name
```

```
user@host# set protocols source-packet-routing segment-list name compute
user@host# set protocols source-packet-routing segment-list name ip-address IPv6-address
```

Use the following CLI configurations to enable IPv6 path end points:

```
user@host# set protocols source-packet-routing compute-profile name ...
user@host# set protocols source-packet-routing source-routing-path name to IPv6-address
user@host# set protocols source-packet-routing source-routing-path name primary name compute
compute-profile-name
```



NOTE: End points must be IPv6 router IDs. Other addresses may be router IDs or interface addresses.

The `show spring-traffic-engineering lsp` command has been enhanced to show the details of IPv6 addresses.

- **Support IPv6 address for seamless BFD over static segment routing MPLS LSPs (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 23.4R1, MX Series devices support IPv6 address family for seamless Bidirectional Forwarding Detection (S-BFD) over static segment-routing MPLS LSPs. The mode of operation for sBFD support for IPv6 in centralised and distributed mode is as follows:
 - IPv6 support for sBFD over static segment routing MPLS LSP for responder and initiator in distributed mode.
 - IPv6 support for sBFD over static segment routing MPLS LSP for initiator in centralised mode.

sBFD IPv6 responder session can only be configured by including the `local-ipv6-address` configuration statement at the `[edit protocols bfd sbfd local-discriminator disc]` hierarchy level as follows:

```
user@host# set protocols bfd sbfd local-discriminator disc local-ipv6-address ipv6-address
```

The IPv6 address that is configured is used as the source IPv6 address in the reply packet.

- **New CLI commands for MPLS LSPs (ACX5448, ACX5448-M, ACX5448-D, MX204, MX240, MX304, MX480, MX960, MX10003, MX10008, MX10016, MX2008, MX2010, MX2020, QFX10008, and QFX10016)**—Starting in Junos OS 23.4R1, you can get more visibility into the current state of the MPLS LSPs on the router to debug suspected anomalies in high scale conditions with the following newly introduced CLI commands.

- `show rsvp session bypass [bypass-name] [protected]` and `show rsvp session [unprotected]` provides visibility into LSPs protected by a specific bypass tunnel.
- `show mpls lsp [make-before-break]` and `show rsvp session [multiple-lsp-sessions]` provides visibility into LSPs undergoing make-before-break.
- `show mpls tunnel-manager-statistics` provides statistics on all local repair and make-before-break events for LSPs.
- `show rsvp session [fr-ingress]` provides visibility into LSPs on flood-reflector edge routers.
- **PCC Policy Association with SR and RSVP LSP (MX960, MX10004, and MX10008)**—Starting in Junos OS 23.4R1, PCC (Path Computation Clients) can link policies with a group of Label Switched Paths (LSPs). This enhancement allows Junos PCC to communicate with a Path Computation Element (PCE) using an extended communication protocol (PCEP). Through this extension, Junos PCC can tell the PCE that a specific LSP is part of a certain Policy Association Group.

Multicast

- **IGMP and MLD snooping version configuration (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, and MX2020)**—Starting in Junos OS Evolved Release 23.4R1, you can configure the version of IGMP or MLD snooping queries for VLANs or bridge domains associated with Layer 2 (L2) multicast. This configuration ensures that end hosts or CPE devices that are not compliant with RFC 4541 and can't normally respond to snooping queries of a later version are now able to process and respond to those snooping queries.

To configure the IGMP or MLD snooping version, use the following CLI statements:

- `set protocols igmp-snooping version version`
- `set protocols mld-snooping version version`

[See [IGMP MLD Snooping Version Configuration](#).]

- **Multiple active and backup paths in RPF list (MX240, MX480, MX960, MX10004, MX10008, and MX10016 with MPC5E and MPC7E line cards)**—Starting in Junos OS Release 23.4R1, the session ID created for a unicast RPF next-hop is used to group labels in the same LSP. This allows Junos to accept and forward traffic from any label with a matching Session ID. This minimizes transmission loss time to sub-50 ms in the cases of MBB in Hot-root standby (HRS) enabled NG-MVPN provider tunnels, and I-PMSI to S-PMSI switchovers.

[See [Multiple Active and Backup Paths in RPF List](#).]

- **Backup UMH selection (MX960)**—In earlier releases, backup upstream multicast hop (UMH) selection was based on the highest IP address. Starting in Junos OS Release 23.4R1, backup UMH selection is based on the same algorithm used to select the primary UMH. This feature is enabled by default.

[See [Backup UMH Selection](#).]

Network Address Translation (NAT)

- **Port overflow burst mode (MX240, MX480, and MX960)**—Starting in Junos OS Release 23.4R1, we support port overflow burst mode. You can use the ports beyond the allocated port blocks with the port overflow burst mode. You can configure a burst pool with a range of ports in an IP address to be reserved for bursting.

There are primary and burst pool types, device uses the burst pool type after the subscribers reach the limit configured in the primary pool.

You can configure one or more IP addresses as a separate burst pool. You can configure ports from the same IP address or separate IP address for bursting.

[See [Port Overflow Burst Mode](#) and [port \(Security Source NAT\)](#).]

- **NAT PBA monitoring (MX240, MX480, MX960, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, we've added the following enhancements:
 - Support for port overloading and index-based port utilization in SNMP MIB table. **jnxJsNatPortOverloadUtilTable**.
 - Support for pool based port utilization MIB object **jnxJsNatPoolUtil** on MX-SPC3.
 - A new trap in the MIB table **jnxJsSrcNatOverloadedPoolThresholdStatus** to alert when the port is overloaded.
 - Support for source NAT PBA table **jnxJsNatPbaStatsTable** in SRX Series Firewall.
 - Display sessions filters:
 - On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.
 - On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm raise-threshold <value>` command.
 - On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.
 - On MX-SPC3, use the `set services nat source port-overloading-usage-alarm raise-threshold <value>` command.
 - Clear sessions filters:

- On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
- On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm clear-threshold <value>` command.
- On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
- On MX-SPC3, use the `set services nat source port-overloading-usage-alarm clear-threshold <value>` command.

[See [show security flow session](#), [clear services sessions](#), [show services sessions](#), [clear security flow session](#), [pool \(Security Source NAT\)](#) and [port \(Security Source NAT\)](#).]

Network Management and Monitoring

- **System logging support to capture the layer 2 error conditions on ports (EX-Series, MX-Series, and QFX-series)**—Starting in Junos OS Release 23.4R1, Junos OS generates system log messages for MAC Limiting, MAC Move Limiting, MAC learning, Storm control, and redundant trunk groups (RTGs) to record the error conditions on ports.

[See [Overview of System Logging](#).]

Platform and Infrastructure

- **Dual-phase bootup (MX Series)**—Starting in Junos OS Release 23.4R1, you can prevent the device from reaching an amnesiac state post-reboot by configuring the dual-phase-bootup feature before the reboot. When a device has a scaled configuration or has a lot of constraints to be validated, upon reboot it may take more than 45 minutes to finish. This lengthy reboot time exceeds the limit set for the watchdog timer. The watchdog timer going off can cause the device to reach an amnesiac state. To avoid reaching an amnesiac state during a future reboot, configure the dual-phase-bootup statement at the [edit system] hierarchy level. If you have configured the dual-phase-bootup statement before the reboot, the device picks up the rescue configuration from the next reboot. Post-reboot, the device's operational state is active and the device automatically loads the last-configured user configuration (**juniper.conf** file), thus preventing the device from reaching an amnesiac state. To be able to commit the configuration for the dual-phase-bootup statement, you must already have created a rescue configuration (**rescue.conf** file). We recommend that you have a minimal rescue configuration.

[See [dual-phase-bootup](#) and [show dual-phase-bootup-status](#).]

- **Support for subscriber management functionality (MX10004, MX10008, and MX10016 using LC9600 line card)**—Starting in Junos OS Release 23.4R1, we provide support for the following features:
 - Basic and advanced CoS and filters (IPv4 or dual stack) for:

- Dynamic VLANs (DVLANS) with DHCP subscribers
- DVLAN with Point-to-Point Protocol (PPP) subscribers
- DVLAN and agent circuit identifier (ACI) with DHCP subscribers
- DVLAN and ACI with PPP subscribers
- Stacked DVLAN with DHCP subscribers
- Stacked DVLAN with PPP subscribers
- Pseudowire DVLAN with DHCP subscribers
- Pseudowire DVLAN with PPP subscribers
- DVLAN with L2TP access concentrator (LAC) (IPv4) basic and advanced CoS and filters
- DVLAN with L2TP network server (LNS) (IPv4 and dual stack) basic CoS and filters
- Advanced CoS and filters (IPv4 or dual stack) support for:
 - DHCP subscribers
 - PPP subscribers
- L2TP tunnels
- Subscriber services (customer solutions test scripts) processing
- Scaling and performance for the following features:
 - DHCP subscribers with authenticated dynamic VLAN
 - DHCP subscribers with authenticated dynamic service VLAN (S-VLAN)
 - LNS subscribers
 - LAC subscribers
 - CoS service
 - Firewall service

[See [Features Supported on MX10008, and MX10016.](#)]

- **Packet Forwarding Engine support on (MX10004)** [See [show pfe fpc.](#)]

Precision Time Protocol (PTP)

- **Support for Precision Time Protocol (PTP) G.8275.2 enhanced profile over LAG with IPv4, IPv6 or mixed mode unicast traffic (MX10K-LC2101 on MX10008)**—Starting in Junos OS Release 23.4R1, the MX10K-LC2101 line card on MX10008 platform supports the PTP G.8275.2 enhanced profile. This is based on Partial Timing Support (PTS) using unicast PTPoIPv4 and PTPoIPv6. The G.8275.2 enhanced profile complies with the performance requirements for T-BC-P/T-TSC-P node types as specified in the ITU-T G.8273.4 specification. This feature provides you flexibility to relax the frequency and phase offsets required for a lock by configuring the frequency-lock-threshold and phase-lock-threshold configuration knobs respectively. In addition, it helps relax the maximum phase offset to adjust in phase-aligned state by configuring the phase-adjust-threshold knob in the PTP configuration.

[See [PTP Profiles](#).]

Routing Options

- **Support for configuring route priority for BGP static routes and route prioritization during reconfiguration (MX240, MX 480, and MX960)**—Starting in Junos OS Release 23.4R1, you can configure a route priority for static routes. Include the priority statement at the [edit routing-options static route destination next-hop] hierarchy level. In addition, when you perform a route reconfiguration, a new routing table policy mechanism ensures that routes are processed based on the configured priority.

[See [BGP Route Prioritization](#).]

Routing Protocols

- **Support for EIBGP multipath ECMP for defined prefixes (MX Series)**—Junos OS Release 23.4R1 supports EIBGP and IBGP (EIBGP) multipath. In the existing BGP multipath, EIBGP routes take priority over IBGP routes because both have different metrics. After you enable EIBGP multipath and there is equal load sharing between EIBGP and IBGP routes, Junos OS initiates ECMP using a blend of both EIBGP and IBGP.

Feature-specific policies specify prefixes that support EIBGP multipath. You can configure the policy to choose the prefixes based on any match condition.

To enable EIBGP multipath, configure the allow-external-internal option at the [edit protocols bgp multipath] or [edit logical-systems *logical-system-name* protocols bgp multipath] hierarchy level.

[See [multipath \(Protocols BGP\)](#).]

- **Support for micro-SIDs in TI-LFA, microloop avoidance, flex algo, and IS-IS MT (MX Series)**—Starting in Junos OS Release 23.4R1, we extend the support of compressing SRv6 addresses into a single IPv6 address (micro-SID) in topology-independent loop-free alternate (TI-LFA), microloop avoidance, and Flexible Algorithm (flex algo) path computations. From this release onward, you can also

configure algorithms for micro-segment identifiers (micro-SIDs) to facilitate the new extended feature. We also support IPv6 unicast topology (part of IS-IS MT) in TI-LFA, microloop avoidance, and flex algo computations.

To enable flex algo to install the ingress routes in transport class routing information bases (RIBs), configure the `use-transport-class` statement at the `[edit routing-options flex-algorithm id]` hierarchy level.

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

- **Support for OSPFv2 HMAC SHA-1 keychain authentication and optimization for multi-active MD5 keys (EX2300, EX2300-C, EX2300-MP, EX2300-VC, EX3400, EX3400-VC, EX4100-24MP, EX4100-24P, EX4100-24T, EX4100-48MP, EX4100-48P, EX4100-48T, EX4100-F-12P, EX4100-F-12T, EX4100-F-24P, EX4100-F-24T, EX4100-F-48P, EX4100-F-48T, EX4300-MP, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, MX204, MX240, MX304, MX480, MX960)**—Starting in Junos OS Release 23.4R1, you can enable OSPFv2 HMAC-SHA1 authentication with keychain to authenticate packets reaching or originating from an OSPF interface. This feature ensures smooth transition from one key to another for OSPFv2 with enhanced security.

You can enable OSPFv2 to send packets authenticated with only the latest MD5 key after all the neighbors switch to the latest configured key. In Junos OS releases earlier than Release 23.4R1, we support advertising authenticated OSPF packets always with multiple active MD5 keys with a maximum limit of two keys per interface.

To enable OSPFv2 HMAC-SHA1 authentication, configure the authentication keychain `<keychain name>` option at the `[edit protocols ospf area area-id interface interface_name]` hierarchy level. To enable optimization of multiple active MD5 keys, configure the `delete-if-not-in-use` option at the `[edit protocols ospf area area-id interface interface_name authentication multi-active-md5]` hierarchy level.

[See [Understanding OSPFv2 Authentication](#).]

- **Support for Next-Hop Dependent Capability Attribute (ACX5448 and MX10016)**—Starting in Junos OS Release 23.4R1, we use the Entropy Label Capability (ELCv3) attribute defined within the IETF BGP Next-Hop Dependent Capability Attribute for load balancing. This attribute replaces the existing ELCv2 attribute. To operate the ELCv2 attribute along with ELCv3, explicitly configure the `elc-v2-compatible` statement at the `[edit protocols bgp family inet labeled-unicast entropy-label]` hierarchy level.

[See [Understanding Entropy Label for BGP Labeled Unicast LSP](#).]

- **Support for limiting the number of BGP sessions belonging to a subnet (MX Series)**—Starting in Junos OS Release 23.4R1, we support limiting the number of BGP sessions belonging to a given subnet that is configured using the `allow` statement. With this feature, you can configure wider subnets by limiting the number of BGP sessions over them. You can set this limit using the `peer-limit` value statement at the `[edit protocols bgp group group-name dynamic-neighbor]` hierarchy level.

[See [peer-limit](#).]

Public Key Infrastructure (PKI)

Services Applications

- **Support for MAP-T solution (MX Series)**—Starting in Junos OS Release 23.4R1, you can configure Mapping of Address and Port using Translation (MAP-T) as an inline service on MX Series routers with MPCs and MICs. MAP-T is a double stateless NAT64-based solution. The MAP-T solution uses IPv4-IPv6 translation as the form of IPv6 domain transport. The translation mode is considered advantageous in scenarios where the encapsulation overhead or IPv6 operational practices rule out encapsulation.

- **Support for consistent hash load balancing on FTIs (MX Series)**—

Starting in Junos OS Release 23.4R1, flexible tunnel interfaces support consistent hash load balancing on the MX Series routers. During load balancing, when the number of ECMP paths crosses the threshold, the server fails and results in traffic skewness.

With consistent hashing, you can avoid skewness of the flows toward initial set of ECMP paths. Only the flows for paths that are inactive are redirected. Flows mapped to servers that remain active are maintained.

[See [Understanding ECMP Groups](#).]

Software Defined Networking (SDN)

- **JDM supports IPv6 addresses (Junos node slicing)**—Starting in release 23.4R1, Juniper Device Manager (JDM) supports configuration and management of IPv6 addresses. This enhancement is applicable to both in-chassis and external server-based Junos node slicing.

[See [Components of Junos Node Slicing](#).]

Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for SRv6 micro-SIDs in IS-IS transport (MX Series)**—Starting in Junos OS Release 23.4R1, you can compress multiple Segment Routing for IPv6 (SRv6) addresses into a single IPv6 address (the micro-SID). Typically, if a packet needs to traverse multiple nodes, IS-IS can stack up the SRv6 segment identifiers (SIDs) using a segment routing header. This stacking of SIDs adds to the bandwidth overhead and the segment routing header processing overhead.

You can now compress the SID list to a single destination address (the micro-SID) and reduce the bandwidth overhead. Segment routing headers can typically allow a stack of only six SRv6 SIDs. For use cases that need to include more than six SRv6 SIDs, micro-SIDs can help in compressing multiple IPv6 addresses.

[See [How to Enable SRv6 Network Programming in IS-IS Networks](#) and [micro-sid](#).]

- **SRv6 dynamic SID support for BGP and IS-IS protocols (MX Series)**—Starting in Junos OS Release 23.4R1, we support dynamic segment identifiers (SIDs) for BGP and IS-IS.

To enable dynamic end SID, include the `dynamic-end-sid` at the `[edit protocols isis source-packet-routing srv6 locator locator-name]` hierarchy level.

To enable dynamic end x SID, include the `dynamic-end-x-sid` at the `[edit protocols isis interface int-name level level-numbersrv6-adjacency-segment protected locator locator-name]` hierarchy level.

[See [level](#) and [srv6](#)]

- **Mitigate traffic congestions using tactical traffic engineered (TTE) tunnels (MX240, MX480, and MX960)**—Starting with Junos OS Release 23.4R1, you can avoid congestions on oversubscribed links or domains using the dynamic tactical traffic engineered (TTE) tunnel solution. The dynamic TTE tunnel solution allows you to define congestion for a link by configuring high and low bandwidth thresholds. If the traffic load on the link exceeds the high threshold, then load-sharing is increased. If the traffic load falls below the low threshold, then load-sharing is decreased.

The TTE solution helps you to:

- Load-balance traffic towards destination prefixes using the congested outgoing interface or through a dynamically installed Tactical TE (TTE) tunnel..
- Monitor the cumulative load and subsequent deactivation of the TTE tunnel(s) when congestion is no longer detected.

To enable congestion protection, include the `congestion-protection` statement at the `[edit routing-options]` hierarchy level. Define high and low bandwidth thresholds by including the `high-threshold` and `low-threshold` statements at the `[edit routing-options congestion-protection template template-name]` hierarchy level. You also need to include the `export isis-export` statement at the `[edit protocols isis]` hierarchy level.

The TTE tunnel solution supports ISIS and uses TI-LFA backup routes for congestion mitigation.

- **BGP classful transport support for IPv4 DTM segment routing traffic engineered (SR-TE) tunnels (MX10004)**—Starting in Junos OS Release 23.4R1, we support transport-rib model for V4 DTM SR-TE tunnels by configuring the `use-transport-class` statement at the `[edit dynamic-tunnels tunnel-name spring-te]` hierarchy level.

If the `use-transport-class` statement is not configured then catch all route and application route is created in the `inetcolor.0` table. If the `use-transport-class` statement is configured then catch all route and application route is created in `color.inet.3` table. This behavior is irrespective of including the `use-transport-class` statement at the `[edit protocols source-packet-routing]` hierarchy. For dynamic tunnels, SR-TE honors the `use-transport-class` statement under the dynamic-tunnel configuration rather than source-packet-routing configuration.

The following IPv4 endpoint for DTM SR-TE tunnels with transport-rib model is supported:

- DCSPF support (using compute-profile)
- Dynamic segment list support. Configured segment list must not have any IPv6 address and MPLS SID based of IPv6.
- Delegation to PCEP controller
- sBFD support
- SPRING-TE route is added only into color.inet.3 table

For IPv4 endpoint for DTM SR-TE tunnels with inetcolor.0 model, if the use-transport-class statement is configured under SR-TE, then dynamically triggered SR-TE tunnel routes is created in both inetcolor.0 table and color.inet.3 table. The use-transport-class statement under dynamic-tunnels hierarchy decides if the SR-TE tunnels need to be placed in color.inet.3 table. SPRING-TE route is added only into inetcolor.0 table for DTM SRTE tunnels for IPv4 endpoints and inetcolor.0 model.

Traffic steering based on extended color community is supported. For transport-rib model for DTM SR-TE tunnels (IPv4 destinations only), enable the computation and setup of interdomain segment routing paths using express-segments with SR-Policy underlay.

Subscriber Management and Services

- **Session scale configurations for wireless CUPS (MX Series)**—Starting in Junos OS Release 23.4R1, you can select the session scaling profile for your specific configuration. The session scaling profile determines how much memory is allocated for your user sessions in wireless control and user plane separation (CUPS). If you don't select a session scale, Junos OS uses the maximum available scale size for your device.

When the number of sessions reaches 80%, 90%, and 100% of the active scaling profile, Junos OS sends telemetry and ERRMSG notifications to you. At 100% usage, Junos OS rejects new sessions..

[See [Session Maintenance and Optimization](#)].

- **Session maintenance support for wireless CUPS (MX Series)**—Starting in Junos OS Release 23.4R1, you can view session entries from the internal table with the transient-sessions filter. This filter enables you to view all sessions and session IDs that are in a transient state. If a session stays in a transient state for a longer duration of several minutes, you can consider it a potentially stuck session.

You can view session summaries in both 5-minute and hourly increments.

You can also manually clear sessions by the session IDs. This action enables you to remove any subscriber sessions that get stuck in any state.

Junos OS deletes exact routes when the last session using that route is deleted. Junos OS will not advertise the deleted routes, and the routes aren't visible to other devices and Junos OS users.

[See [Session Maintenance and Optimization](#)].

- **Peer group routing instance support for wireless CUPS**—Starting in Junos OS Release 23.4R1, you must designate a routing instance in Junos OS for each peer group on the same user plane function (UPF). Doing this isolates control traffic when more than one subscriber management function (SMF) terminates on the same UPF.

[See [Session Maintenance and Optimization](#)].

- **PCEF Diameter Enhancements (MX480)** – Starting in Junos OS Release 23.4R1, the MX480 router supports the following enhancements to the policy and charging enforcement function (PCEF) for the diameter application:
 - Customization of Subscription-Id-Data attribute-value pair (AVP) in Credit-Control Request (CCR), sourced from the RADIUS server. The external subscription ID is activated by default.
 - Customization of Calling-Station-Id in RADIUS requests. To customize Calling-Station-Id in RADIUS requests, configure the command `remote-circuit-id-format (postpend | prepend)` under `[edit access profile <profile-name> radius options]hierarchy` level.
 - Usage monitoring through Third-Generation Partnership Project (3GPP) attribute-value pairs (AVPs) defined as diameter Gx for subscriber services using the dynamic-profile configuration.

[See [Understanding Junos Subscriber Aware Policy and Charging Enforcement Function \(PCEF\)](#) and [Configuring Diameter AVPs for Gx Applications](#).]

- **Support for one-to-many SCTP associations (MX204, MX240, MX480, MX960, and MX10003)**—Starting in Junos OS Release 23.4R1, Junos OS supports a one-to-many style SCTP endpoint on the Access Gateway Function (AGF).

[See [SCTP](#).]

- **Broadband edge static framed-route for subscriber management (MX Series)**—Starting in Junos OS Release 23.4R1, you can now set up static subscriber IP addresses for multiple hosts on a site as follows:
 - Enable, disable, add, update, or delete static framed routes when subscribers are not up and attach the configured static framed route when a subscriber logs in. Static framed routes are supported for IPv4 only.
 - Use the `set routing-instances routing-instance routing-options access route ip` command to configure and commit routes to the routing table. The routes are hidden, until the configured subscriber IP comes up.

- Use the `static-framed-route` command at `[edit system services subscriber-management]` hierarchy level to configure the static framed-route on the Broadband Network Gateway (BNG) towards a specific subscriber. You can now use the RADIUS server only for authentication purposes.

[See [No Link Title](#), [No Link Title](#), [No Link Title](#), and [No Link Title](#).]

System Logging

- **Support for log profiles and templates on MX-SPC3 (MX Series)**—Starting in Junos OS Release 23.4R1, we support policy-related logs for these features:
 - Session
 - Network Address Translation (NAT)
 - PCP
 - SFW

[See [System Log Error Messages for Next Gen Services](#).]

VPNs

- **Support for robust protection against DDoS attacks on IKE protocol with `iked` process (MX240, MX480, and MX960 with SPC3, SRX1500, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, you can efficiently monitor and mitigate DDoS attacks on IKEv1 and IKEv2 protocols when your firewall runs the `iked` process for the IPsec VPN service.

To support the feature, we introduce the following configuration statements at the `[edit security ike]` hierarchy level:

- `session`—Tune parameters to manage the behavior of negotiations with the remote peers to protect the security associations. Configure the parameters at the `[edit security ike session half-open]` and `[edit security ike session full-open]` hierarchy levels.
- `blocklists`—Define multiple blocklists and their associated rules for blocking an IKE ID. Configure the blocklists at the `[edit security ike session blocklists]` hierarchy level. You must attach a blocklist to one or more IKE policies at the `[edit security ike policy policy-name blocklist blocklist-name]` hierarchy level.

Use the following commands to view and clear statistics and other details about the in-progress, failed, blocked, and backoff peers:

- `show security ike peer statistics` and `show security ike peer`.
- `clear security ike peers statistics` and `clear security ike peers`.

[See [IKE Protection from DDoS Attacks](#), [session \(Security IKE\)](#), [blocklists \(Security IKE\)](#), [show security ike peers statistics](#), [show security ike peers](#), [clear security ike peers statistics](#), and [clear security ike peers](#).]

Additional Features

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

- **400G-ZR-M Optics Support on MX304**—Starting in Junos OS Release 23.4R1, we support 400G OpenZR+ optics on MX304 devices. The supported feature includes high Tx (0dBm) power. You can view the advertised applications and can switch between the applications.



NOTE: MX304 devices do not support application selection, transmit output power and enhanced loopback options.

See [400ZR and 400G OpenZR+](#)

- **CoS support for BNG on pseudowire service interface over active-active RLT interface (MX304)**
[See [Anchor Redundancy Pseudowire Subscriber Logical Interfaces Overview](#), [targeted-options \(PS interface\)](#), [logical-interface-fpc-redundancy \(PS interface\)](#), [rebalance-subscriber granularity](#), and [show interfaces demux0 \(Demux Interfaces\)](#).]
- **Load-balancing support for subscriber traffic on pseudowire service interface (MX304)**
[See [Pseudowire Subscriber Logical Interfaces Overview](#).]
- **Logging support for Routing Engine shell (MX240, MX480, MX960, MX10003, MX10004, MX10008, and MX10016).** You can log commands executed from the shell when you configure `set system syslog shell`.
[See [shell](#) and [syslog \(System\)](#).]
- **Support for Access Gateway Function (AGF)** (MPC10 line cards on MX240, MX480, and MX960 routers and MK10K-LC9600 line cards on the MX10004 and MX10008 routers)—This feature applies to the line cards with core facing N3 interfaces.
[See [Access Gateway Function User Guide](#).]
- **Support for FXC service on EVPN-VPWS networks.**(MPC2, MPC5, MPC7, MPC8, MPC9,MPC10, MPC11, MX304, and MK10K-LC9600) We support the following flexible cross-connect (FXC) operations in an Ethernet VPN–virtual private wireless service (EVPN-VPWS) network:
 - Single-homing and single-active multihoming support
 - Pseudowire Subscriber (PS) interfaces with the logical tunnel or redundant logical tunnel endpoints.

- Static VLAN demultiplexing (demux) interfaces
- Dynamic VLAN demux Interfaces with DHCP and PPPoE

[See [Overview of Flexible Cross-Connect Support on VPWS with EVPN](#), [Pseudowire Subscriber Logical Interfaces Overview](#), and [Subscriber Interfaces and Demultiplexing Overview](#).]

- **Support for MACsec VLAN tag in the clear support** (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48T, and MX304)

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

- **Support for retrieving NETCONF state information** (MX960). NETCONF clients can retrieve NETCONF state information for the following `netconf-state` subtrees:

- capabilities—Supported NETCONF operations
- datastores—Supported configuration datastores
- sessions—Active NETCONF sessions
- statistics—NETCONF server performance data

[See [NETCONF Monitoring](#).]

- **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 HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- [Class of Service \(CoS\) | 83](#)
- [General Routing | 83](#)
- [Junos XML API and Scripting | 84](#)
- [Network Management and Monitoring | 84](#)
- [Platform and Infrastructure | 85](#)
- [User Interface and Configuration | 85](#)

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

Class of Service (CoS)

- You cannot apply a classifier to a physical interface on MX Series routers. On MX Series routers, you must apply the classifier to a logical interface.
- **Changes to the XML output for CoS RPCs (MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020)**—We've updated the `junos-rpc-class-of-service` YANG module and the corresponding Junos XML RPCs to ensure that the RPC XML output conforms to the YANG schema. As a result, we changed the XML output for the following class of service (CoS) RPCs:
 - `<get-cos-adjustment-control-profile-information>`—The `<adjustment-control-profile-name>` tag is a child of the `<adjustment-control-profile>` element instead of a sibling.
 - `<get-cos-red-information>`—The `<red>` tag no longer emits the `xmlns="m-t-mx-j-series-cosinfo-red-entry-format"` namespace attribute.
 - `<get-cos-slice-information>`—The XML output only emits integers for parameters such as `<shaping-rate>`, `<delay-buffer-rate>`, and similar fields. The output does not include any units.
 - `<get-scheduler-map-table-map-information>`—The `<cos-scheduler-map-table-information>` tag does not emit a namespace attribute.

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.
- **Deprecated license revoke information**—Starting in Junos OS Release 23.4R1, we've deprecated the `show system license revoked-info` command. You can use the `show system license` and `show system license usage` commands to know the license information.
- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)**—We've introduced the extensive option for the `show security ipsec security-associations` command. Use this option to display IPsec security associations with all the tunnel events. Use the existing `detail` option to display upto ten events in reverse chronological order.

[See [show security ipsec security-associations](#).]

- **Change in the XML tags displayed for the `show virtual-network-functions` command in JDM (Junos node slicing)** — To align the XML tags displayed for the `show virtual-network-functions "gnf-name" | display xml` with the new XML validation logic, we have replaced the underscores (`_`) in the output with hyphens (`-`) as shown below:

Old output:

```
user@jdm> show virtual-network-functions mgb-gnf-d | display xml
```

This change is applicable to any RPC that previously had underscores in the XML tag name.

Junos XML API and Scripting

- **Ability to commit extension-service file configuration when application file is unavailable**—When you set the optional option at the `edit system extension extension-service application file file-name` hierarchy level, the operating system can commit the configuration even if the file is not available at the `/var/db/scripts/jet` file path.

[See [file \(JET\)](#).]

- **XML output tags changed for `request-commit-server-pause` and `request-commit-server-start` (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the `request system commit server pause` command (`request-commit-server-pause` RPC) and the `request system commit server start` command (`request-commit-server-start` RPC). The root element is `<commit-server-operation>` instead of `<commit-server-information>`, and the `<output>` tag is renamed to `<message>`.

Network Management and Monitoring

- **NETCONF `<copy-config>` operations support a `file://` URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF `<copy-config>` operation supports using a `file://` URI when `<url>` is the target and specifies the absolute path of a local file.

[See [<copy-config>](#).]

Platform and Infrastructure

- Previously, shaping of Layer 2 pseudowires did not work on logical tunnel interfaces. This has been fixed for all platforms except QX chip-based MICs and MPCs.

User Interface and Configuration

- Viewing files with the `file compare files` command requires users to have maintenance permission**—The `file compare files` command in Junos OS and Junos OS Evolved requires a user to have a login class with maintenance permission.

[See [Login Classes Overview](#).]

Known Limitations

IN THIS SECTION

- [General Routing | 85](#)
- [Infrastructure | 86](#)

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

- On the MX2000 line of routers, you might see RPD usage hit 100% when you start running OCST polling. The spike in RPD usage is expected because of the very large scale and OCST in general. This issue should not affect any RPD functionality if that is the concern since telemetry streaming is the lowest priority task in RPD. [PR1614978](#)

- It is recommended to use IGP shortcut with strict SPF SIDs in SRTE path. if Strict SPF SIDs are used then this issue would not occur. This issue will occur only if regular ISIS SIDs are used in SRTE path and IGP shortcut is enabled. with this, if customer perform multiple times deactivate/activate for SRTE telemetry. [PR1697880](#)
- On older MPC Cards (for example, MPC6) that have PPC as the host CPU, the CPU usage can exceed 95% whenever the host-bound traffic rate is more than 5k-6k PPS. SNMP polling consumes a significant amount of CPU resources; disabling it will allow the system to handle some amount of additional PPS host-bound traffic. In current PR context, disabling SNMP allowed the system to handle an additional 2k-3k PPS of host-bound traffic. When the CPU usage is greater than 95 percent, host-bound routing protocol packets (for example, BGP and ISIS) may not be drained fast enough, which may result in flaps. [PR1749829](#)

Infrastructure

- Juniper Routing-Engines with HAGIWARA CF card installed, after upgrade to 15.1 and later releases, the failure message about "smartd[xxxx]: Device: /dev/ada1, failed to read SMART Attribute Data" might appear on messages log. [PR1333855](#)
- When upgrading from releases before Junos OS Release 21.2 to Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. <https://kb.juniper.net/TSB18251> [PR1568757](#)

Open Issues

IN THIS SECTION

- [EVPN | 87](#)
- [Flow-based and Packet-based Processing | 87](#)
- [General Routing | 87](#)
- [Interfaces and Chassis | 90](#)
- [MPLS | 90](#)
- [Multicast | 90](#)
- [Network Management and Monitoring | 90](#)
- [Platform and Infrastructure | 91](#)

- Routing Protocols | 91
- Services Applications | 92

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

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

EVPN

- A few duplicate packets might be seen in an A/A EVPN scenario when the remote PE device sends a packet with an IM label due to MAC not learned on the remote PE device, but learned on the A/A local PE device. The nondesignated forwarder sends the IM-labeled encapsulated packet to the PE-CE interface after MAC lookup instead of dropping the packet, which causes duplicate packets to be seen on the CE side. [PR1245316](#)
- After GRES, VPWS switchover occurs only after NSR phantom timer expires. The NSR phantom timer is configurable. This can result in packet loss for that duration. [PR1765052](#)

Flow-based and Packet-based Processing

- The subscription path for flow sensor shall be changed from `/junos/security/spu/flow/usage` to `/junos/security/spu/flow/statistics`. This change is done to maintain uniform format for subscription path in request and response data. [PR1738832](#)

General Routing

- `fpc3` cannot scan `phys_mem_size.out` syslog error occurs at `/var/log/*.out (0;0xdd3f6ea0;-1)`. [PR1548677](#)
- Because of a race condition, the `show multicast route extensive instance instance-name` output can display the session status as invalid. Such an output is a cosmetic defect and not indicative of a functional issue. [PR1562387](#)

- When the active slave interface is deactivated, the PTP lock status is set to 'INITIALIZING' state in `show ptp lock-status` output for few seconds before BMCA chooses the next best slave interface. This is the day-1 behavior and there is no functional impact. [PR1585529](#)
- Output of the `show network agent` command shows null indicating the statistic per component after GRES. [PR1610325](#)
- 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](#)
- Current stack and display is correctly set to 128 ports that is qualified on all MX10K8 linecards [PR1706376](#)
- 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](#)
- Next Hop counts are not as expected. [PR1710274](#)
- The commit notification from 'edit private' mode won't produce correct patch. [PR1713447](#)
- rpd might generate core file when running slow related gribi toby scripts in fusion system. Running same scripts in manually deployed testbed will not trigger rpd core file. [PR1715599](#)
- Segmentation fault on grpc timer thread (might be related to keepalive) #32085 grpc issue <https://github.com/grpc/grpc/issues/32085> grpc stack needs to be upgraded to 1.53 or later. [PR1722414](#)
- With a two-color policer configured on aggregated Ethernet interfaces, the "queue-counters-trans-bytes-rate" counter might display an incorrect value. [PR1735087](#)
- On all Junos OS devices, the time needed to commit increases when a Trusted Platform Module (TPM) is configured. [PR1738193](#)
- There must be at least 1 minute spacing between consecutive key rollovers. This includes key rollovers triggered by key chain, sak_key_interval, primary/fallback, packet count rollovers. [PR1739933](#)
- Given that JNP10K-PWR-AC3 has four inputs, it will be useful to provide the operating state information of the feed in Snmp. This is planned as an enhancement in future releases. [PR1742996](#)
- On MX Series platforms with MS-MPC/MS-DPC, when the system is busy in the creation/deletion of sessions results in the picd process crashes for executing the CLI command `show service sessions/flows` or `clear service sessions/flows` aggressively (executing CLI command in 5-10 secs iteration). [PR1743031](#)

- On MX10004 and MX10008 platforms, the DIP Switch - 15A or 20A does not get displayed in the CLI output. This is in line with the existing 5.5KW power supplies. The actual DIP switch has to be checked physically. [PR1744396](#)
- [TIMING BITS] - LOS alarm not generating when BITS is in LOS state. [PR1744419](#)
- Session synchronization is not working on standby even after replication-threshold timer (150 seconds) is complete with SRD configuration. [PR1744420](#)
- On MX10004, MX10008, and MX10016 routers, some enhanced fans is not working after hot-insertion of Fan Tray. [PR1745299](#)
- On all Junos OS platforms, due to timing issues the Packet Forwarding Engine and the Physical Interface Card (PIC) will be slow and services will face slowness issue and error message: 'Minor potential slow peers are: X' will be seen. This is rare timing issue. [PR1747077](#)
- On Junos using afeb/tfeb way of communication to PFE that is MX80/MX104 platforms with Virtual Router Redundancy Protocol (VRRP) configured, deleting a member link from the aggregated Ethernet (AE) bundle removes the VRRP filter entry in the Packet Forwarding Engine which causes VRRP traffic to get dropped even though other active member links in the aggregated Ethernet bundle exists. [PR1747289](#)
- On MX104 platform with MACSEC MIC, the per-unit-scheduler configuration on the MACSEC MIC interface results in the PFE crash leading to traffic impact. [PR1747532](#)
- On MX10000 platforms, when fan trays are removed, the chassisd log messages displays normal and when fans are running, it displays full speed. These log messages are incorrect and there is no functionality impact. [PR1753787](#)
- When you remove fantray, the SNMP logs message displays Fan Tray 0 Fan 0 in jnxContentsDescr instead of Fan Tray 0. However, the chassisd log message displays Fan TRAY 0 is absent, which is correct. SNMP code by design does not consider Fans Tray as a separate entity and is associated with the Fans. There is no separate OID for Fan Tray. Logs and SNMP Traps mislead the Fan Tray issues. [PR1753801](#)
- MX304 core-spmbpfe-bugatti-pvl-b1-node seen in re1. [PR1758480](#)
- SRv6 TE with logical-systems is not qualified in any release. [PR1760727](#)
- For certain releases, performing unified ISSU on MPC10 or MPC11 can generate an FPC core file. [PR1766307](#)
- Ability to track partially upgraded PSM is not available under the show system firmware command. This is due to current limitation of the show system firmware command. [PR1768500](#)

- Removing PEM FRU from the chassis during its firmware upgrade is currently not allowed due to firmware upgrade limitations, leading to undefined software behaviour in such situations. [PR1773895](#)
- When UPs are not connected, the user cannot delete a configured SGRP. [PR1774717](#)

Interfaces and Chassis

- You can configure the routing platform to track IPv6-specific packets and bytes passing through the router. To enable IPv6 accounting, include the route-accounting statement at the [edit forwarding-options family inet6] hierarchy level: [edit forwarding-options family inet6] route-accounting; By default, IPv6 accounting is disabled. If IPv6 accounting is enabled, it remains enabled after a reboot of the router. To view IPv6 statistics, issue the show interface statistics operational mode command. Can be found here: http://www.juniper.net/techpubs/en_US/junos10.4/topics/usage-guidelines/policy-configuring-ipv6-accounting.html [PR717316](#)
- The link aggregation group (LAG) member links may flap on all Junos OS platforms except MX Series when the configuration of any interface is changed or modified. The flap is not seen always. [PR1679952](#)

MPLS

- The default behavior of local reversion has changed from Junos OS Release 16.1 and that impacts the LSPs for which the ingress does not perform make-before-break. Junos OS does not perform make-before-break for no-cspf LSPs. [PR1401800](#)

Multicast

- Observed vglfpc core @__kernel_vsyscall,__GI___open_catalog. [PR1740390](#)

Network Management and Monitoring

- In some NAPT44 and NAT64 scenarios, duplicate SESSION_CLOSE Syslog will be seen. [PR1614358](#)

Platform and Infrastructure

- L2-Trans: pm_soam_frame_rx count is not incrementing as expected. [PR1729970](#)
- MVPN RVT MX EA cards: RVT interface traffic statistics are not proper [PR1755516](#)
- In EVPN Multi-Home AA scenario, random drops will be observed on the non-designated-forwarder for ARP-REPLY generated in response to ARP-REQ received for Virtual-Gateway-Address defined on IRB interface. [PR1772733](#)

Routing Protocols

- Certain BGP traceoption flags (for example, "open", "update", and "keepalive") might result in (trace) logging of debugging messages that do not fall within the specified traceoption category, which results in some unwanted BGP debug messages being logged to the BGP traceoption file. [PR1252294](#)
- On all Junos OS platforms and Junos OS Evolved with scaled BFD sessions, FPC reload/restart results in few BFD session flap. [PR1698373](#)
- BFD sessions bounce during unified ISSU if authentication is used. [PR1723992](#)
- openconfig-local-routing.yang from "1.0.0" to "2.0.0" in which this module is deprecated now. As we upgraded yang model for local-routes, it deprecated few xpaths that were previously supported: /local-routes/static-routes/static/ /local-routes/local-aggregates/aggregate/ [PR1735926](#)
- The set routing-instance *ri_name* protocols igmp-snooping for non-MX Series platforms like QFX series, EX series, ACX5K and all EVO platforms supporting snooping need to mandtorily pass vlan option for set routing-instance *ri_name* protocols igmp-snooping. The instance level snooping for these is supported using set routing-instance *ri_name* protocols igmp-snooping vlan all. [PR1736608](#)
- rpd core is generated in master Routing Engine @ block_id_free_unique_blk, block_id_free_unique_blk, rt_instance_delete_master_lsi_ifl_data. [PR1742915](#)
- There are streaming discrepancies for /adjacency-sids/adjacency-sid in /network-instances/network-instance/protocols/protocol/isis between Junos OS Releases 22.3R2-S1 and 20.X75-D51. There is a OC YANG version difference between the two releases and the OC YANG versions are not backwards compatible. The YANG version is tightly coupled with the release. [PR1750314](#)

Services Applications

- On Junos OS MX80, MX240, MX480, MX960 platforms, in an issue where an old dynamic security association_configuration (sa_cfg) with a different instance is present and trying to establish new sets of IPSec Security Association (IPSec SAs) using a new Internet Key Exchange security associations (IKE SA) established for the same remote device but with different instance. This can happen, if for some reason old sa_cfg is not cleaned (failed in clean-up). On crash, the Key Management Daemon (kmd) restarts but fails because of kernel instance mismatch present in the kernel database (DB). So all the IPsec tunnels will be impacted.[PR1771009](#)

Resolved Issues

IN THIS SECTION

- Class of Service (CoS) | 93
- EVPN | 93
- Forwarding and Sampling | 94
- General Routing | 94
- High Availability (HA) and Resiliency | 103
- Interfaces and Chassis | 103
- Junos Fusion Satellite Software | 104
- Junos XML API and Scripting | 104
- Layer 2 Ethernet Services | 104
- MPLS | 104
- Network Management and Monitoring | 105
- Platform and Infrastructure | 105
- Routing Policy and Firewall Filters | 106
- Routing Protocols | 107
- Services Applications | 109
- 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 CoS scheduler map will not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured on it [PR1734013](#)
- "load override" followed by ISSU will introduce incorrect class-of-service FC(Forwarding Class)-to-Q(queue) table mapping [PR1755540](#)
- Change in the cosd behaviour due to the CoS interface specific wildcards [PR1760817](#)

EVPN

- SRv6 locator change results in rpd crash [PR1724845](#)
- EVPN-VXLAN interconnection DCI forwarding problem was observed when one of the AGW IRB interfaces failed in data centers spine [PR1732414](#)
- While doing a migration from VPLS to EVPN, when any changes are done like FPC restart or device reboot, the crash is observed [PR1734686](#)
- After switchover EVPN-VPWS SID is not allocated [PR1735856](#)
- The rpd crash on EVPN VPWS environment [PR1738032](#)
- Evpn-vxlan comp nh is not installed in pfe after peer reboot [PR1739686](#)
- ARP/FIB are added even if IRB in EVPN is disabled [PR1743529](#)
- BGP NH resolution should happen using locator and without extra policy at egress. [PR1745991](#)
- The user will be unable to configure the interface having stacked outer VLAN and a list of inner VLANs [PR1746787](#)
- Intermittent packet loss can be observed in evpn-vpws local switching scenario [PR1747706](#)
- Re-ARP is not sent before MAC entry expires in EVPN environment on Junos OS MX Series platforms. [PR1751386](#)

- EVPN AD per EVI route might not carry SRv6 sid post GRES switchover. [PR1756536](#)
- MAC addresses programming failure resulting in traffic flooding [PR1758677](#)
- The rpd can crash on all Junos platforms in Seamless DCI scenario [PR1761852](#)
- [EVPN/MPLS] Color related LSPs for next-hop will disappear from EVPN routes on mpls.0 routing-table by changing 'fallback none' option in 'transport-class' config. [PR1764126](#)
- Migrating from L2 Circuit to EVPN results in rpd crash. [PR1767914](#)
- In EVPN-VXLAN scenario, arp flag may not be set properly due to mac-ip entry age out not handled properly. [PR1773734](#)

Forwarding and Sampling

- Traffic not hitting the policer after configuring macroflow filter [PR1718147](#)
- FPC cards restart unexpectedly [PR1743032](#)
- High CPU utilization of the mib2d process will be observed with error messages due to stale SNMP requests [PR1749092](#)
- Traffic loss observed when using ingress-queuing-filter on non zero PFE interface [PR1751494](#)

General Routing

- The mustd process may crash on all platforms [PR1562848](#)
- Inter vlan ipv6 traffic loss for some hosts after configuration remove and restore. [PR1629345](#)
- Delegated BFD sessions configured on routing-instance may fail to come up [PR1633395](#)
- Continuous error logs and Telemetry data might not be populated [PR1661423](#)
- Telemetry data is not being captured [PR1666714](#)
- 22.3TOT :: IFL packet counters not working on show AMS interface extensive for sub interfaces [PR1673337](#)
- LC9600 line card not booting-up [BIOS corruption]. [PR1677757](#)

- A new command has been introduced that will display the differences between the destroute entries learned within l2ald and present in the kernel [PR1677996](#)
- The PFE will get disabled for underrun cmerrors observed when traffic ingressing over the AF interface [PR1681428](#)
- xml validation failure seen for "show security macsec connections | display xml validate" with ERROR: Duplicate data element [PR1691435](#)
- MFT: RPD may restart during Multi-Feature-Test with BGP-MP, L3VPN/L2VPN, over RSVP/LDP transport, as well as colored SRTE, and SRv6 tunnel transport along with BGP CT. [PR1699773](#)
- EX4400: pps counter does not show correct values for jubmo frames [PR1700309](#)
- Alarms for PEMs are still seen when PEM are removed from the chassis [PR1703566](#)
- Link is not going down physically while disabling the l2circuit configured interface on Junos based ACX5448 platform [PR1703935](#)
- Interface flaps are seen after PTP GM changes to a different FPC slot [PR1704633](#)
- Next Hop counts are not as expected. [PR1710274](#)
- The dcpe process will crash due to memory fragmentation. [PR1711860](#)
- The agentd would become unresponsive on all Junos platforms [PR1715377](#)
- Inconsistent RPD crash found in rt_walk, task_job_run_job_bg, task_scheduler [PR1715599](#)
- BMP station will not receive the RIBs as expected [PR1715886](#)
- Same MAC address is assigned to cbp and physical interfaces instead of being unique on MX304 [PR1719084](#)
- The subscribers will be stuck in a terminated state when an FPC is taken offline [PR1719427](#)
- The evo-aftmand-bt process may restart when an app exit [PR1719739](#)
- Continuous messages indicating duplicate IP address L2ALM_DUPLICATE_IP_ADDR will be seen in MCLAG and VRRP scenario [PR1719868](#)
- Removing a PEM that doesn't have power feed does not generate the SNMP TRAP for "Power Supply Removed" [PR1719915](#)
- The ES-IS route is not getting installed in the (instance-name).iso.0 routing table. [PR1720303](#)
- Reachability loss between Master and backup Routing Engine in certain condition on MX2008 platform [PR1720407](#)

- The bbe-statsd process crash is observed on the backup Routing Engine immediate after GRES was disabled [PR1720978](#)
- MFT : "no-reduced-srh" SRV6 encap mode is not working as expected on MX304. [PR1721404](#)
- L2alm sends IPv6 NS with IRB link local address even though target IP is global address [PR1722102](#)
- BNG CUPS Controller: authd core after enabling a configured SGRP and subscriber-group-default-tags [PR1722802](#)
- The FPC crash is observed on Junos MX10008 platform when connected to non-Juniper SFP [PR1722823](#)
- PADT response will not be sent for an incoming PPPoE/PPP data Packet from an unknown session ID [PR1722945](#)
- PS interface remains up while LT or RLT interface is down [PR1724298](#)
- Help string "Display information for a specified VLAN" is changed to "Display information for a specified bridge domain" [PR1724489](#)
- gNMI native Junos configuration push commit fails if configuration has special character [PR1724746](#)
- Memory initialization and scrub operation using PFE's fails [PR1724841](#)
- The entPhysicalSoftwareRev MIB object returns Junos OS version value for components which do not run Junos OS [PR1725078](#)
- The "show network-access address-assignment address-pool-manager status command" reports APM not connected when in fact it is connected [PR1725143](#)
- The error logs "fpc0 expr_hostbound_packet_handler: Receive pe 254?" would be generated [PR1725716](#)
- Root user is unable to login using public key authentication after reboot or upgrade [PR1726621](#)
- Upgrading the i40e NVM Firmware on Routing Engines with VM Host Support [PR1726775](#)
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning is configured [PR1727119](#)
- "/lib/systemd/system/docker.socket is marked executable" logs flood after system reboot . [PR1727524](#)
- On all Junos and Junos Evolved platforms the l2ald process memory usage is seen to increase over time. [PR1727954](#)
- A panic reboot will be observed due to deadlock on VMhost platforms. [PR1727985](#)

- DHCP subscribers are stuck in DHCP-renew state when 'overrides always-write-giaddr' is enabled. [PR1729913](#)
- MX304 Major Alarm "Host 0 detected AER correctable error" after Routing Engine switchover. [PR1731237](#)
- IPv6 to IPv4 translation is not happening for traceroutev6 traffic. [PR1731341](#)
- Auto-sw-sync doesn't trigger upgrade/restart of rRouting Engine. [PR1731877](#)
- Traffic drop will be observed when RIPv2 is enabled on IPv4 interface. [PR1732673](#)
- The xmlproxyd crash might be observed when there are multiple collectors [PR1732763](#)
- Error logs are seen with a non-vxlan dot1x enabled port [PR1733365](#)
- 23.2R1 :USF_DNSF:log messages are not generated when Sending MX query with domain name in black list with action as report after configure the web filtering with one/more profile and template. [PR1733435](#)
- In TCP flow, the initial SYN+ACK packet will not be marked with specified CoS related action on Junos Evolved platforms [PR1733509](#)
- Traffic loss is seen when "larp force-up" knob is configured [PR1733543](#)
- PTP will get stuck in acquiring state which leads to improper time synchronization after system reboot [PR1734235](#)
- Script is failing when trying to verify Radius ngs_pppoev4_dynamic accounting stop stats [PR1734608](#)
- Junos OS: jkdsd crash due to multiple telemetry requests (CVE-2023-44188) [PR1734718](#)
- The bbe-smgd crash can be seen in a certain scenario [PR1735560](#)
- Control plane flap, data drop, unexpected behavior of PFE or device is observed when file storage is impacted in a continuous ksyncd process crash scenario [PR1735685](#)
- Crash on all Junos VMhost platforms due to deadlock panic [PR1735843](#)
- Junos OS: EX Series: A PHP vulnerability in J-Web allows an unauthenticated attacker to control important environment variables (CVE-2023-36844) [PR1736937](#)
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario [PR1736954](#)
- MAPT : ICMP Response not coming properly for downstream traceroute UDP traffic [PR1736972](#)
- The CLI command "show class-of-service classifier" hangs intermittently [PR1737009](#)
- BGP sessions flap due to license updates [PR1737035](#)

- The traffic blackhole will be observed when the SRTE shortcut is configured [PR1737119](#)
- Traffic drop can be seen in the MPLS traffic Engineering scenario [PR1737594](#)
- URL-Filtering few HTTP sites are getting bypassed and redirect is not happening [PR1737670](#)
- Junos OS installation using USB can fail on SRX4600 [PR1737721](#)
- PSoRLT Aggregate Stats: ipv4 leaf elements for ps transport ifl are exported , since ps is I2 interface no stats under ipv4 should be exported, [PR1737935](#)
- After picd restart, traffic was not recovered on MACsec enabled ports [PR1738038](#)
- JV DB is missing leaf: /interfaces/interface[name='ae0']/state/counters/out-octets, out-pkts, out-unicast-pkts, out-broadcast-pkts, out-multicast-pkts, in-errors, out-errors, in-discards ,out-discards ,in-pause-pkts, out-pause-pkts [PR1738395](#)
- VC case not handled properly while calling brcm_vxlan_port_discard_set api. [PR1738404](#)
- PTP time sync issues after release upgrade or rebooting the device. [PR1738458](#)
- DHCP offer is dropped at MX and specific EX platforms when an It interface is used as the transport. [PR1738548](#)
- An rpd crash will be observed due to inconsistency between rpd and kernel. [PR1738820](#)
- The interface goes down and the error message floods due to the FD leak in the picd process. [PR1738854](#)
- with multiple reboot srx300 going into panic: sleeping thread. [PR1739219](#)
- The ksyncd process crash would be seen on backup Routing Engine. [PR1739258](#)
- Installation of third party package on one Routing Engine and using auto-sync to add another Routing Engine into the dual Routing Engine setup might result in app not starting on the later inserting Routing Engine [PR1739286](#)
- Memory leak in PKID. [PR1739342](#)
- FPC generates a core file and crashes in a race condition. [PR1739595](#)
- Duplicate BUM traffic is observed after the WAN interface flaps in the EVPN-VXLAN multihomed DC scenario [PR1739632](#)
- FTC X FTC FPGA minimum supported firmware version mismatch alarm raised by OIR FTC [PR1739842](#)
- Major alarms will be observed on the FPC when ALB is enabled under aggregated Ethernet interface. [PR1739854](#)

- FPC crashes and remains offline after the upgrade of RE BIOS to 0.15.1 version [PR1739922](#)
- Layer 2 traffic will be dropped on VSTP disabled interface [PR1739975](#)
- Traffic loss is seen due to anomalies after the recreation of IFLs [PR1740561](#)
- System not bootable after request system zeroize [PR1740989](#)
- The traffic drop is observed due to the MAC source address being learned from the incorrect direction. [PR1741316](#)
- The BGP routes gets stuck in BMP withdraw state [PR1741732](#)
- Fans may stop working after removal and insertion of Fan Tray [PR1742174](#)
- SPMB process will crash and PICs will not come online [PR1742186](#)
- Tunnel interfaces are getting bounced causing a momentary impact on traffic [PR1742510](#)
- Race condition where FLOOD ROUTE DEL event can cause l2ald crash. [PR1742613](#)
- Traffic verification failed for DHCPv6 relay. [PR1743087](#)
- The l2ald crashes when there is recursive deletion of IFBD or when BGP neighborship is cleared in EVPN-VXLAN multi-homed configuration [PR1743282](#)
- FTI interface status (up/down) does not sync between master and backup Routing Engine. [PR1743306](#)
- The chassisd crash is observed on Junos MX204 platforms due to Fabric request timeout [PR1743379](#)
- pppoe subscriber over PS ifd over rlt, when rlt mode change between active-active to active-backup, core ->subscriber direction, forwarding path uses the wrong Unilist aft node. [PR1743515](#)
- After this PR fix, to enable the xSTP support in ephemeral DB, below config command needs to be used: "set protocols layer2-control ephemeral-db-support" [PR1743632](#)
- Due to SPMB restarts in the middle of the FPC boot process, FPC wont come up [PR1743686](#)
- The switch-options settings on the logical-system will be not reflected after Routing Engine rebooting or Routing Engine switchover [PR1743737](#)
- If more than 32 vlan ranges are configured under the dynamic-profile then login issue and traffic impact can be seen with subscribers of random VLANs [PR1743903](#)
- Traffic drop is observed after the addition or removal of the "filter-specific" knob under the policer [PR1743930](#)

- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device [PR1743978](#)
- [USF - SPC3 - LOGGING] "log-tag" is not populated in the cgnat syslogs intermittently [PR1744563](#)
- With multiple Traffic Selectors having same remote-ip, the traffic works only for first tunnel on MX Series platforms with SPC3 cards. [PR1744601](#)
- 100G interfaces will flap due to Routing Engine switchover on Junos MX platforms with MPC3E-3D-NG/MPC-3E-3D-NG-Q linecards. [PR1744883](#)
- Enhancement of PoE controller firmware files into Junos OS Software. [PR1745088](#)
- Fans may stop working after removal and insertion of Fan Tray [PR1745299](#)
- MPC10E - PIC bounce/config change on a PIC with 10G QSA adaptor can cause a FPC restart [PR1745317](#)
- Packet drops may be seen in the "show network-agent statistics detail" CLI output when subscribing to sensors using gRPC [PR1745451](#)
- rpd core at #2 0x00007f9b2512742c in __assert_fail_base (fmt=0x7f9b2528bae8 "%s%s%s:%u: %s %sAssertion `%s' failed.\n%n", assertion=0x55be37507a48 "nh_idx_t_getval(nhid) == nh_idx_t_getval(rt_nexthops_nhid(rtnh))", file=0x55be375077e8 "../..../src/layer3/usr.sbin/rpd/lib/krt/common/krt_ack.c", line=1306, function=optimized out) at assert.c:92 [PR1745509](#)
- The hwdre application restarted due to memory leak [PR1745749](#)
- The rpd crashes when BGP sharding, multipath and dynamic tunnel are configured [PR1746012](#)
- Node-segment reachability will be lost in Multitopology based IS-IS [PR1746304](#)
- MPC10E line card crashes when it reboots after FPC firmware upgrade [PR1746541](#)
- traffic degradation in 25% down might be seen under high load traffic at srx4600 with fpga v1.65 [PR1746567](#)
- PTP master feature will not work as expected [PR1746984](#)
- Traffic from subscribers will be dropped by Junos based MX platforms [PR1747009](#)
- MX204 - INLINE NAT - address-prefix any-ipv4 reporting wrong. [PR1747483](#)
- Control board is stuck in Present state [PR1747567](#)
- MX2k Platform: frequent fabric plane Check state reported due to remote destination timeouts [PR1747893](#)
- The memory consumption increases due to memory leak [PR1747992](#)

- The rpd process shuts down on all Junos OS and Junos OS Evolved platforms. [PR1749252](#)
- Connectivity fails intermittently on 802.1x enabled ports. [PR1749312](#)
- Packet Forwarding Engine Flow ID doesn't show correct in show subscriber extensive output. [PR1749336](#)
- Router crashes if routing services over PS are configured [PR1749748](#)
- The authentication algorithm hmac-sha-256-128 for IPsec SA is not working and causing interoperability issues between Junos Evolved platforms and other devices [PR1749779](#)
- IRB interface state remains up on local-remote option on all platforms along with EVPN-VxLAN configuration [PR1750146](#)
- SyncE stuck in holdover upon PTP slot switchover without change in PTP phase align state [PR1750316](#)
- MX304: ssh is not enabled by default. [PR1750596](#)
- Transferring or receiving traffic is impacted for SPC3 CPU cores connected to the affected PCIe bus when the SPC3 card boots up. [PR1750634](#)
- The mspmand daemon crashes causing traffic loss. [PR1750823](#)
- The Packet Forwarding Engine process crashed while removing and applying the firewall filters. [PR1750828](#)
- MPC10E: Support of G.8275.1 PTP Hybrid mode with speed 25G and 400G [PR1750885](#)
- ARP learning issue for dynamic ARP entry for the DVLAN stacked frame route not resolved [PR1751656](#)
- Traffic loss with preserve-nexthop-hierarchy enabled on MX platforms with a combination of MPC1-9, LC480, LC2101, and MPC10E, MPC11E, LC9600 line cards [PR1751699](#)
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on L2 ports [PR1751700](#)
- FPC reboots observed during ISSU on MX10008 and MX10016 resulting in ISSU being unsuccessful [PR1751785](#)
- Service PIC enabled with url-filtering may crash and gets into booting loop [PR1751860](#)
- The mspmand process crashes when MPLS VRF Route table is not present for a MPLS route and MPLS route is deleted [PR1752132](#)
- Firmware upgrade will fail, if "set system services ssh root-login deny" knob is present in configuration [PR1752765](#)

- Port et-0/0/4 and xe-0/0/5:0 can not be up at the same when port 4 is configured as 100g and port 5 is configured as 1x10G on MX304 [PR1752831](#)
- MPC11E suddenly goes offline due to power failure causing multitude fabric stream drain failures on all other MPC11 [PR1753374](#)
- FPC reboot can cause a crash while UDP streaming of packet usage sensor path [PR1753394](#)
- PIM neighborship, or other control protocols flaps due to host-bound queue (Q3) congestion [PR1753853](#)
- Incorrect egress encapsulation corrupting packets of IRB interface on MPC10E with MXVC results in traffic loss [PR1753951](#)
- Traffic impact will be seen for static VoIP VLAN on access interface if same VLAN configured as data VLAN [PR1754474](#)
- "set services evpn global-parameters virtual-gateway v6-mac" is broken [PR1754493](#)
- The interface stats interrupt may be lost resulting in stats not getting updated [PR1755161](#)
- Users authenticated via captive portal experience a noticeable delay of atleast 2-5 mins [PR1755593](#)
- Continuous fpc0-aftd-trio coredump on MX304 when turning up ipv6 neighbors with LMIC 2 [PR1755950](#)
- High CPU utilization observed after a few days of operation when BGP RIB sharding is enabled. [PR1765417](#)
- HMC errors will be observed on Junos platforms with LC480 [PR1756780](#)
- Prolonged SNMP polling leads to kernel crash in SCU/DCU scenario [PR1767098](#)
- macsec license get cleared on master member post nssu/reboot [PR1757835](#)
- Interface using QSA adapter with 1G speed wont work after upgrade to Junos OS 21.4R3-S4.9 [PR1757878](#)
- MX10008 :: LC2101 :: PLD is higher than 2000 msec on ungraceful removal of a Fabric board [PR1758348](#)
- mcsnoopd process generates a core file with EVPN-MPLS and VPLS with multicast configuration. [PR1758659](#)
- The remote end of the link goes down on JNP10K-LC480 line card after unified ISSU [PR1758764](#)
- On JNP10K-LC9600, shared-bandwidth-policer may be loaded into irrelevant Packet Forwarding Engine depending on choice of member port of aggregated Ethernet. [PR1758935](#)

- AFTD crash while rollback/config delete [PR1759899](#)
- RPD process crash is seen post Routing Engine switchover [PR1759991](#)
- On Junos OS and Junos OS Evolved platforms the rpd crashed abnormally and later chassisd crashed as well [PR1761667](#)
- LLDP neighborship will not be formed on all Junos devices [PR1763053](#)
- BFD session detection time is higher than expected leading to traffic drop [PR1763667](#)
- Interface flaps leading to PFE crash due to FPC heap corruption [PR1764083](#)
- High RPD CPU due to BMP station config [PR1764911](#)
- A warning message is seen while installing a license key with an unknown feature. [PR1766515](#)
- PFE component of /interfaces/interface/subinterfaces/subinterface/state/ sensor may send data with frequency higher than requested by collector. [PR1772266](#)
- MX2K | SFB2 | MPC8E | FI: Reorder cell timeout | FI: Cell underflow | FI: Cell jump drop error. [PR1774558](#)
- After the device reboot the interested clients will not be able to receive the inactive routes [PR1774975](#)
- JNP10K-PWR-AC3 PSM on MX10004 and MX10008 platforms display snmp mib walk jnxFruTemp updating just inlet TEMP sensor. Updating all supported temperature sensors is necessary. [PR1775383](#)
- In the BNG CUPS system after GRES subscribers will fail to login. [PR1775539](#)

High Availability (HA) and Resiliency

- The traffic drop is observed during the graceful restart on Junos OS and Junos OS Evolved platforms. [PR1727957](#)

Interfaces and Chassis

- Physical link remains stuck in down state on certain MX Series platforms [PR1707707](#)
- Traffic impact will be seen with mismatched speeds on the LAG interface and member interface [PR1725168](#)

- The lt/vt/ut interfaces may not recover from the disable-pfe (admin down) state if the GRES switchover is done before restarting FPC [PR1731190](#)
- Changing speed and adding to aggregated Ethernet in the same commit fails [PR1743461](#)
- Out of range "Near-end loss" percentage or jnxSoamLmCurrentStatsBackwardAvgFlr [PR1754637](#)
- High memory utilization is observed on all Junos OS platforms [PR1757801](#)
- Backup Routing Engine reset followed by Master Routing Engine reset traffic loss will be observed on aggregated Ethernet links. [PR1767397](#)

Junos Fusion Satellite Software

- Junos Fusion Satellite device will be stuck in the SyncWait state [PR1733558](#)

Junos XML API and Scripting

- Junos OS platform device unable to commit configuration in recovery mode [PR1717425](#)
- OpenConfig data obtained with gNMI GetRequest in json format displays module prefix [PR1736286](#)

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only) [PR1722082](#)
- DHCP ALQ no-advertise-routes-on-backup functionality does not work in VRF for Framed-Route. [PR1740822](#)
- Active bulk leasequery is not working for IPv6 DHCP local server on MX Series platforms [PR1744162](#)

MPLS

- Static MPLS LSP (transit) stats are not incrementing post the rpd restart [PR1719162](#)

- LDP sync not complete with NSR (stuck at Inprogress forever) when "protocols ldp strict-targeted-hellos" is enabled when LDP signalled VPLS is configured [PR1725519](#)
- Traffic silently drops because of an additional label when CCNH is toggled [PR1738774](#)
- LSP with auto bandwidth enabled is not updating its Max AvgBW value, preventing the LSP from being resized [PR1740226](#)
- rpd crash observed during Routing Engine switchover or Route Convergence [PR1747365](#)
- In-place-lsp-update failure causing ungraceful tear down of LSP [PR1756096](#)
- Memory exhaustion leading to FPC core with auto-policing enabled MPLS with Multicast P2MP [PR1757984](#)
- After the switchover, auto-bandwidth functionality does not work and LSPs do not get adjusted according to the traffic in the network [PR1772634](#)

Network Management and Monitoring

- Syslog filter not functioning with generating /etc/syslog.conf+ file after syslog config is deactivated and re-activated [PR1726925](#)
- The mgd process crash is observed in VMhost platforms during system reboot [PR1732379](#)
- Syslog messages modification for SNMPv3 authentication failure [PR1734549](#)

Platform and Infrastructure

- VRRP does not work when a firewall filter is configured to accept VRRP packets with a TTL value of 255 [PR1701874](#)
- Remote EVPN router is not receiving ARP packets for double-tag VLAN when sender is sent a packet from MPC10 and MPC11 line card [PR1718372](#)
- ksyncd core with dhcp subscribers [PR1722708](#)
- VPLS traffic gets blackholed by qualified-bum-pruning mode [PR1731564](#)
- Heap memory leak on MPCs used for subscriber termination. [PR1732690](#)
- Intermittent flooding of traffic every 40 sec [PR1736667](#)

- The CoS rewrite rules will not be working in the EVPN with IRB scenario [PR1736890](#)
- MPC1 to MPC13E/LC2101,LC2103,LC480/T4000-FPC5/MPC built-in Trio based line card reboots when subscriber management services are configured [PR1737615](#)
- Host communication does not work in EVPN-L2VPN-CCC setup [PR1740606](#)
- Inline-monitoring will not work as expected when more than one instances are configured [PR1742123](#)
- PFE will wedge for RVTEP connectivity having unilist VENH [PR1743947](#)
- show system connections and show-routing-instances reports all routing-instances as unknown. [PR1746779](#)
- PSoRLT telemetry | UDP | oc path /qos/interfaces/interface/output/queues/queue/state/ is not exporting results for ps IFL and It interfaces | UDP sensor will be using different yang and there was a missing dr:source for a container which impacted the streaming in UDP. [PR1750995](#)
- [MX480/MX240] Multicast ping ff02::1 cannot perform reply on MX240/480 platform from MX204 via VXLAN [PR1751846](#)
- The ksyncd process crashes with replication error after performing restart routing [PR1752151](#)
- TCP window scaling may be not applied to the first TCP packet sent to the client after the three-way handshake, leading to unnecessary segmentation. [PR1761242](#)
- Routing protocol session down with native VLAN configuration on MX Series platforms [PR1763706](#)
- core-dump-AFEB core happened with heap high [PR1770750](#)
- In EVPN-MPLS Multi-Home Active/Active scenario, random packet drops observed. [PR1772733](#)
- Cos queueing issue with tunnel interface when HCOS hierarchy is configured on it [PR1772826](#)

Routing Policy and Firewall Filters

- The static routes are installed in the routing table even though interface routes are not present. [PR1714163](#)
- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration [PR1744449](#)

Routing Protocols

- The mscnood process crash will be observed when snooping configuration is removed [PR1696374](#)
- Junos OS and Junos OS Evolved: A crafted BGP UPDATE message allows a remote attacker to de-peer (reset) BGP sessions (CVE-2023-4481) [PR1709837](#)
- The PE advertises incorrect next-hop towards CE although BGP export policy configured with next-hop under policy-statement [PR1712527](#)
- The RPD process will be stuck at a high CPU when OSPF areas are configured at a high scale and after starting the protocol [PR1728573](#)
- Traffic impact is seen when there is a single peer in the proxy BGP group connected to the BGP route reflector [PR1728604](#)
- BMP leads to prolonged high rpd CPU utilization upon committing the BGP peer import policy configuration [PR1729733](#)
- The rpd process will crash in a scaled BGP setup with traceoptions configured [PR1732087](#)
- IP-IP tunnel traffic drop is seen when "preserve-nexthop-hierarchy" knob is enabled [PR1733803](#)
- Enabling bgp traceoptions flags will log frequently to the trace file. [PR1735189](#)
- RPD crash when attempting to send a very long AS PATH to a non-4-byte-AS capable BGP neighbor (CVE-2023-44186) [PR1736029](#)
- commit FAILs when more than one locators are configured with same prefix. [PR1736746](#)
- The rpd crash files are seen due to a use-after free of objects [PR1737679](#)
- OSPFv3 using the VIP address on the IRB interface will not form adjacencies between peers [PR1737978](#)
- BFD session for BGP remains down in a specific scenario [PR1738074](#)
- RPD crashes when multiple ISIS processes are configured [PR1738222](#)
- Traffic loss will be seen in IPv6 only IS-IS topologies [PR1738901](#)
- The rpd process crash will be observed when the prefix-limit exceeds on the backup Routing Engine [PR1739335](#)
- The IPv6 link local based BFD session over an AE interface will be stuck in Init state [PR1739860](#)
- Error message for mld static group configuration is not proper. [PR1741370](#)

- Memory leak observed when reconfiguring the flow routes [PR1742147](#)
- Partial application of BGP import policy with BMP configuration and after back-to-back commits changes BGP import policy [PR1742222](#)
- RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer [PR1742416](#)
- When BGP is configured in routing-instance of type virtual-router, default MPLS table is being created for that virtual-router, unexpectedly [PR1742513](#)
- CPU in rpd spikes and scheduler slips will be observed when the duplicate community is added [PR1745073](#)
- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE [PR1746439](#)
- Stale IP prefixes when issuing "show isis route flex-algorithm-id" [PR1746557](#)
- With RIB sharding configuration upon rpd restart the rpd crash will be observed [PR1748152](#)
- Multi-instance isis route leaking for inet.3 is not working as expected [PR1748223](#)
- The device will not be reachable over the loopback interface for the IS-IS nodes even though the neighborhood may exist [PR1749850](#)
- RPD may crash when deactivate protocol ISIS [PR1751210](#)
- ISIS export policy does not export all default routes (IPv6 and IPv4) from BGP (or any other protocol) [PR1751371](#)
- Traffic drop is seen if chained-composite-next-hop is turned on for Segment Routing [PR1752551](#)
- Deletion of routing-instance with 3K paths per prefix takes a long time with the rpd CPU usage at 100% [PR1752594](#)
- The rpd crashes on all Junos and Junos Evolved platforms with IS-IS, segment routing and flex algo configured [PR1753003](#)
- The BFD process crash will be observed when telemetry is used [PR1754535](#)
- BGP multipath route is not correctly applied after changing the IGP metric [PR1754935](#)
- The BGP LU labels can have next-hops pointing to each other in multi-homed PE setup [PR1760885](#)
- Memory spike will be observed on the system with BFD enabled for OSPF/ISIS [PR1761232](#)
- The rpd process crashes after clearing ISIS database or restarting the rpd process. [PR1759728](#)

- An rpd crash is observed when mvpn-mode is configured as "rpt-spt" and multicast snooping is enabled. [PR1769782](#)

Services Applications

- L2TP tunnels may time out if creation of bbe-smgd core dump takes a long time. [PR1720994](#)
- Crash file is generated when local certificate keychain is missed repeatedly [PR1728605](#)

Subscriber Access Management

- Potential memory leak in authd process [PR1729035](#)
- Test aaa command may failure due to "Subscriber creation failed" [PR1759048](#)
- BNG Dynamic Pools JUNOS 22.4R3: Algorithm to determine prefix count for apportionment requests to APM is over aggressive [PR1768651](#)

User Interface and Configuration

- After the device reboot BGP sessions configured with authentication will be down [PR1726731](#)
- The 'load replace' operation might result in mustd and mgd crash. [PR1740289](#)
- Attribute GLOBALIPOWNER doesn't exist is reported on primary Routing Engine when commit synchronizes to secondary Routing Engine. [PR1741284](#)
- The `commit confirm` and `commit race condition` commands crashes the firewall functionality. [PR1743038](#)
- The mgd process crash is observed when 'show' is executed from the configuration mode [PR1745565](#)
- Subsequent commits hang will be seen, when transfer-on-commit fails [PR1752374](#)

VPNs

- In MPLS-L2VPN/BGP-VPLS setup the flow-label route update is not propagating to neighbouring devices [PR1751717](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Basic Procedure for Upgrading to Release 23.4R1 | 111](#)
- [Procedure to Upgrade to FreeBSD 11.x-Based Junos OS | 111](#)
- [Procedure to Upgrade to FreeBSD 6.x-Based Junos OS | 114](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 116](#)
- [Upgrading a Router with Redundant Routing Engines | 117](#)
- [Downgrading from Release 23.4R1 | 117](#)

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

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

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

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

Basic Procedure for Upgrading to Release 23.4R1



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

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

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

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

Procedure to Upgrade to FreeBSD 11.x-Based Junos OS

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

To download and install FreeBSD 11.x-based Junos OS:

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

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



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

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-32-23.4R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-23.4R1.9-signed.tgz
```

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

- For 32-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-32-23.4R1.x-limited.tgz
```

- For 64-bit Routing Engine version:

```
user@host> request system software add no-validate reboot source/junos-install-mx-
x86-64-23.4R1.9-limited.tgz
```

Replace source with one of the following values:

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

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

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

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

Rebooting occurs only if the upgrade is successful.



NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).
- Starting in Junos OS Release 23.4R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
 - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

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



NOTE: After you install a Junos OS Release 23.4R1 `jinstall` package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add no-validate` command and specify the `jinstall` package that corresponds to the previously installed software.



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

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

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

To download and install FreeBSD 6.x-based Junos OS:

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



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

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

```
user@host> request system software add validate reboot source/jinstall-ppc-23.4R1.9-
signed.tgz
```

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

```
user@host> request system software add validate reboot source/jinstall-ppc-23.4R1.9-
limited-signed.tgz
```

Replace source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.



NOTE: After you install a Junos OS Release 23.4R1 jinstall package, you cannot return to the previously installed software by issuing the request system software rollback command. Instead, you must issue the request system software add validate command and specify the jinstall package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, EOL and EEOL:

- 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](#).

Upgrading a Router with Redundant Routing Engines

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

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

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

Downgrading from Release 23.4R1

To downgrade from Release 23.4R1 to another supported release, follow the procedure for upgrading, but replace the 23.4R1 jinstall package with one that corresponds to the appropriate release.



NOTE: You cannot downgrade more than three releases.

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

Junos OS Release Notes for NFX Series

IN THIS SECTION

- [What's New | 118](#)
- [What's Changed | 120](#)
- [Known Limitations | 120](#)

- [Open Issues | 121](#)
- [Resolved Issues | 122](#)
- [Migration, Upgrade, and Downgrade Instructions | 123](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 118](#)
- [Class of Service | 119](#)
- [Flow-based and Packet-based Processing | 119](#)
- [Software Installation and Upgrade | 119](#)

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

To view features supported on the NFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R1, click the Group by Release link. You can collapse and expand the list as needed.

- [NFX150](#)
- [NFX250](#)
- [NFX350](#)

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Support for firewall users log off, custom logo and banner (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, firewall users can log off using the logoff button displayed in captive portal after a successful login.

SRX and NFX administrators can set custom logo for captive portal. SRX and NFX administrators can configure custom login-success, login-fail banner messages in captive-portal. You can configure logo option under `set access firewall-authentication web-authentication hierarchy level` for custom-logo. You can configure banner option under `set access firewall-authentication web-authentication hierarchy level` for banner messages.

[See [firewall-authentication](#).]

- **Support for client/server certificate validation using TLS protocol mutual authentication (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, a client can authenticate without password based on client/server certificate validation using Mutual-TLS authentication. You can configure `mtls-profile` option at the `set security firewall-authentication hierarchy level`.

[See [firewall-authentication \(Security\)](#).]

Class of Service

- **Routing-instance based classification (SRX1500, SRX4100, SRX4200, SRX4600, vSRX3.0, NFX 150, NFX250, NFX350)**—Starting in Junos OS Release 23.4R1, SRX1500, SRX4100, SRX4200, SRX4600, vSRX3.0, NFX150, NFX250, and NFX350 Firewalls support routing-instance based classification. You use routing instance-based classifiers to classify packets based on the virtual routing and forwarding (VRF) of incoming packets. For routing instances with VRF table labels enabled, you can apply a custom MPLS EXP, DSCP, or IEEE802.1 classifier to the routing instance.

[See [classifiers \(Routing Instance\)](#).]

Flow-based and Packet-based Processing

- **Support drop-flow to prevent security attack - (SRX Series Firewall, vSRX3.0, cSRX, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, we support a new feature drop-flow to prevent security attack. You can control and limit the number of max-session for the drop-flow. The session in the drop-flow is valid for 4 seconds by default. During a drop-flow, the session state displays as Drop, but in the flow, the state remains as Valid.

The drop-flow feature is enabled by default. To disable the feature, use the `set security flow drop-flow max-sessions 0` command. To delete only the drop-flow feature, use the `run clear security flow session drop-flow` command.

To view the current drop-flow configuration, use the `show security flow drop-flow` command, and the view all the available drop-flow, use the `show security flow session drop-flow` command.

[See [Flow Based Session](#).]

Software Installation and Upgrade

- **Migration of Linux OS version (NFX Series)**—

Starting in Junos OS Release 23.4R1, the NFX150, NFX250, and the NFX350 platforms support Wind River Linux LTS19 . The updated versions are as follows:

- Open vSwitch—version 2.11.0
- DPDK—version 18.11.2
- libvirt—version 5.5.0

What's Changed

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

Known Limitations

IN THIS SECTION

- [General Routing | 120](#)
- [Virtual Network Functions \(VNFs\) | 121](#)

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

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

General Routing

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

As a workaround, upgrade both the partitions with same image versions [PR1753117](#).

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](#)

Open Issues

IN THIS SECTION

- [General Routing](#) | [121](#)
- [VPNs](#) | [121](#)

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

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

General Routing

- On NFX350 platforms, dcpfe core is seen with `show chassis fpc pic-status` command. We recommend not to use this command for Junos OS Release 23.1R1 [PR1705697](#).

VPNs

- On NFX250 platforms, IKED fails to install when you execute the command `request vmhost software add optional junos-ike.tgz` [PR1718048](#).

Resolved Issues

IN THIS SECTION

- [Flow-Based and Packet-Based Processing](#) | 122
- [Interfaces](#) | 122
- [VPNs](#) | 123
- [VNFs](#) | 123

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.

Flow-Based and Packet-Based Processing

- High latency and packet drops will be observed with the "transmit-rate exact" knob enabled for one or more schedulers of an IFL/IFD. [PR1692559](#).

Interfaces

- 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](#).
- When issuing request support information, there was a syntax error when looking at the nfx-back-plane (was nfx-backplane, instead of nfx-back-plane) [PR1720228](#).
- On Junos NFX350 Platforms, if you disable any RJ-45 interface through configuration, auto-negotiation at the MAC (Media Access Control) level on the remaining ports of the group of 4 ports (either 0-3 or 4-7) is disabled, resulting in traffic disruption. The impact is confined to the group of ports on which the port is disabled and the other group is not affected [PR1731242](#).

VPNs

- IPsec tunnel is down if IKE external-interface is configured with IPv4 and IPv6 address.

As a workaround, specify the local-address inside the ike gateway object if the configured external-interface contains both IPv4 and IPv6 address hosted on it. [PR1716697](#).

VNFs

- On Junos NFX350 Platforms, in spite of disabling the Auto Negotiation (AN) on the interface through configuration, it stays enabled on the copper ports. This could result in mismatch of AN settings with the remote side configuration and disrupt traffic. [PR1719973](#).

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases](#) | 123
- [Basic Procedure for Upgrading to Release 23.4](#) | 124

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



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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, 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](#).

For more information on EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

Basic Procedure for Upgrading to Release 23.4

When upgrading or downgrading Junos OS, use the `jinstall` package. For information about the contents of the `jinstall` package and details of the installation process, see the [Installation and Upgrade](#)

Guide. Use other packages, such as the jbundle package, only when so instructed by a Juniper Networks support representative.



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



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

To download and install Junos OS Release 23.4R1:

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

- [What's New | 126](#)
- [What's Changed | 131](#)
- [Known Limitations | 134](#)
- [Open Issues | 134](#)
- [Resolved Issues | 136](#)
- [Migration, Upgrade, and Downgrade Instructions | 141](#)

What's New

IN THIS SECTION

- [Authentication and Access Control | 127](#)
- [EVPN | 127](#)
- [Interfaces | 129](#)
- [Junos Telemetry Interface | 130](#)
- [Network Management and Monitoring | 130](#)
- [Additional Features | 131](#)

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

To view features supported on the QFX platforms, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R1, click the Group by Release link. You can collapse and expand the list as needed.

- [QFX10002](#)
- [QFX10008](#)

- [QFX10016](#)
- [QFX10002-60C](#)

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Control device access privileges with exact match configuration** (ACX5448, ACX5448-M, ACX5448-D, ACX710, EX2300, EX2300-MP, EX2300-C, EX2300-VC, EX3400, EX3400-VC, EX4100-48MP, EX4100-H-12P, EX4100-H-12P-DC, EX4100-H-24P, EX4100-H-24P-DC, EX4100-H-24F, EX4100-H-24F-DC, 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, EX9214, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, QFX10002-60C, QFX10002, QFX10008, and QFX10016)—Starting in Junos OS Release 23.4R1, you can configure access privileges for login classes by allowing or denying full hierarchy strings with the `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration options. The exact match configuration enables you to set separate permissions for set, delete, activate, or deactivate operators for any hierarchy.

The `allow-configuration-exact-match` and `deny-configuration-exact-match` configuration options support full hierarchy strings as well as wildcard characters and regular expressions.

[See [Understanding Exact Match Access Privileges for Login Classes](#).]

EVPN

- **Static configuration of MAC-IP bindings with EVPN-VXLAN** (EX4100-24MP, EX4300-MP, EX4400-48MP, EX4650, MX204, MX240, MX480, MX960, MX10004, MX10008, MX2010, and QFX10002-60C)—Starting in Junos OS Release 23.4R1, we've added the functionality to allow static configuration of MAC-IP bindings on an interface, similar to configuring static MACs on an interface. This feature enables the static configuration of IP and MAC entries for crucial services provided by management and infrastructure hosts. It proves particularly advantageous in Internet Exchange Point (IXP) networks where participant Customer Edge routers (CEs) remain well-known and static, not transitioning to different Provider Edge (PE) devices.

You can now utilize a new feature that establishes a static link between an IP address and a MAC for a logical interface within a bridge domain or VLAN. When you provision a static MAC-IP entry on a PE, the PE will initiate a probe following an exponential backoff pattern. The probe will use an all-zero sender IP address on the associated interface. If the entity owning the IP to MAC entry

responds to the probe, the system will learn the IP to MAC binding as static. Subsequently, it will be propagated to remote PEs through the BGP/EVPN Type 2 MAC advertisement route. The corresponding MAC will be recognized as a dynamic entry. If you want to deactivate the probing mechanism for learning the IP to MAC binding, you can do so by configuring a new configuration option [arp-nd-probe-disable]. Without probing, both the MAC and IP to MAC binding will be acquired from network traffic and communicated using EVPN.

We've introduced the following commands and configuration statements:

- Configuration of static IP to MAC bindings



NOTE: A maximum of 8 MACs can be configured per static IP address.

- QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options interface
interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn interface interface-name static-mac-ip ip-
address [MAC1 MAC2 ... MACn]
```

The aforementioned commands provide an option to configure router and override bits for IPV6 entries. For example:

QFX:

```
set vlans vlan-name switch-options interface interface-name static-mac-ip ip-address [MAC1 MAC2 ... MACn]
<router | override>
```

- Disable probing on configuration of static IP to MAC entries:

To turn off the default probing on configuration of static IP to MAC entries, you can use the global configuration statement `arp-nd-probe-disable`.

```
set protocols l2-learning arp-nd-probe-disable
```

- Enable logging for failed probing of static IP to MAC entries:

To turn on the logging, configure the global configuration statement `arp-nd-probe-failed-log`.

```
set protocols l2-learning arp-nd-probe-failed-log
```

- Enable GARP/unsolicited-NA for local and remote static entries

If this feature is required, you must configure the global configuration statement `garp-na-enable`.

```
set protocols l2-learning garp-na-enable
```

- Disable dynamic learning [all static provisioning]

If dynamic learning of MAC-IP entries is not required, configure the statement `drop-unknown-macip` under BD/VLAN.

- QFX:

```
set vlans vlan-name switch-options drop-unknown-macip
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options drop-unknown-macip
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn drop-unknown-macip
```

- Drop unicast ARP request

To drop unicast address resolution requests (for instance, NUD NS messages), you can configure the statement `block-unicast-arp` at global level for QFX and per BD level for MX.

- QFX:

```
set protocols l2-learning block-unicast-arp
```

- MX instance-type virtual-switch:

```
set routing-instances routing-instance-name bridge-domains bridge-domain-name bridge-options block-unicast-arp
```

- MX instance-type evpn:

```
set routing-instances routing-instance-name protocols evpn block-unicast-arp
```

[See [EVPN Proxy ARP and ARP Suppression](#), and [Proxy NDP and NDP Suppression](#) and [interface-mac-ip-limit](#).]

Interfaces

- **Support for port bounce (EX Series, MX Series, QFX Series, and PTX Series)**—Starting in Junos OS Release 23.4R1, you can shut down the interface for a given time by using the request `interface bounce interface_name interval seconds`. The interface goes up at the end of the configured time.

[See [request interface bounce](#).]

Junos Telemetry Interface

- 802.1X configuration and operational state sensors using OpenConfig (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, EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX10003, MX10004, MX10008, MX10016, MX2008, MX2010, MX2020, and QFX10002-60C)—Starting in Junos OS Release 23.4R1, we support configuration and telemetry streaming of operational state data based on the OpenConfig data model `openconfig-if-8021x.yang`.

[For state sensors, see [Junos YANG Data Model Explorer](#). For OpenConfig configuration, see [Mapping OpenConfig 802.1X Commands to Junos Configuration](#).]

- LACP telemetry support for new leaves (ACX5448, ACX5448-M, ACX5448-D, ACX710, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX10002, QFX10002-60C, QFX10008, and QFX10016)—Starting in Junos OS Release 23.4R1, we now support the new LACP leaves `last-change` and `lacp-timeout` introduced in the OpenConfig data model `openconfig-lacp.yang` (version 1.2.0).

[For sensors, see [Junos YANG Data Model Explorer](#).]

- STP OpenConfig and operational state sensor support (ACX710, ACX5448, ACX5448-M, ACX5448-D, 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, EX4400-24X, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, EX4650-48Y-VC, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, QFX10002, QFX10002-60C, QFX10008, and QFX10016)—Starting in Junos OS Release 23.4R1, we support OpenConfig STP configurations and sensors based on the OpenConfig data model `openconfig-spanning-tree` (Version 1, Revision 0.3.1).

[For OpenConfig configuration, see [Mapping OpenConfig STP Commands to Junos Configuration](#). For state sensors, see [Junos YANG Data Model Explorer](#).]

Network Management and Monitoring

- System logging support to capture the layer 2 error conditions on ports (EX-Series, MX-Series, and QFX-series)—Starting in Junos OS Release 23.4R1, Junos OS generates system log messages for MAC Limiting, MAC Move Limiting, MAC learning, Storm control, and redundant trunk groups (RTGs) to record the error conditions on ports.

[See [Overview of System Logging](#).]

Additional Features

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

- **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 HCT and provide the first supported release information when the optic becomes available.

What's Changed

IN THIS SECTION

- [General Routing | 131](#)
- [EVPN | 132](#)
- [Interfaces and Chassis | 133](#)
- [Junos XML API and Scripting | 133](#)
- [Network Management and Monitoring | 133](#)
- [User Interface and Configuration | 134](#)

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

General Routing

- Before this change most list were ordered by the sequence in which the user configured the list items, for example a series of static routes. After this change the list order is determined by the system with items displayed in numerical sequence rather than by the order in which the items were configured. There is no functional impact to this change.
- **Deprecated license revoke information?** Starting in Junos OS Release 23.4R1, we've deprecated the `show system license revoked-info` command. You can use the `show system license` and `show system license usage` commands to know the license information.
- **NOTE:** In the CLI using the command `request chassis feb slot slot-number offline` if you make the primary FEB offline, a traffic loss warning message is displayed and the FEB offline request is

rejected. If offline/restart is still intended for primary FEB, use force option in addition to the command. WARNING message displayed in the CLI: "warning: RCB and FEB work in the paired slot mode. FEB %s offline/restart will result in traffic loss and does not cause a switchover. Please re-try after initiating a mastership switchover using 'request chassis routing-engine master switch' CLI. If offline/restart is still intended, use 'force' option in addition to this CLI."

EVPN

- **Default behavior changes and new options for the easy EVPN LAG configuration (EZ-LAG) feature—**
The easy EVPN LAG configuration feature now uses some new default or derived values, as follows:
 - Peer PE device `peer-id` value can only be 1 or 2.
 - You are required to configure the loopback subnet addresses for each peer PE device using the new `loopback-subnet peer1-subnet` and `loopback peer2-subnet` options at the `edit services evpn device-attribute` hierarchy level. The commit script uses these values for each peer PE device's loopback subnet instead of deriving those values on each PE device. The `loopback-subnet` option at the `edit services evpn device-attribute` hierarchy level has been deprecated.
 - If you configure the `no-policy-and-routing-options-config` option, you must configure a policy statement called `EXPORT-LO0` that the default underlay configuration requires, or configure the new `no-underlay-config` option and include your own underlay configuration.
 - The commit script generates "notice" messages instead of "error" messages for configuration errors so you can better handle `edit services evpn` configuration issues.
 - The commit script includes the element names you configure (such as IRB instance names and server names) in description statements in the generated configuration.

This feature also now includes a few new options so you have more flexibility to customize the generated configuration:

- `no-underlay-config` at the `edit services evpn` hierarchy level—To provide your own underlay peering configuration.
- `mtu overlay-mtu` and `mtu underlay-mtu` options at the `edit services evpn global-parameters` hierarchy level—To change the default assigned MTU size for underlay or overlay packets.

[See [Easy EVPN LAG Configuration](#).]

- **Change in options and generated configuration for the EZ-LAG configuration IRB subnet-address statement—**With the EZ-LAG `subnet-address inet` or `subnet-address inet6` options at the `edit services evpn evpn-vxlan irb irb-instance` hierarchy, you can now specify multiple IRB subnet addresses in a single statement using the list syntax `addr1 addr2 ?`. Also, in the generated configuration for IRB interfaces,

the commit script now includes default router-advertisement statements at the edit protocols hierarchy level for that IRB interface.

[See [subnet-address \(Easy EVPN LAG Configuration\)](#).]

Interfaces and Chassis

- Starting in Junos OS release 23.2R1, the output of show chassis power command displays the state of the power supply in PTX10003 and QFX10003 platforms.

[See [show chassis power](#).]

Junos XML API and Scripting

- XML output tags changed for request-commit-server-pause and request-commit-server-start (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the request system commit server pause command (request-commit-server-pause RPC) and the request system commit server start command (request-commit-server-start RPC). The root element is <commit-server-operation> instead of <commit-server-information>, and the <output> tag is renamed to <message>.

Network Management and Monitoring

- NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.

[See [<copy-config>](#).]

- ephemeral-db-support statement required to configure MSTP, RSTP, and VSTP in the ephemeral configuration database (ACX Series, EX Series, and QFX Series)**—To configure Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or VLAN Spanning Tree Protocol (VSTP) in the ephemeral configuration database, you must first configure the ephemeral-db-support statement at the [edit protocols layer2-control] hierarchy level in the static configuration database.

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

User Interface and Configuration

- **Viewing files with the `file compare files` command requires users to have maintenance permission** — The `file compare files` command in Junos OS and Junos OS Evolved requires a user to have a login class with maintenance permission.

[See [Login Classes Overview](#).]

Known Limitations

IN THIS SECTION

- [Infrastructure](#) | 134

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

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

Infrastructure

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

Open Issues

IN THIS SECTION

- [General Routing](#) | 135

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

- On QFX10002, QFX10008, and QFX10016 switches, the following error message is observed during specific steps while clearing and loading the scaled configuration again:
PRDS_SLU_SAL:jprds_slu_sal_update_lrnCnt(),1379: jprds_slu_sal_update_lrnCnt call failed. This issue is observed in a scaled setup with scaled VLANs and traffic flowing through all VLANs. If the configuration is cleared and loaded again using the below steps: load override <base-config> rollback 1 commit Then the base configuration is loaded, all learned MACs are aged out and the MAC entries are marked as invalid. Aging thread scans and finds SMAC ref bit transition for cleared MAC entries and gets added to a stale MAC software table. In a scaled setup where 2000 MACs are learned over a port, not all MACs are cleared at one hardware trigger. This happens in a batch of 256 entries in a MAC table at a time as per the design of the QFX10000 lines of switches. In the meantime, it is expected that IFBD on which the MACs were learned is deleted. This is the reason why Lport+IFL mapping is not found while clearing such MACs and throws an error. [PR1522852](#)
- When TISSU upgrade is done from 22.4 release onwards, the box come up as backup Routing Engine. Work-around:- To make is primary following command needs to be run again. sysctl -w hw.lc.issuboot=0 sleep 10 sysctl -w hw.re.issu_state=0 sleep 10 sysctl -w hw.re.tissu=0 sleep 10 sysctl -w hw.product.pvi.config.chasd.no_re_status_on_backup=1 sleep 60 [PR1703229](#)
- Disable the VME interfaces or have the default route added properly from the shell script for the connectivity with the ZTP server to work. [PR1743222](#)
- On all Junos OS platforms, due to timing issues the PFE (Packet Forwarding Engine) /PICs (Physical Interface Card) will be slow and services will face slowness issue and error message: **Minor potential slow peers are: X** will be seen. This is rare timing issue. [PR1747077](#)

Interfaces and Chassis

- The LAG (Link Aggregation Group) member links might flap on all Junos OS platforms except MX when the configuration of any interface is changed or modified. The flap is not seen always. [PR1679952](#)

Resolved Issues

IN THIS SECTION

- [EVPN | 136](#)
- [General Routing | 137](#)
- [Interfaces and Chassis | 140](#)
- [Junos XML API and Scripting | 140](#)
- [Layer 2 Ethernet Services | 140](#)
- [MPLS | 140](#)
- [Platform and Infrastructure | 140](#)
- [Routing Policy and Firewall Filters | 140](#)
- [Routing Protocols | 141](#)

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

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

EVPN

- EVPN-VXLAN comp nh is not installed in Packet Forwarding Engine after peer reboot. [PR1739686](#)
- After deactivating or activating GBP configuration in the MH AE scenario all tag entries not getting re-learned on leaf nodes in the ethernet-switching table resulting in traffic loss. [PR1739878](#)
- ARP or FIB are added even if IRB in EVPN is disabled. [PR1743529](#)

- IRB reachability issues might be observed in the EVPN-VXLAN environment when looped ARP comes on ESI-LAG. [PR1743913](#)
- MAC addresses programming failure resulting in traffic flooding. [PR1758677](#)

General Routing

- Minor packet drops due to hardware programming issues. [PR1700927](#)
- The dcpfe process will crash due to memory fragmentation. [PR1711860](#)
- QSFP-100G-LR4-T2 optics will stay down after ISSU/TISSU. [PR1713010](#)
- The dot1x-protocol subsystem is not responding to management requests while verifying in show security mka sessions. [PR1713881](#)
- IGMP/MLD queries might get dropped if received on a port on the backup VC member when IGMP/MLD snooping is enabled. [PR1716902](#)
- Layer 2 Multicast traffic drops when PIM is configured without IGMP snooping enabled. [PR1720527](#)
- Momentary traffic loss is observed when interface with local Type-1 ESI goes down. [PR1722348](#)
- The error logs **fpc0 expr_hostbound_packet_handler: Receive pe 254?** would be generated. [PR1725716](#)
- The class of service subsystem crashed after the device is restarted or the switchover is performed. [PR1726124](#)
- The EVPN-VXLAN proxy-arp will respond with the wrong MAC when no-mac-learning is configured. [PR1727119](#)
- On all Junos OS platforms, the l2ald process memory usage is seen to increase over time. [PR1727954](#)
- [QFX] debugging command `show aq107 xxx` on VTY might generate an error on 10GBASE-T SFP if AQ index exceeds 48. [PR1728452](#)
- Traffic loss will be observed due to CRC errors with QSFP+-40G-ACU10M plugged. [PR1729067](#)
- Traffic drops when any of the VXLAN VLAN is deleted. [PR1731583](#)
- On router reboot an interface in SP style blocks all packets on **family inet/inet6** interfaces if VSTP is configured on vlan-bridge encapsulated VLANs. [PR1732718](#)
- Traffic loss is seen when `l2cp force-up` configuration statement is configured. [PR1733543](#)

- Online SIBs will go down due to a faulty SIB that triggers spmbpfe crash. [PR1734734](#)
- Packet drop is observed due to SIB ASIC issue on fabric. [PR1734735](#)
- BFD session remains stuck in INIT state on certain QFX platforms. [PR1736348](#)
- Unexpected VLAN tagging behavior would be observed in the EVPN-VXLAN scenario. [PR1736954](#)
- Blackholing of I3-inject traffic on QFX10000 platforms. [PR1738197](#)
- Traffic drop observed when encapsulation ethernet-bridge is configured on the AE interface associated with VxLAN VLAN. [PR1738205](#)
- High convergence time in the EVPN-VxLAN uplink failover scenario. [PR1738276](#)
- VC case not handled properly while calling brcm_vxlan_port_discard_set api. [PR1738404](#)
- An rpd crash will be observed due to inconsistency between rpd and kernel. [PR1738820](#)
- DSCP classifier is not created on IP interfaces. [PR1738981](#)
- The ksyndcd process crash would be seen on backup Routing Engine. [PR1739258](#)
- The loop-detect is not working in the VXLAN scenario. [PR1740327](#)
- Traffic loss is seen due to anomalies after the recreation of IFLs. [PR1740561](#)
- Enabling sflow triggers ddos-protection violation of protocol group resolve. [PR1741461](#)
- SPMB process will crash and PICs will not come online. [PR1742186](#)
- Traffic dropped is observed in the MPLS LDP scenario when the peer device MAC address is changing. [PR1742364](#)
- Race condition where FLOOD ROUTE DEL event can cause I2ald crash. [PR1742613](#)
- Traffic drop will be observed after extended-vni-list configuration change with EVPN-VXLAN scenario. [PR1742763](#)
- GRE over IPv6 will not work resulting in traffic impact post-upgrading the device. [PR1743978](#)
- BPDU Protection with packet-action drop support on QFX10002-60C. [PR1745102](#)
- Clear error command support for QFX10002-60c. [PR1746244](#)
- QFX10002-60c port et-0/0/30 part of a lag is dropping peer ARP reply after configuring a GRE tunnel. [PR1746435](#)
- Soft OIR of the link connected to 10GBASE-T SFP will not update the link state at the other end. [PR1747277](#)

- Alarm LED is lit due to LICENSE_EXPIRED on Virtual Chassis backup even with the valid license. [PR1747720](#)
- Traffic drop will be observed when Label MPLS traffic egressing out on the IRB interface as IPV4. [PR1748500](#)
- L3VPN traffic destined for hosts learned over IRB/VXLAN will get dropped on QFX10000 platforms. [PR1750468](#)
- The PFE process crashed while removing and applying the firewall filters. [PR1750828](#)
- Incorrect egress MTU errors when larger than 1500 byte packets are sent on Layer 2 ports. [PR1751700](#)
- PIM neighborship, or other control protocols flaps due to host-bound queue (Q3) congestion. [PR1753853](#)
- QFX: VC(virtual chassis) does not get formed when using 100G for vc port. [PR1754838](#)
- Learning stops in logical interface in QFX10000 platforms. [PR1756672](#)
- The dcpfe process crash will be seen when L2PT interfaces are configured with multiple protocols. [PR1757329](#)
- The mcsnoopd cored with EVPN-MPLS and VPLS with multicast configuration. [PR1758659](#)
- Generate an empty file whose name is secondary_vlan when executing RSI. [PR1759875](#)
- Traffic drop will be seen when packets are sent with incorrect VLAN tag. [PR1760823](#)
- ECMP traffic drop after the AE interface flap. [PR1761887](#)
- LLDP neighborship will not be formed on all Junos OS devices. [PR1763053](#)
- VPLAG information not installed correctly in hardware results in traffic flooding. [PR1763116](#)
- BFD session detection time is higher than expected leading to traffic drop. [PR1763667](#)
- A warning message is seen while installing a license key with an unknown feature. [PR1766515](#)
- The PVST BPDU packet get dropped in transparent EVPN-VXLAN on the ingress PE-CE port of SP style on Junos OS QFX platforms. [PR1771739](#)

Interfaces and Chassis

- Traffic impact will be seen with mismatched speeds on the LAG interface and member interface. [PR1725168](#)
- High memory utilization is observed on all Junos OS platforms. [PR1757801](#)
- Services using the management interface will be affected on all Junos OS platforms. [PR1757936](#)

Junos XML API and Scripting

- Junos OS platform device unable to commit configuration in recovery mode. [PR1717425](#)

Layer 2 Ethernet Services

- DHCP binding is not happening in EVPN VXLAN topology with DHCP stateless relay (forward-only). [PR1722082](#)

MPLS

- The rpd crash observed during RE switchover or Route Convergence. [PR1747365](#)

Platform and Infrastructure

- The CoS rewrite rules will not be working in the EVPN with IRB scenario. [PR1736890](#)

Routing Policy and Firewall Filters

- Policy change to a rib-group import-policy configured with global routing-options interface-routes causes the rpd issue on all platforms with EVPN-VXLAN configuration. [PR1744449](#)

Routing Protocols

- Memory leak observed when reconfiguring the flow routes. [PR1742147](#)
- Route-distinguisher change leads to the route being present in rpd, but not installed in kernel/PFE. [PR1746439](#)
- BGP multipath route is not correctly applied after changing the IGP metric. [PR1754935](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 141](#)
- [Installing the Software on QFX10002-60C Switches | 143](#)
- [Installing the Software on QFX10002 Switches | 144](#)
- [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 | 145](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 146](#)
- [Performing a Unified ISSU | 150](#)
- [Preparing the Switch for Software Installation | 151](#)
- [Upgrading the Software Using Unified ISSU | 151](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 153](#)

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 **23.4** 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 23.4 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-x86-64-23.4-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 23.4 jinstall package, you can issue the `request system software rollback` command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

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

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



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



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

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

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

For example:

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


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

For example:

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

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

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

Installing the Software on QFX10002 Switches



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



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

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

For example:

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

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

For example:

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

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

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

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



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

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

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

To install the software on re0:

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

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

For example:

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

To install the software on re1:

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

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

For example:

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

Reboot both Routing Engines.

For example:

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

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

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

Installing the Software on QFX10008 and QFX10016 Switches

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



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



WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the

software does not install properly. Make sure you issue the CLI `delete chassis redundancy` command when prompted. If GRES is enabled, it will be removed with the `redundancy` command. By default, NSR is disabled. If NSR is enabled, remove the `nonstop-routing` statement from the `[edit routing-options]` hierarchy level to disable it.

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

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

2. From the command line, enter configuration mode:

```
user@switch> configure
```

3. Disable Routing Engine redundancy:

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

4. Disable nonstop-bridging:

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

5. Save the configuration change on both Routing Engines:

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

6. Exit the CLI configuration mode:

```
user@switch# exit
```

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

12. Transfer routing control to the backup Routing Engine:

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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 151](#)
- ["Upgrading the Software Using Unified ISSU" on page 151](#)

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

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

To verify that nonstop active routing is enabled:



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

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

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

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

Upgrading the Software Using Unified ISSU

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

To upgrade the switch using unified ISSU:

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

4. Start the ISSU:

- On the switch, enter:

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

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



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

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

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

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



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



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

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

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

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

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

We have two types of releases, 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 – 23.4, 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](#).

Junos OS Release Notes for SRX Series Firewalls

IN THIS SECTION

- [What's New | 155](#)
- [What's Changed | 190](#)
- [Known Limitations | 194](#)
- [Open Issues | 195](#)
- [Resolved Issues | 196](#)
- [Migration, Upgrade, and Downgrade Instructions | 202](#)
- [Documentation Updates | 203](#)

What's New

IN THIS SECTION

- [Hardware | 156](#)
- [Application Identification \(AppID\) | 174](#)
- [Authentication and Access Control | 175](#)
- [Chassis | 175](#)
- [Class of Service | 176](#)
- [Content Security | 176](#)
- [Device Security | 176](#)
- [Flow-based and Packet-based Processing | 177](#)
- [High Availability | 178](#)
- [Interfaces | 180](#)
- [J-Web | 180](#)
- [Juniper Advanced Threat Prevention Cloud \(ATP Cloud\) | 184](#)
- [Junos Telemetry Interface | 185](#)
- [Network Address Translation \(NAT\) | 186](#)
- [Network Management and Monitoring | 187](#)
- [Public Key Infrastructure \(PKI\) | 187](#)
- [VPNs | 188](#)
- [Additional Features | 189](#)

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

To view features supported on the SRX Series Firewall, view the Feature Explorer using the following links. To see which features were added in Junos OS Release 23.4R1, click the Group by Release link. You can collapse and expand the list as needed.

- [SRX300](#)
- [SRX320](#)
- [SRX340](#)
- [SRX345](#)

- [SRX380](#)
- [SRX1500](#)
- [SRX1600](#)
- [SRX2300](#)
- [SRX4100](#)
- [SRX4200](#)
- [SRX4600](#)
- [SRX5400](#)
- [SRX5600](#)
- [SRX5800](#)

Hardware

- **New SRX1600 Firewall**—Starting in Junos OS Release 23.4R1, we introduce the SRX1600 Firewall. The SRX1600 Firewall is an entry-level firewall that consolidates firewall and security features. The SRX1600 is ideal for small-medium enterprise edge, campus edge, data center edge, and secure VPN router deployments for distributed enterprise use cases.

Table 7: Features Supported on SRX1600 Firewall

Feature	Description
Chassis	<ul style="list-style-type: none"> Chassis and FRU management support, including: <ul style="list-style-type: none"> Temperature threshold monitoring using sensors Power supply unit PIC detection Fabric management Fan speed adjustment as per EM policy <p>[See Chassis-Level User Guide.]</p> <ul style="list-style-type: none"> Resiliency support for the following hardware components: <ul style="list-style-type: none"> CPU PCI Memory I2C (Inter-Integrated Circuit) Temperature sensor Two power supply units (PSUs) in 1+1 redundancy mode Fan <p>Hardware resiliency monitors hardware devices periodically, performs alarm management, and takes corrective actions if an anomaly is persistently encountered.</p> <p>[See Chassis-Level User Guide.]</p>

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Chassis Cluster	<ul style="list-style-type: none"> • Chassis cluster support, including: <ul style="list-style-type: none"> • Dual redundant fabric ports • Redundant interfaces (reth) and redundancy groups for failovers • Monitoring process (flowd and chassisd) • Management of control link (HLd, JSRPd) • Configuration synchronization, Routing Engine kernel synchronization, and session data synchronization (RTO) • Fault monitors, event registers, and failover facilities <p>[See SRX Series Chassis Cluster Configuration Overview.]</p> • Support for dual control links with MACsec <p>[See Media Access Control Security (MACsec) on Chassis Cluster]</p> <ul style="list-style-type: none"> • Support for In-Service Software Upgrade (ISSU). <p>[See Upgrading Both Devices in a Chassis Cluster Using ISSU.]</p>
Class of service (CoS)	<ul style="list-style-type: none"> • Support for CoS. <p>[See Understanding Class of Service.]</p>
Flow monitoring	<ul style="list-style-type: none"> • Support for strict packet order for multicast. <p>[See flow (Security Flow).]</p> <ul style="list-style-type: none"> • Increased flow session capacity of 5 million sessions. You can enable the increased flow session capacity using the <code>set security forwarding-process scaled-14-firewall-mode</code> CLI command. <p>[See Flow-Based Performance.]</p>

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Hardware	<ul style="list-style-type: none"> • The SRX1600 is a 1-U chassis with the following ports and supports both AC and DC variants: <ul style="list-style-type: none"> • Sixteen 1Gigabit-Ethernet (GbE) BASE-T ports • Four 10GbE SFP+ MACsec ports • Two 25GbE SFP28 MACsec ports • Two 1GbE SFP HA MACsec ports <p>To install the SRX1600 hardware and perform initial software configuration, routine maintenance, and troubleshooting, see SRX1600 Firewall Hardware Guide.</p> <p>[See Feature Explorer https://apps.juniper.net/feature-explorer/ for the complete list of features for any platform.]</p>
High availability (HA) and resiliency	<ul style="list-style-type: none"> • Support for BFD: <ul style="list-style-type: none"> • Support up to 3 x 300 msec failure detection time • Support up to 100 BFD sessions <p>[See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.]</p> <ul style="list-style-type: none"> • Support for Multinode High Availability: <p>[See Multinode High Availability.]</p>
Interfaces	<ul style="list-style-type: none"> • Supports three PICs (PIC 0, PIC 1, and PIC 2) with 1 Gbps, 25 Gbps, and 10 Gbps speeds: <ul style="list-style-type: none"> • PIC 1 supports three different speed modes; 1 Gbps, 10 Gbps, and 25 Gbps. • PIC 2 supports mixed speed of 1 Gbps or 10 Gbps. <p>Junos OS creates the PIC 0 by default.</p> • The Junos OS creates PIC 1 and PIC 2 interfaces once you install the Optics module. <p>[See SRX1600 Port Speed Overview.]</p>

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Junos Telemetry Interface	<p>Junos telemetry interface (JTI) streaming support for the following sensors:</p> <ul style="list-style-type: none"> • System log messages (/junos/events/) • Memory utilization for routing protocol tasks (/junos/task-memory-information/) • Interfaces (/interfaces/) • Hardware operational states for Routing Engine, power supply units (PSUs), switch fabric boards, control boards, switch interface boards, MICs, and PICs (/components/) • Sensor for flow sessions (/junos/security/spu/flow/) <p>[See Junos YANG Data Model Explorer.]</p>
Layer 2 features	<ul style="list-style-type: none"> • Support for Layer 2 transparent mode. [See Ethernet Switching and Layer 2 Transparent Mode Overview.] • Support for secure wire. [See Secure Wire on Security Devices.] • Support for 802.1X authentication protocol in transparent mode. [See 802.1X Authentication.]

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Layer 7 security features	<ul style="list-style-type: none"> • Support for advanced policy-based routing (APBR) . [See Advanced Policy-Based Routing.] • Support for application identification (APPID). [See APPID Overview.] • Support for application quality of experience (AppQoE). [See Application Quality of Experience.] • Support for application quality of service (AppQoS). [See Application QoS.] • Support for Content Security. [See Content Security Overview.] • Support for intrusion detection and prevention (IDP). [See Intrusion Detection and Prevention Overview.] • Support for Juniper Advanced Threat Prevention (ATP) Cloud. [See File Scanning Limits and Troubleshooting Juniper Advanced Threat Prevention Cloud: Checking the application-identification License.] • Support for Juniper Networks Deep Packet Inspection-Decoder (JDPI). [See Overview.] • Support for SSL proxy. [See SSL Proxy.]
MACsec	<ul style="list-style-type: none"> • Support for Media Access Control Security (MACsec) in static CAK mode with GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128, and GCM-AES-XPB-256 encryption. [See Configuring MACsec in Static CAK Mode.]

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Network management and monitoring	<ul style="list-style-type: none">• Support for the filter based packet capture which captures the real-time data packets traveling over the network. <p>[See Example: Configure a Firewall Filter for Packet Capture.]</p>
Remote access	<ul style="list-style-type: none">• Support for remote access using Juniper Secure Connect Client. <p>[See Juniper Secure Connect Application Overview.]</p>
Routing policy and firewall filters	<ul style="list-style-type: none">• Support for firewall filters. <p>[See Firewall Filters Overview.]</p>

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Routing protocol	<p>Support for the following routing protocols:</p> <ul style="list-style-type: none"> • RIPv1, RIPv2, and RIPv6 [See RIP and RIPv6 Overview.] • OSPFv2 and OSPFv3 [See Introduction to OSPF.] • BGP [See BGP Overview.] • Multicast, IGMP, and PIM [See Multicast Overview, Configuring IGMP, and PIM Overview.] • Virtual Routers [See Understanding VRRP.] • Static Route [See Understand Basic Static Routing.] • LACP [See Understanding LACP on Standalone Devices.] • VLAN tagging [See Configuring VLAN Tagging.]

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
Services applications	<ul style="list-style-type: none"> • Support for Application Layer Gateway (ALG). [See ALG Overview.] • Support for Domain Name System (DNS) [See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.] • Support for user authentication. [See User Authentication Overview.] • Support for security policies. [See Configuring Security Policies.] • Support for security zones. [See Security Zones.] • Support for Network Address Translation (NAT). [See NAT Configuration Overview.] • Support for screens options for attack detection and prevention. [See Screens Options for Attack Detection and Prevention.] • Support for traffic processing. [See Traffic Processing on SRX Series Firewalls Overview.] • Support for integrated user firewall. [See Configure Integrated User Firewall.] • Support for IPsec VPN with ike process. Support for the Policy-based VPN and Group VPN is not yet available. [See IPsec VPN Configuration Overview.] • Support for PowerMode IPsec (PMI). [See PowerMode IPsec.]

Table 7: Features Supported on SRX1600 Firewall *(Continued)*

Feature	Description
	<ul style="list-style-type: none"> • Support for DHCP. [See DHCP Overview.] • Support for GPRS Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP). [See Monitoring GTP Traffic and SCTP Overview.] • Support for on-box reporting. [See report (Security Log).] • Support for inline active flow monitoring [See Understand Inline Active Flow Monitoring.] • Support for Two-Way Active Measurement Protocol (TWAMP) [See Understand Two-Way Active Measurement Protocol.] • Support for real-time performance monitoring (RPM). [See Real-Time Performance Monitoring for SRX Devices.] • Support for logical systems. [See Logical Systems Overview.]

Table 7: Features Supported on SRX1600 Firewall (Continued)

Feature	Description
Software installation and upgrade	<ul style="list-style-type: none"> • Support for BIOS, Secure Boot and Bootloader. [See Secure Boot.] • Support for Jfirmware. [See request system firmware upgrade and show system firmware.] • Support for NVMe SSD Software. [See Upgrading the SSD Firmware on Routing Engines with VM Host Support.] • Support for secure ZTP. [See Secure Zero Touch Provisioning.] • Support for switching between secure ZTP and ZTP on secure platforms. [See Switching between Secure Zero Touch Provisioning and Zero Touch Provisioning.]
User access and authentication administration	<ul style="list-style-type: none"> • Support for trusted platform module [See Overview.]

- **New SRX2300 Firewall**—Starting in Junos OS Release 23.4R1, we introduce the mid-range SRX2300 Firewall. The SRX2300 Firewall provides next-generation firewall capabilities and advanced threat detection and mitigation. This firewall is ideal for small-medium enterprise edge, campus edge, data center edge firewall and secure VPN router deployments for distributed enterprise use-cases.

Table 8: Features Supported on SRX2300 Firewall

Feature	Description
Chassis	<ul style="list-style-type: none"> • Support for chassis management and temperature monitoring infrastructure [See Chassis-Level User Guide.]

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
Chassis Cluster	<ul style="list-style-type: none"> Support for ISSU and dual control links with MACsec <p>[See Upgrading a Chassis Cluster Using In-Service Software Upgrade and Media Access Control Security (MACsec) on Chassis Cluster.]</p>
Class of service (CoS)	<ul style="list-style-type: none"> Support for CoS <p>[See Understanding Class of Service.]</p>
Hardware	<ul style="list-style-type: none"> The SRX2300 is a 1-U chassis with the following ports. All the ports are MACsec capable ports: <ul style="list-style-type: none"> Eight 10Gigabit-Ethernet (GbE) BASE-T ports Eight 10GbE SFP+ ports Four 25GbE SFP28 ports Two 100GbE QSFP28 ports Two 1GbE SFP HA ports <p>To install the SRX2300 hardware and perform initial software configuration, routine maintenance, and troubleshooting, see SRX2300 Firewall Hardware Guide.</p> <p>[See Feature Explorer https://apps.juniper.net/feature-explorer/ for the complete list of features for any platform.]</p>

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
High availability (HA) and resiliency	<ul style="list-style-type: none"> • Support for BFD <ul style="list-style-type: none"> • Support up to 3 x 300 msec failure detection time • Support up to 100 BFD sessions [See Understanding BFD for Static Routes for Faster Network Failure Detection and Understanding How BFD Detects Network Failures.] • Support for Multinode High Availability [See Multinode High Availability.]
Interfaces	<p>Supports four PICs (PIC 0, PIC 1, PIC 2, and PIC 3) with the following interfaces:</p> <ul style="list-style-type: none"> • PIC 0 has eight Base-T interfaces • PIC 1 has eight SFP+ interfaces • PIC 2 has four SFP28 interfaces • PIC 3 has two QSFP28 interfaces <p>The Junos OS creates PIC 0 ports by default. You can channelize the QSFP28 (PIC 3) ports into 4x25 Gbps and 4x10 Gbps.</p> <p>[See SRX2300 Port Speed Overview.]</p>

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
Junos Telemetry Interface	<p>Junos telemetry interface (JTI) streaming support for the following sensors:</p> <ul style="list-style-type: none"> • System log messages (/junos/events/) • Memory utilization for routing protocol tasks (/junos/task-memory-information/) • Interfaces (/interfaces/) • Hardware operational states for Routing Engine, power supply units (PSUs), switch fabric boards, control boards, switch interface boards, MICs, and PICs (/components/) • Sensor for flow sessions (/junos/security/spu/flow/) <p>[See Junos YANG Data Model Explorer.]</p>

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
Layer 7 security features	<ul style="list-style-type: none"> • Support for advanced policy-based routing (APBR) [See Advanced Policy-Based Routing.] • Support for application identification (APPID) [See APPID Overview.] • Support for application quality of experience (AppQoE) [See Application Quality of Experience.] • Support for application quality of service (AppQoS) [See Application QoS.] • Support for Content Security [See Content Security Overview.] • Support for intrusion detection and prevention (IDP) [See Intrusion Detection and Prevention Overview.] • Support for Juniper Advanced Threat Prevention (ATP) Cloud [See File Scanning Limits.] • Support for Juniper Networks Deep Packet Inspection-Decoder (JDPI) [See Overview.] • Support for SSL proxy [See SSL Proxy.]

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
MACsec	<ul style="list-style-type: none">• Support for Media Access Control Security (MACsec) <p>[See Understanding Media Access Control Security (MACsec).]</p>
Network management and monitoring	<ul style="list-style-type: none">• Support for the filter based packet capture which captures the real-time data packets traveling over the network. Support for data path debugging is not yet available. <p>[See Example: Configure a Firewall Filter for Packet Capture.]</p>

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
Services applications	<ul style="list-style-type: none"> • Support for Application Layer Gateway (ALG) [See ALG Overview.] • Support for Domain Name System (DNS) [See Understanding and Configuring DNS, DNS ALG, DNS Proxy Overview, DNS Names in Address Books, and DNSSEC Overview.] • Support for user authentication [See User Authentication Overview.] • Support for security policies [See Configuring Security Policies.] • Support for security zones [See Security Zones.] • Support for Network Address Translation (NAT) [See NAT Configuration Overview.] • Support for screens options for attack detection and prevention [See Screens Options for Attack Detection and Prevention.] • Support for traffic processing [See Traffic Processing on SRX Series Firewalls Overview.] • Support for integrated user firewall [See Configure Integrated User Firewall.] • Support for IPsec VPN withiked process. Support for the Policy-based VPN and Group VPN is not yet available.

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
	<p data-bbox="898 359 1328 386">[See IPsec VPN Configuration Overview.]</p> <ul style="list-style-type: none"> <li data-bbox="862 422 1273 449">• Support for PowerMode IPsec (PMI) <p data-bbox="898 485 1149 512">[See PowerMode IPsec.]</p> <ul style="list-style-type: none"> <li data-bbox="862 548 1089 575">• Support for DHCP <p data-bbox="898 611 1133 638">[See DHCP Overview.]</p> <ul style="list-style-type: none"> <li data-bbox="862 674 1393 737">• Support for GPRS Tunneling Protocol (GTP) and Stream Control Transmission Protocol (SCTP) <p data-bbox="898 772 1414 800">[See Monitoring GTP Traffic and SCTP Overview.]</p> <ul style="list-style-type: none"> <li data-bbox="862 835 1198 863">• Support for on-box reporting <p data-bbox="898 898 1170 926">[See report (Security Log).]</p> <ul style="list-style-type: none"> <li data-bbox="862 961 1321 989">• Support for inline active flow monitoring <p data-bbox="898 1024 1398 1052">[See Understand Inline Active Flow Monitoring.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1087 1349 1150">• Support for Two-Way Active Measurement Protocol (TWAMP) <p data-bbox="898 1186 1398 1249">[See Understand Two-Way Active Measurement Protocol.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1285 1377 1348">• Support for real-time performance monitoring (RPM) <p data-bbox="898 1383 1398 1446">[See Real-Time Performance Monitoring for SRX Devices.]</p> <ul style="list-style-type: none"> <li data-bbox="862 1482 1179 1509">• Support for logical systems <p data-bbox="898 1545 1230 1572">[See Logical Systems Overview.]</p>

Table 8: Features Supported on SRX2300 Firewall *(Continued)*

Feature	Description
Software Installation and Upgrade	<ul style="list-style-type: none"> Support for BIOS, Secure Boot and boot loader [See Secure Boot.] Support for Jfirmware [See request system firmware upgrade and show system firmware.] Support for secure ZTP [See Secure Zero Touch Provisioning.]
User access and authentication administration	<ul style="list-style-type: none"> Support for trusted platform module [See Overview.]

Application Identification (AppID)

- **Subject Alternative Name in custom application signatures (SRX Series Firewalls, vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can create an application identification (AppID) custom signature using the Subject Alternative (SAN) certificate attribute for SSL signatures. You can use the SAN attribute to specify multiple host names or IP addresses in a single certificate. With this enhancement, custom application signatures can detect applications based on the application's host names listed in the SAN field of the SSL certificate.

You can configure SAN using the `ssl-subject-alt-name` option under `[edit services application-identification application name over SSL signature name member name context]` hierarchy.

See [\[Context \(Application Signatures\)\]](#).

- **Micro-applications enhancements (SRX Series Firewalls and vSRX)**—Starting in Junos OS Release 23.4R1, we've enhanced the detection of micro-applications. Application identification (AppID) now uses string-based attributes of the application for matching micro-applications in addition to using the integer-based attributes of application.

You can now manage applications with a finer level of control at the sub-function level.

See [\[Application Identification Support for Micro-Applications\]](#).

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Support for firewall users log off, custom logo and banner (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, firewall users can log off using the logoff button displayed in captive portal after a successful login.

SRX and NFX administrators can set custom logo for captive portal. SRX and NFX administrators can configure custom login-success, login-fail banner messages in captive-portal. You can configure logo option under set access firewall-authentication web-authentication hierarchy level for custom-logo. You can configure banner option under set access firewall-authentication web-authentication hierarchy level for banner messages.

[See [firewall-authentication](#).]

- **Support for client/server certificate validation using TLS protocol mutual authentication (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, a client can authenticate without password based on client/server certificate validation using Mutual-TLS authentication. You can configure mtls-profile option at the set security firewall-authentication hierarchy level.

[See [firewall-authentication \(Security\)](#).]

- **Support for destination identity in firewall policy (SRX Series Firewalls, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can control network access based on destination identity in security policy. You can match the traffic based on destination identity information. You can configure destination-identity-context option at the set security policies from-zone *zone-name* to-zone *zone-name* match hierarchy level.

You can configure identity-context-profile *profile-name* option at the set user-identification device-information hierarchy level. You can configure destination-identity-context-profile option at the set security policies from-zone *zone-name* to-zone *zone-name* match hierarchy level.

[See [user-identification \(Services\)](#), [match \(Security Policies\)](#), [identity-context-profile](#), [destination-identity-context](#), and [destination-identity-context-profile](#).]

Chassis

Class of Service

- **Routing-instance based classification (SRX1500, SRX4100, SRX4200, SRX4600, vSRX3.0, NFX 150, NFX250, NFX350)**—Starting in Junos OS Release 23.4R1, SRX1500, SRX4100, SRX4200, SRX4600, vSRX3.0, NFX150, NFX250, and NFX350 Firewalls support routing-instance based classification. You use routing instance-based classifiers to classify packets based on the virtual routing and forwarding (VRF) of incoming packets. For routing instances with VRF table labels enabled, you can apply a custom MPLS EXP, DSCP, or IEEE802.1 classifier to the routing instance.

[See [classifiers \(Routing Instance\)](#).]

Content Security

- **Juniper NextGen Web Filtering (SRX Series and cSRX)**—Starting in Junos OS Release 23.4R1, Juniper NextGen Web Filtering (NGWF) is available as the URL filtering infrastructure in the Juniper cloud. It uses the OEM Cloud for URL reputation and category. NGWF enables the SRX Series Firewall and cSRX Container Firewall to permit or deny access to specific URLs based on the reputation and category to which the URLs belong. It intercepts, scans, and acts upon HTTP or HTTPS traffic to prevent inappropriate Web content access. It also provides better visibility into the URL traffic.

[See [Juniper Web Filtering](#).]

- **URL feed support for Content Security (SRX Series and vSRX)**—Starting in Junos OS Release 23.4R1, we introduce URL feed for Content Security. The URL feed reduces your effort to add multiple URLs into a single URL pattern automatically. You should add the URLs that need to be added in the URL pattern to the URL feed file saved in the HTTPS server. When you configure the URL feed, the system downloads the file from the HTTPS server and creates the URL pattern automatically.

[See [url-feed](#), [request security utm custom-objects url-feed update feed-name](#), [request security utm custom-objects url-feed update feed-name force](#), and [show security utm custom-objects url-feed status feed-name](#).]

Device Security

- **Pre-ID default policy enhancements (SRX Series Firewalls and vSRX Virtual Firewall)**—Starting in Junos OS Release 23.4R1, the Pre-ID default policy (`pre-id-default-policy`) denies the flow before performing application identification (AppID) when there are no potential policies to permit the flow.

When the device receives the first packet of a traffic flow, it performs a basic 5-tuple matching and checks the defined potential policies to determine how to treat the packet. If all potential policies have action as "deny", and the default policy action is also set to "deny", then the device denies the traffic and does not perform application identification.

If any policy has action other than "deny", then the device performs deep packet inspection (DPI) to identify the application.

The device checks for potential policies on both zone context and global context.

See [[Pre-id-default-policy](#)].

- **Security Policy Support for Explicit Web Proxy (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support explicit web proxy profile security policy. The Juniper Networks® SRX Series Firewalls apply security enforcement based on the rules created in the explicit web proxy profile policy.

The explicit proxy profile policy can enforce fine-grained rules to filter and inspect the web traffic.

See [[Explicit Web Proxy](#)].

- **User authentication for Explicit Proxy (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support firewall LDAP-based user authentication to control user access to the network for explicit web-proxy deployments. We support web authentication with web redirection and usage of captive portals.

With explicit web proxy authentication in place, when a user first connects to the proxy server, the browser is prompted to provide their credentials. The explicit proxy then verifies the username and password with the LDAP server. If the credentials are valid, the proxy grants access to the client and stores their information in the database.

See [[Explicit Web Proxy](#)].

- **Explicit Web Proxy support is available for on-premises deployment (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, Explicit Web Proxy support is available for on-premises deployment use cases on the following platforms:

SRX1500

SRX4100

SRX4200

SRX4600

vSRX3.0

The Explicit Web Proxy feature and the configurations are available by default.

SSL proxy support is required to enable SSL decryption service for explicit proxy sessions.

Flow-based and Packet-based Processing

- **Express Path support for Fragmentation (SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.4R1, we support fragmentation for unequal maximum transmission units (MTUs) on service offload (SOF) path in network processing unit (NPU).

For more information, see [Express Path Overview](#)

- **Support drop-flow to prevent security attack - (SRX Series Firewall, vSRX3.0, cSRX, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, we support a new feature drop-flow to prevent security attack. You can control and limit the number of max-session for the drop-flow. The session in the drop-flow is valid for 4 seconds by default. During a drop-flow, the session state displays as Drop, but in the flow, the state remains as Valid.

The drop-flow feature is enabled by default. To disable the feature, use the `set security flow drop-flow max-sessions 0` command. To delete only the drop-flow feature, use the `run clear security flow session drop-flow` command.

To view the current drop-flow configuration, use the `show security flow drop-flow` command, and the view all the available drop-flow, use the `show security flow session drop-flow` command.

[See [Flow Based Session](#).]

- **Support for TCP enhancement - (SRX Series Firewall)**—Starting in Junos OS Release 23.4R1, we support TCP fast open (FSO) and TCP selective acknowledge. FSO uses the first TCP connection to acquire the FSO cookie, in the second connection TCP FSO uses the cookie acquired through the first session to perform fast open. When you invoke SYN proxy for a specific TCP connection, TCP fast open for this connection is disabled.

[See [TCP Sessions](#).]

- **Support for aggressive aging- (SRX Series Firewall)**—Starting in Junos OS Release 23.4R1, in addition to the existing aging control, we have add a more fine-tuned control on early-ageout for a session based on application, protocol, and default. If all the three cutoff time options are configured, the application cutoff time takes precedence followed by protocol, and then the default.

[See [Understanding Session Characteristics for SRX Series Firewalls](#).]

- **Global IP allowlist support for all screen options (SRX Series Firewall and vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can configure an allowlist for all IP screen options at a zone level. When you configure an allowlist at a zone level, all the addresses from the specific sources are allowed to bypass the attack detection check. Global IP allowlist supports both IPv4 and IPv6 addresses and a maximum of 32 allowlist groups. You can configure a single address or a subnet address.

[See [White-list \(Security-Zone\)](#), [Understanding Allowlists for All Screen Options](#), and [Screens Options for Attack Detection and Prevention](#).]

High Availability

- **IPv6 Addresses support for BFD monitoring (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can configure Bidirectional Forwarding Detection (BFD) monitoring using IPv6 addresses in a Multinode High Availability setup.

See [[Multinode High Availability](#)].

- **Active-active Multinode High Availability (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can operate Multinode High Availability in active-active mode on SRX1500, SRX4100, SRX4200, and SRX4600 Firewalls.

Multinode High Availability supports IPsec VPN in active-active mode with multiple SRGs (SRG1+). In this mode, you can establish multiple active tunnels from both the nodes, based on SRG activeness. Since different SRGs can be active on different nodes, tunnels belonging to these SRGs come up on both nodes independently. Having active tunnels on both the nodes enables encrypting/decrypting data traffic on both the nodes resulting in efficient use of bandwidth.

See [[Multinode High Availability](#)].

- **Enhancements for Multinode High Availability monitoring features (SRX1500, SRX4100, SRX4200, and SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.4R1, we have added new enhancements for the path monitoring features.

The enhancements add more granular control for the path monitoring by:

- Grouping of monitoring functions
- Monitoring based on the direction (upstream and downstream) associated with an SRG path
- Adding weights associated with each monitoring function
- Monitoring for SRG0 in addition to SRG1+

By grouping related attributes together, the system can process them as a unit, which can lead to more efficient computation and resource utilization.

See [[Path Monitor in Multinode High Availability](#)].

- **Split-brain protection support for BFD- based probing (SRX1500, SRX4100, SRX4200, and SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.4R1, we introduce Bidirectional Forwarding Detection (BFD)-based probing for split-brain protection in Multinode High Availability. This enhancement allows you to use fine-grained control over the probing parameters, providing you the ability to specify the interface, set the minimal-interval, and define the multipliers.

BFD-based probing starts immediately after configuring a service redundancy group (SRG) resulting in quicker response times, providing a significant improvement in the containment of potential split-brain scenarios.

See [[Path Monitor in Multinode High Availability](#)].

- **Support for asymmetric traffic flows in Multinode High Availability (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.4R1, SRX Series Firewalls in Multinode High Availability support asymmetric traffic flows.

While performing deep packet inspection or stateful firewall activity, it is a must that the firewall in the return path have the same state information associated with a packet flow as the state information is built in the originating firewall.

To handle asymmetric traffic flows, the Multinode High Availability requires an additional link known as Inter Chassis Datapath (ICD). ICD has the ability to route the traffic between two nodes. It enables the nodes to redirect asymmetric traffic flows to the peer node that is originally in charge of providing stateful services for these flows.

This feature ensures the completion of TCP security check (such as three-way handshake and sequence check with window scale factor) for asymmetric traffic flows, thereby enhancing the performance and reliability of the network.

See [\[Asymmetric Traffic Flow Support for Multinode High Availability\]](#).

Interfaces

- **Support for VXLAN on flexible tunnel interfaces (SRX Series and vSRX)**—Starting in Junos OS Release 23.4R1, we support VXLAN on flexible tunnel interface (FTI) on Juniper Networks® SRX Series Firewalls (SRX series). To configure FTIs on your device, use the `vxlan-gpe` parameter under the `tunnel-endpoint VXLAN encapsulation` at the `[edit interfaces interface-name unit logical-unit-number tunnel encapsulation]` hierarchy level. When you configure an FTI on SRX series devices, you must also configure the following:
 - A security zone for the FTI.
 - The security policy with security rules for traffic sent to the FTI.

For more information, see [Flexible Tunnel Interfaces Overview](#) and [Configuring Flexible Tunnel Interface on an SRX](#).

J-Web

- **Support for Juniper NextGen Web Filtering (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, **Juniper NextGen** is available at **Security Services > Content Security**:
 - In **Default Configuration**, under **Web Filtering**.
 - In **Web Filtering Profiles > Create Web Filtering Profiles**, under **Engine Type**.

Juniper NextGen intercepts the HTTP and HTTPS traffic and sends URL or destination IP address information to the Juniper NextGen Web Filtering (NGWF) Cloud. The Juniper Networks® SRX Series Firewalls (SRX Series) use URL categorization and site reputation information from the NGWF Cloud to act on traffic.

]See [About the Default Configuration Page](#) and [Add a Web Filtering Profile](#).]

- **Support for migrating to Juniper NextGen (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Migrate to Juniper NextGen** in **Security Services > Content Security > Web Filtering Profiles**. You can use this option to migrate from Juniper Enhanced Web Filtering profile to Juniper NextGen Web Filtering profile.

[See [About the Web Filtering Profiles Page](#).]

- **Support for Juniper NextGen base filter (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **ng-default-filter** base filter in **Device Administration > Security Package Management > URL Categories**. You can click on **ng-default-filter** to view the available Juniper NextGen base filter categories.

[See [About the Security Package Management Page](#).]

- **Support for URL categorization (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports:
 - **Manage URL Categorization** under **URL Categorization** in **Device Administration > Security Package Management > URL Categories**. You can use this page to add a new URL to a category or change the category of an existing URL.
 - **Check URL Categorization Status** under **URL Categorization** in **Device Administration > Security Package Management > URL Categories**. You can use this page to check the URL recategorization status.

[See [Manage URL Categorization](#) and [Check URL Recategorization Status](#).]

- **Support for SRX1600 Firewall (SRX1600)**—Starting in Junos OS Release 23.4R1, J-Web supports SRX1600 Firewall.

[See [The J-Web Setup Wizard](#), [Explore J-Web](#), [Dashboard Overview](#), [Monitor Interfaces](#), and [About Reports Page](#).]

- **Support for internal SA encryption algorithm (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added **Algorithm** under **Internal SA Encryption** in **Network > VPN > IPsec VPN > Global Settings**. The 3DES-CBC algorithm specifies the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec SA configuration. The AES-128-CBC algorithm specifies the encryption algorithm for high availability encryption link.

[See [IPsec VPN Global Settings](#).]

- **Support for IKE HA link (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added **IKE HA Link** under **Internal SA Encryption** in **Network > VPN > IPsec VPN > Global Settings**. You can use this to enable or disable HA link encryption IKE internal messages for chassis cluster devices.

[See [IPsec VPN Global Settings](#).]

- **Support for installation or uninstallation of IKE package (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, you can install or uninstall IKE package on your Juniper Networks® SRX Series Firewall using **Install IKE package** or **Uninstall IKE package**. This option is available in **Network > VPN > IPsec VPN > Global Settings**.

[See [IPsec VPN Global Settings](#).]

- **Support for SNMP Traps (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added the following fields under General in **Network > VPN > IPsec VPN > Global Settings**.
 - IKE SNMP trap—Controls the sending of SNMP traps.
 - Tunnel Down—Generates traps for IPsec tunnel going down only when the associated peer IKE SA is up.
 - Peer Down—Generates traps when peer goes down.

[See [IPsec VPN Global Settings](#).]

- **Support for Internet Control Message Protocol (ICMP) Big Packet Warning (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for **junos-ike package** installed devices, J-Web supports **ICMP big packet warning** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. You can use this option to enable or disable sending ICMP packet too big notifications for IPv6 packets.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for Tunnel MTU (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for **junos-ike package** installed devices, J-Web supports **Tunnel MTU** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. Tunnel MTU specifies the maximum transmit packet size for IPsec tunnels.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for Extended Sequence Number (ESN) (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for **junos-ike package** installed devices, J-Web supports **ESN** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. ESN allows IPsec to use 64-bit sequence number. If ESN is not enabled, 32-bit sequence number is used by default.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **IKE settings enhancements (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the **junos-ike** package installed devices:
 - **SHA 512-bit** IKE authentication algorithm under **IKE Settings** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. Juniper Networks® SRX Series Firewalls use these authentication algorithms to verify the authenticity and integrity of a packet.
 - **Group 15**, **group 16**, and **group 21** DH groups under **IKE Settings** for **IKE Settings** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. A Diffie-Hellman (DH) exchange allows the participants to produce a shared secret value.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **IPsec settings enhancements (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the **junos-ike** package installed devices:
 - **HMAC-SHA 384** and **HMAC-SHA 512** IPsec authentication algorithm under **IPsec Settings** for **IKE Settings** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. SRX Series Firewall uses these authentication algorithms to verify the authenticity and integrity of a packet.
 - **Group 15**, **group 16**, and **group 21** IPsec perfect forward secrecy keys under **IPsec Settings** for **IKE Settings** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. The Juniper Networks® SRX Series Firewalls use this method to generate the encryption key.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for SRX2300 Firewall (SRX2300)**—Starting in Junos OS Release 23.4R1, J-Web supports SRX2300 Firewall.

[See [The J-Web Setup Wizard](#), [Dashboard Overview](#), [Monitor Interfaces](#), and [About Reports Page](#).]

- **Support for IPv6 address (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the **junos-ike** package installed devices:
 - External Interface supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway**.
 - Global Address supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway > Protected Networks > Add**.

- Address assignment supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway > User Authentication > Add**.
- Source Interface supports IPv6 address in **Security Services > Firewall Authentication > Access Profile > Create Access Profile**.

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

- **Support for excluded address ranges (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Excluded Address Ranges** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to exclude a single address or range of addresses.

[See [Add an Address Pool](#).]

- **Support for static address binding (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Static Address Binding** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to assign a specific IP address to a username or MAC address.

[See [Add an Address Pool](#).]

- **Support for linked address pool (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Linked Address Pool** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to create a secondary assignment pool and link it to a primary address assignment pool. The secondary pool provides a backup pool for local address assignment.

[See [Add an Address Pool](#).]

- **Support for LDAP traffic over Secure Sockets Layer/Transport Layer Security (SSL/TLS) technology (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **LDAP over TLS/SSL** in **Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create LDAP Server**. You can set LDAP traffic to be confidential and secure by using Secure Sockets Layer/Transport Layer Security (SSL/TLS) technology.

[See [Add an Access Profile](#).]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Flow-based antivirus solution (SRX Series and vSRX)**—Starting in Junos OS Release 23.4R1, you can use the flow-based antivirus solution to scan your network traffic and prevent threats in real time using a unified pattern-matching engine. With the flow-based antivirus solution, you can:
 - Implement explicit byte-pattern matching on the firewall device to improve the performance and efficiency of your network traffic.
 - Enable inline-blocking capability based on threat intelligence and recent threat detection events.

To enforce flow-based antivirus solution, you must install the Juniper Antivirus license, *Juniper AV* and enable the antivirus policy. Use the `set services anti-virus policy <policy-name>` command to enable the antivirus policy. Apply the antivirus policy to a network firewall policy using the `set security policies from-zone from-zone to-zone to-zone policy policy-name` then permit application-services anti-virus-policy *av-policy* command.

To query the antivirus scan statistics, use the `show services anti-virus statistics` command.

By default, the latest antivirus signature pack is automatically downloaded from the Juniper Networks content delivery network (CDN) server to your firewall device every five minutes. You can also customize the setting by using the `set services anti-virus update automatic interval <5...60>` command.

[See [Example: Configure Flow-based Antivirus Policy](#), [anti-virus](#), [request services anti-virus update](#), and [show services anti-virus statistics](#).]

Junos Telemetry Interface

- **Telemetry streaming with operational state sensors (SRX1500, SRX4100, SRX4200 and SRX4600)**—Starting in Junos OS Release 23.4R1, you can stream statistics through Junos telemetry interface (JTI) to an external collector. Support includes operational state sensors under the following resource paths:

- `/junos/events/junos/task-memory-information/`
- `/interfaces/`
- `/components/`
- `/lcp/`
- `/lldp/`
- `/arp-information/`
- `/nd6-information/`

[See [Junos YANG Data Model Explorer](#).]

- **Streaming flow Session and packet data (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 23.4R1, you can stream flow session and packet data using Junos telemetry interface (JTI) and gRPC Network Management Interface (gNMI) to an outside collector. Distributed sensors with multiple Services Processing Units (SPUs) are supported.

To stream statistics, include one of the following sensors in a subscription:

- `/junos/security/spu/flow/usage/` streams statistics about the security flow session and flow packets for the whole system.

- `/junos/security/spu/flow/lsys/usage/` streams statistics about the security flow session and flow packets for logical systems.

The *spu-name* in the streamed data displays as `node<node-id>:fpc<fpc-id>:pic<pic-id>`. For example, from vSRX and TVP devices, the *spu-name* is

`fpc0:pic0 (no-HA), node0:fpc0:pic0 and node1:fpc0:pic0.`

[For state sensors, see [Junos YANG Data Model Explorer](#).]

Network Address Translation (NAT)

- **Enhanced persistent NAT binding support (SRX4100, SRX4200, and vSRX)**—Starting in Junos OS release 23.4R1, we've increased the number of persistent NAT bindings supported. The increased persistent NAT binding support is based on the available memory and sessions.

The internal host must have previously sent a packet to the external host's IP address. All requests from a specific internal IP address and port are mapped to the same reflexive transport address. Any external host can send a packet to the internal host by sending the packet to the reflexive transport address.

[See [Persistent NAT and NAT64](#).]

- **NAT PBA monitoring (MX240, MX480, MX960, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, we've added the following enhancements:
 - Support for port overloading and index-based port utilization in SNMP MIB table. `jnxJsNatPortOverloadUtilTable`.
 - Support for pool based port utilization MIB object `jnxJsNatPoolUtil` on MX-SPC3.
 - A new trap in the MIB table `jnxJsSrcNatOverloadedPoolThresholdStatus` to alert when the port is overloaded.
 - Support for source NAT PBA table `jnxJsNatPbaStatsTable` in SRX Series Firewall.
 - Display sessions filters:
 - On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.
 - On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm raise-threshold <value>` command.
 - On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.

- On MX-SPC3, use the `set services nat source port-overloading-usage-alarm raise-threshold <value>` command.
- Clear sessions filters:
 - On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
 - On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm clear-threshold <value>` command.
 - On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
 - On MX-SPC3, use the `set services nat source port-overloading-usage-alarm clear-threshold <value>` command.

[See [show security flow session](#), [clear services sessions](#), [show services sessions](#), [clear security flow session](#), [pool \(Security Source NAT\)](#) and [port \(Security Source NAT\)](#).]

Network Management and Monitoring

- **On-box reporting and Logging Enhancement (cSRX, SRX Series Firewall, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, we've made the following enhancements to the on-box reporting and logging feature:
 - Option to limit number of users in application visibility CLI
 - Additional filters support for on-box reporting feature.

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

Public Key Infrastructure (PKI)

- **Support for dynamic update of trusted CA bundle for SSL proxy (SRX Series, cSRX, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support dynamic update of default trusted CA certificates for SSL proxy. Earlier in Junos OS Release 23.2R1, we introduced dynamic update of default trusted CA certificates for Junos OS devices. In the current release, we've made the following enhancements:
 - The Juniper content delivery network (CDN) server (<http://signatures.juniper.net/cacert>) is up to date with the latest copy of trusted CA certificates.
 - The SSL proxy on your SRX Series Firewall uses the latest trusted CA certificate from the default trusted CA bundle downloaded to your device from the CDN server.

With this feature, we ensure authenticity, confidentiality, and integrity of SSL proxy-based communication.

[See [Configuring a Trusted CA Profile Group](#).]

VPNs

- **Support for ADVPN with ike process (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support the Auto Discovery VPN (ADVPN) configuration on firewalls that run the ike process for the IPsec VPN service. With the ike process, you can continue to configure advpn at the [edit security ike gateway *gateway-name*] hierarchy level.

[See [Auto Discovery VPNs](#).]

- **Support for lifetime-kilobytes, install-interval, and idle-time options with ike process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support the idle-time, install-interval, and lifetime-kilobytes options on firewalls that run the ike process for the IPsec VPN service.

You can continue to configure the following options:

- lifetime-kilobytes at the [edit security ipsec proposal *proposal-name*] hierarchy level.
- idle-time and install-interval at the [edit security ipsec vpn *vpn-name*] hierarchy level.

[See [ike \(Security IPsec VPN\)](#) and [proposal \(Security IPsec\)](#).]

- **Support for multiple peer addresses in DPD configuration with ike process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, when your firewall runs the ike process for the IPsec VPN service, the IKE connection supports multiple peer addresses per gateway, ensuring DPD failover. You must configure the dead-peer-detection option at the [edit security ike gateway *gateway-name*] hierarchy level before configuring multiple peer addresses. You can use the address option at the same hierarchy level to configure multiple peer addresses.

Note the following behavior with the DPD failover feature:

- You can configure one active peer and up to four backup peer addresses.
- If the first peer address, which is the active peer, is not reachable, the IKE protocol negotiates with the next available peer based on the order of peer address configuration. You'll notice traffic disruption when DPD failover is in progress with the current active peer unreachable.

[See [gateway \(Security IKE\)](#), [dead-peer-detection](#), and [Dead Peer Detection](#).]

- **Support for robust protection against DDoS attacks on IKE protocol with ike process (MX240, MX480, and MX960 with SPC3, SRX1500, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, you can efficiently monitor and mitigate DDoS

attacks on IKEv1 and IKEv2 protocols when your firewall runs the `iked` process for the IPsec VPN service.

To support the feature, we introduce the following configuration statements at the `[edit security ike]` hierarchy level:

- **session**—Tune parameters to manage the behavior of negotiations with the remote peers to protect the security associations. Configure the parameters at the `[edit security ike session half-open]` and `[edit security ike session full-open]` hierarchy levels.
- **blocklists**—Define multiple blocklists and their associated rules for blocking an IKE ID. Configure the blocklists at the `[edit security ike session blocklists]` hierarchy level. You must attach a blocklist to one or more IKE policies at the `[edit security ike policy policy-name blocklist blocklist-name]` hierarchy level.

Use the following commands to view and clear statistics and other details about the in-progress, failed, blocked, and backoff peers:

- `show security ike peer statistics` and `show security ike peer`.
- `clear security ike peers statistics` and `clear security ike peers`.

[See [IKE Protection from DDoS Attacks](#), [session \(Security IKE\)](#), [blocklists \(Security IKE\)](#), [show security ike peers statistics](#), [show security ike peers](#), [clear security ike peers statistics](#), and [clear security ike peers](#).]

- **Support for VPN monitoring and datapath verification with the `iked` process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support VPN monitoring and datapath verification on firewalls that run the `iked` process for the IPsec VPN service. With the `iked` process, you can continue to configure `vpn-monitor` and `verify-path` at the `[edit security ipsec vpn vpn-name]` hierarchy level.

We provide the following enhancements with the feature:

- Configuration and deletion of VPN monitoring functionality on an active tunnel does not cause any service disruption.
- After you've configured VPN monitoring, the functionality is active only after the tunnel is up.
- Configuration of `verify-path` on an active tunnel causes service disruption and performs renegotiation after the tunnel is down.

[See [vpn-monitor](#), [verify-path](#), and [VPN Tunnel Monitoring](#).]

Additional Features

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

- **Support for firewall filter flexible match conditions** (SRX4600, SRX5400, SRX5600, and SRX5800)

[See [Firewall Filter Flexible Match Conditions](#).]

What's Changed

IN THIS SECTION

- [Content Security](#) | 190
- [J-Web](#) | 191
- [Junos XML API and Scripting](#) | 191
- [Network Management and Monitoring](#) | 192
- [User Interface and Configuration](#) | 192
- [VPNs](#) | 192

Learn about what changed in this release for SRX Series Firewalls.

Content Security

- **Avira antivirus scanning mode supported on SRX1600 device (SRX1600)**—SRX1600 device supports the Avira antivirus scan in light mode only and it does not support the heavy mode. Therefore, we've removed the `onbox-av-load-flavor` statement at the `edit chassis` hierarchy level for SRX1600 device.

See [Example: Configure Avira Antivirus](#).

- **URL check operational command update (SRX Series)**—Starting in Junos OS Release 23.4R1, you can use the `test security utm web-filtering url-check test` command to check the category and reputation of a URL. Earlier to this release the `test security utm enhanced-web-filtering url-check test` command was used to check the category and reputation of a URL.

See [test security utm enhanced-web-filtering url-check](#).

J-Web

- **Updated Security Package URL (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've updated the security package URL in **Device Administration > Security Package Management > URL Categories Settings**. You can use this URL to download Juniper NextGen or Juniper Enhanced Web Filtering package.

[See [URL Categories Settings](#).]

- **Internal SA is now called Internal SA Encryption (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Internal SA** to **Inter SA Encryption** and **Internal SA Keys** to **Key** in **Network > VPN > IPsec VPN > Global Settings**.

[See [IPsec VPN Global Settings](#).]

- **Name is now called Identifier (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Name** to **Identifier** and **Network Address** to **Subnet** in **Security Services > Firewall Authentication > Address Pools**.

[See [About the Address Pools Page](#).]

- **Address Range is now called Named Address Ranges (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Address Range** to **Named Address Ranges** in **Security Services > Firewall Authentication > Address Pools**.

[See [About the Address Pools Page](#).]

- **Routing Instance is now called Source Virtual Router (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Routing Instance** to **Source Virtual Router** and **Source Address** to **Source Interface** in **Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create Radius Server and Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create LDAP Server**.

[See [Add an Access Profile](#).]

Junos XML API and Scripting

- **XML output tags changed for request-commit-server-pause and request-commit-server-start (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the request system commit server pause command (request-commit-server-pause RPC) and the request system commit server

start command (request-commit-server-start RPC). The root element is <commit-server-operation> instead of <commit-server-information>, and the <output> tag is renamed to <message>.

Network Management and Monitoring

- **NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.

[See [<copy-config>](#).]

User Interface and Configuration

- **Viewing files with the file compare files command requires users to have maintenance permission** —The file compare files command in Junos OS and Junos OS Evolved requires a user to have a login class with maintenance permission.

[See [Login Classes Overview](#).]

VPNs

- **Invalid kmd-instance option when iked is enabled for IPsec VPNs (SRX Series)**—We have removed the option kmd-instance when you enable the iked process using junos-iked package for running IPsec VPN features in Junos OS Release 23.4R1. This option is applicable when you have kmd process for IPsec VPN features.

[See [show security ipsec security-associations](#).]

- **Options related to FPC, PIC and KMD instance are invalid in show security ike sa command with IKED process (SRX Series)**—With junos-ike package installed for running IPsec VPN using IKED process, the options fpc, pic and kmd-instance will not be seen in show security ike security-associations hierarchy. These options are invalid and removed from the CLI from Junos OS Release 23.4R1. This means, you cannot use show security ike sa fpc 0 pic 0 command with IPsec VPN running IKED process on your SRX Series Firewall.

[See [show security ike security-associations](#).]

- **Enhancements to IKE configuration management for clearing IKE stats on secondary node (SRX Series)**—In Earlier Junos OS Releases, in a Chassis Cluster mode, the ike-config-Management (IKEMD) process did not respond to management requests on the secondary node. The command `clear security ike stats`, fails with the error message error: IKE-Config-Management not responding to management requests on the secondary node. Starting in Junos OS Release 22.4R3, the command runs successfully without the error on the secondary node.
- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)**—We've introduced the extensive option for the `show security ipsec security-associations` command. Use this option to display IPsec security associations with all the tunnel events. Use the existing detail option to display upto ten events in reverse chronological order.

[See [show security ipsec security-associations](#).]

- **Enhancements to address CA certificate validation failure (SRX Series and vSRX 3.0)**—For the CA certificates, the certificate validation fails with the Lets Encrypt server when using the configuration statement `set security pki ca-profile ISRG revocation-check crl url` as PKI sends the OCSP request on HTTP 1.0 with the *requestorName*. We made modifications to the behaviour in order to send the OCSP request using HTTP 1.1 without the *requestorName* by default.
 - To send the *requestorName* when using HTTP 1.1, use the hidden option `add-requestor-name-payload` at the `edit security pki ca-profile ca-profile-name revocation-check ocsf hierarchy level`.
 - To send the OCSP request using the HTTP 1.0, use the hidden option `use-http-1.0` at the `edit security pki ca-profile ca-profile-name revocation-check ocsf hierarchy level` to ensure backward compatibility.

[See [revocation-check \(Security PKI\)](#).]

- **Enhancements to the IKE configuration management commands in chassis cluster (SRX Series)**—In earlier Junos OS releases, in a chassis cluster mode, the following commands failed with the error message error: IKE-Config-Management not responding to management requests on the secondary node:
 - `show security ike statistics`
 - `show security ike sa ha-link-encryption`
 - `show security ipsec sa ha-link-encryption`
 - `show security ipsec inactive-tunnels ha-link-encryption`
 - `clear security ike sa ha-link-encryption`
 - `clear security ipsec sa ha-link-encryption`

You should run these commands only on the primary node rather than the secondary node. Starting in Junos OS Release 23.4R1, you'll not see the error message as the secondary node has no output to display.

- **Enhancements to the output of show security ipsec security-associations detail command (SRX Series and vSRX 3.0)**—We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the `edit security ipsec vpn vpn-name` hierarchy level, when your firewall runs IPsec VPN services with the new `iked` process. The output displays threshold and interval values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

[See [show security ipsec security-associations](#).]

- **Modification to the XML tags for show security ipsec commands (SRX Series and vSRX 3.0)**—We've changed the XML tags for the following commands at `show security ipsec`.

Command	New XML Tag	Old XML Tag
<code>show security ipsec tunnel-events-statistics display xml validate</code>	<code>ipsec-tunnel-event-statistics</code>	<code>usp-ipsec-tunnel-event-statistics-information</code>
<code>show security ipsec inactive-tunnels detail display xml validate</code>	<code>ipsec-unestablished-tunnel-information</code>	<code>ipsec-security-association-information</code>

Starting in Junos OS Release 23.4R1, with the new XML tags, you'll notice that the `show security ipsec commands` emits valid XML.

Known Limitations

IN THIS SECTION

- [General Routing | 195](#)
- [Infrastructure | 195](#)

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

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

General Routing

- We recommended to use IGP shortcut with strict SPF SIDs in SR-TE path. [PR1697880](#)

Infrastructure

- When upgrading from releases before Junos OS Release 21.2 to Junos OS Release 21.2 and onward, validation and upgrade might fail. The upgrade requires using the 'no-validate' option to complete successfully. <https://kb.juniper.net/TSB18251> [PR1568757](#)

Open Issues

IN THIS SECTION

- [Authentication and Access Control | 195](#)
- [General Routing | 196](#)
- [VPNs | 196](#)

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

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

Authentication and Access Control

- The authentication entries on SRX Series Firewalls might be lost during ISSU or during Junos OS version upgrades to Junos OS Release 23.1 or to Junos OS Release 23.4 from prior versions. The issue is because of upgrades done to authentication database on the new Junos OS versions. As a

workaround, recreate user event on clearpass after the upgrade, or configure clearpass user-query with inline-lookup configured to trigger user-reauthentication. [PR1732210](#)

General Routing

- When non-root user tries to generate archive file for /var/log, it either fails or generates an archive with partial log files. This happens due to permission of files under /var/log/hostlogs/. [PR1692516](#)
- When input traffic is more and output traffic is expected equal to maximum capacity of egress interface, set the shaping explicitly equal to interface maximum capacity if default shaping does not work. [PR1712964](#)
- The NSD process might generate core files. [PR1716686](#)

VPNs

- When multiple VPNs have same TS and different st0, in on-traffic tunnel establishment, ARI routes for the same destination and different st0 gets overwritten and only the latest route will be added. As a result, traffic over only one VPN continues and other VPN is down. In case of DPD failover, when one of the VPN is down and peer initiates DPD failover to route traffic via other VPN, due to missing ARI route on responder-side, traffic will be down. As a work-around, for DPD failover to work seamlessly, configure 2 st0s in different VRFs so both routes can be installed and failover can continue to work. [PR1727795](#)
- On SRX1600 and SRX2300, the SCTP over IPSEC tunnel does not work. [PR1778106](#)

Resolved Issues

IN THIS SECTION

- [Chassis Clustering | 197](#)
- [Class of Service \(CoS\) | 197](#)
- [Flow-Based and Packet-Based Processing | 197](#)
- [General Routing | 198](#)

- [Intrusion Detection and Prevention \(IDP\) | 200](#)
- [J-Web | 200](#)
- [Layer 2 Ethernet Services | 200](#)
- [Platform and Infrastructure | 201](#)
- [Routing Protocols | 201](#)
- [Content Security | 201](#)
- [User Interface and Configuration | 201](#)
- [VPNs | 201](#)

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

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

Chassis Clustering

- Unsupported configuration for interface st0 16000 to 16385 is possible when using replace pattern on SRX Series Firewall devices. [PR1731593](#)
- In SRX MNHA cluster setup the RSI takes long time to generate. [PR1736498](#)
- BFD session fails to re-establish on SRX cluster mode. [PR1737520](#)
- SRX dropping GTP ChangeNotificationRequest messages due to Non-zero TID or TEID. [PR1750988](#)

Class of Service (CoS)

- The CoS scheduler map might not get attached to the sub-interface correctly when shaping-rate and scheduler-map are configured. [PR1734013](#)

Flow-Based and Packet-Based Processing

- The datapath-debug packet-dump feature is not capturing the transit traffic packets. [PR1727027](#)

- Traffic loss is observed for the existing session if there is an update for the next-hop MAC address. [PR1755181](#)
- Buffer leak when PMI sends out packet on egress interface with MTU smaller than the packet length. [PR1758208](#)
- In NAT46 or NAT64 scenario, the packet that trigger NDP or ARP learning might get dropped. [PR1759202](#)
- Source port for GTPv2 traffic is copied as same as destination port for the create session response packet. [PR1771176](#)

General Routing

- The mustd process might stop. [PR1562848](#)
- The 8-Port GbE SFP XPIM not passing traffic after software upgrade. [PR1620982](#)
- The DNS information is getting lost when IPCP flaps. [PR1658968](#)
- The fxp0 interface works under disable state in SRX300. [PR1661816](#)
- Secondary node goes into disabled state after failover due to control link going down in a cluster. [PR1703220](#)
- High latency will be observed while pinging to peer device. [PR1714620](#)
- Interface speed stays 100 Mbps when removing speed and duplex command separately. [PR1715247](#)
- OAM not working with flexible-vlan-tagging. [PR1719108](#)
- The show system firmware shows available version as 0 after upgrading to BSD12 image. [PR1729959](#)
- The flowd-octeon.elf.core generates core files rarely in SRX380 cluster. [PR1732378](#)
- Intermittent core files are received when SMB protocol is enabled on AAMW policy and Packet Forwarding Engine memory is exhausted. [PR1737442](#)
- Junos OS installation using USB can fail on SRX4600. [PR1737721](#)
- Failover can be seen on SRX5000 line of devices cluster with SPC2 cards while executing RSI. [PR1738188](#)
- Minor autorecovery information needs to be saved alarm are not displayed after zeroize. [PR1738271](#)

- Traffic drop caused by Packet Forwarding Engine memory leak on SRX Series Firewall devices. [PR1738656](#)
- With multiple, reboot SRX300 going into sleep thread. [PR1739219](#)
- Memory leak in PKID. [PR1739342](#)
- Random physical interfaces doesn't come up after a reboot. [PR1739520](#)
- SRX4100 and SRX4200 accepts the datapath-debug configuration although it does not support it. [PR1739559](#)
- Existing primary node not upgraded or rebooted, secondary node got upgraded but PICs didn't came online and vmcore.live.0 generated. [PR1739673](#)
- Processing a TWAMP packet and terminating the TWAMP session might generate core files in a corner case scenario. [PR1739733](#)
- The flowd process might pause. [PR1743107](#)
- Commit panic reboot observed after implementing system processes watchdog timeout 180 on SRX Series Firewall devices. [PR1744108](#)
- Added FQDN-name counter in the show services user-identification identity-management status output. [PR1745588](#)
- The traffic degradation in 25percentercent down might be seen under high load traffic at SRX4600 with FPGA v1.65. [PR1746567](#)
- SRX4600 misleading fan speed syslog output after removing or inserting one fan tray unit. [PR1748971](#)
- SRX Series Firewall devices might take time to come up in HA or device will go down in standalone setup. [PR1749584](#)
- SPC3 PIC pause. [PR1749830](#)
- Large TLS1.3 session tickets to an SRX SPC3 device result in srxpfe process pause. [PR1752678](#)
- The flowd process might pause due to memory stress. [PR1753540](#)
- Users authenticated through captive portal experience a noticeable delay of at least 2 to 5 minutes. [PR1755593](#)
- The Packet Forwarding Engine or flowd process might stop when NAT and tcp-encap is enabled. [PR1756193](#)
- Changing IKE GW address from IPv6 to IPv4 causes failure in tunnel distribution during next tunnel establishment. [PR1757072](#)

- AAMW hyper scan goes to lock state during reload. [PR1757794](#)
- Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution [PR1758332](#)
- False SNMP traps for PSU failure generated on SRX4100 and SRX4200 platforms [PR1761668](#)
- The set system license log-frequency time-interval command does not work. [PR1766874](#)
- ARP is not getting resolved. [PR1768050](#)

Intrusion Detection and Prevention (IDP)

- Multiple network issues are seen after the upgrade with lower IDP packet-log total-memory percentage. [PR1741887](#)

J-Web

- The process httpd might pause on SRX Series Firewall devices. [PR1732269](#)
- Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845) [PR1736942](#)
- Certificate Management issues. [PR1738316](#)
- Cannot add custom defined security address-book under Security Policies Objects > Security Policies > Create > Source Zone > Select Sources. [PR1748078](#)
- Junos upgrades from J-Web returns failed in each step. [PR1755072](#)

Layer 2 Ethernet Services

- Delay in getting IP through DHCP cause traffic loss. [PR1752804](#)

Platform and Infrastructure

- The message "kernel: %KERN-6:ARP UNICAST MODE 0; retrans_timer - 8" might be seen when commit command is run for configuration which is not related to ARP. [PR1735686](#)

Routing Protocols

- BFD session for BGP remains down in a specific scenario. [PR1738074](#)
- RPD scheduler slip is observed when the BGP session flaps and subsequent configuration changes for the same peer. [PR1742416](#)
- When BGP is configured in routing-instance of type virtual-router, default MPLS table is being created for that virtual-router, unexpectedly. [PR1742513](#)
- System reboot or IPsec restart causes routes with incorrect next hop interface to be installed in the routing table. [PR1752133](#)

Content Security

- Outlook notification channel connection is not established. [PR1725938](#)

User Interface and Configuration

- The mgd process generates core files when show command is executed from the configuration mode. [PR1745565](#)

VPNs

- The show security ike tunnel-map command is invalid with IKED. [PR1738335](#)
- The show security ike sa fpc 0 pic 0 command is invalid with IKED. [PR1739494](#)
- IPsec VPN does not come up in NAT-T scenario. [PR1745174](#)
- Error seen while clearing ike statistics in secondary node. [PR1748531](#)

- After clearing security group-vpn member ike SA, IKE SA goes down traffic disruption is observed.
[PR1758940](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 202

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

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

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

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

We have two types of releases, EOL and EEOL:

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

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

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

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

Table 9: EOL and EEOL Releases

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

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

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

Documentation Updates

IN THIS SECTION

- [Guide Name Change](#) | 203

This section lists the errata and changes in Junos OS Release 23.4R1 for the SRX Series Firewalls documentation.

Guide Name Change

The *Authentication and Integrated User Firewalls User Guide* has been renamed *Identity Aware Firewall User Guide* in Junos OS Release 23.4R1. For more information, see [Identity Aware Firewall Guide](#).

The following enhancements and additions apply to the Guide:

- [Overview of Identity Aware Firewall](#)
- [Active Directory as Identity Source](#)

Junos OS Release Notes for vRR

IN THIS SECTION

- [What's New | 205](#)
- [What's Changed | 207](#)
- [Known Limitations | 207](#)
- [Open Issues | 207](#)
- [Resolved Issues | 207](#)



NOTE: Junos OS Release 23.4R1 is the last-supported release for the following SKUs:

Product Line	SKUs	Junos OS Release
vRR	S-VRR-V-L	Junos OS Release 23.4R1
vRR	S-VRR-V-L-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-L-3Y	Junos OS Release 23.4R1
vRR	S-VRR-V-M	Junos OS Release 23.4R1

(Continued)

Product Line	SKUs	Junos OS Release
vRR	S-VRR-V-M-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-M-3Y	Junos OS Release 23.4R1
vRR	S-VRR-V-S	Junos OS Release 23.4R1
vRR	S-VRR-V-S-1Y	Junos OS Release 23.4R1
vRR	S-VRR-V-S-3Y	Junos OS Release 23.4R1

What's New

IN THIS SECTION

- [Junos Telemetry Interface | 205](#)

Learn about new features introduced in this release for vRR.

Junos Telemetry Interface

- **Resource Public Key Infrastructure (RPKI) enhanced streaming telemetry support (MX480 and vRR)**—Starting in Junos OS Release 23.4R1, we now support enhanced statistics for RPKI databases and RPKI sessions and validation-related statistics per route, per RIB and per BGP peer basis. Using these

statistics, you can perform operational debugging on your network and take appropriate mitigating actions.

These existing Junos operational mode commands contain new statistics:

- `show route [extensive|detail]` displays origin validation information for each route entry
- `show bgp neighbor validation statistics <peer>` displays BGP peer-RIB validation statistics
- `show route validation-statistics` displays local routing information base (RIB) specific validation statistics
- `show validation statistics` displays new counters for the Validated Route Payload (VRP) table

We now support the following telemetry sensors (with leaves):

- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/routes/route/origin-validation-state`
- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/routes/route/origin-validation-invalid-reason`
- `/state/routing-instances/routing-instance/protocols/bgp/groups/group/neighbors/neighbor/afi-safis/afi-safi[ipv4|ipv6]/validation-counters/`
- `/state/routing-instances/routing-instance/protocols/bgp/groups/group/neighbors/neighbor/afi-safis/afi-safi[ipv4|ipv6]/validation-counters`
- `/state/routing-instances/routing-instance/protocols/bgp/rib/afi-safis/afi-safi/[ipv4|ipv6]-unicast/loc-rib/validation-counters/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/rpki-rtr/groups/group/sessions/session/rpki-session-counters/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/route-validation-databases/route-validation-database/[ipv4|ipv6]/`
- `/state/routing-instances/routing-instance/routing-options/route-validation/rpki-rtr/groups/group/sessions/session/`

[For sensors, see [Junos YANG Data Model Explorer](#).] For operational mode commands, see [show route](#), [show bgp neighbor validation statistics](#), [show route validation-statistics](#), and [show validation statistics](#).

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 23.4R1, see "[Known Limitations](#)" on page 85 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

There are no resolved issues 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.

Junos OS Release Notes for vSRX Virtual Firewall

IN THIS SECTION

- [What's New | 208](#)
- [What's Changed | 220](#)
- [Known Limitations | 224](#)
- [Open Issues | 224](#)
- [Resolved Issues | 224](#)
- [Migration, Upgrade, and Downgrade Instructions | 226](#)

What's New

IN THIS SECTION

- [Application Identification \(AppID\) | 209](#)
- [Authentication and Access Control | 209](#)
- [Content Security | 210](#)
- [Device Security | 210](#)
- [Flow-based and Packet-based Processing | 211](#)
- [J-Web | 212](#)
- [Juniper Advanced Threat Prevention Cloud \(ATP Cloud\) | 216](#)
- [Network Address Translation \(NAT\) | 216](#)
- [Platform and Infrastructure | 217](#)
- [Public Key Infrastructure \(PKI\) | 218](#)
- [VPNs | 218](#)

Learn about new features introduced in this release for vSRX Virtual Firewall.

Application Identification (AppID)

- **Subject Alternative Name in custom application signatures (SRX Series Firewalls, vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can create an application identification (AppID) custom signature using the Subject Alternative (SAN) certificate attribute for SSL signatures. You can use the SAN attribute to specify multiple host names or IP addresses in a single certificate. With this enhancement, custom application signatures can detect applications based on the application's host names listed in the SAN field of the SSL certificate.

You can configure SAN using the `ssl-subject-alt-name` option under `[edit services application-identification application name over SSL signature name member name context]` hierarchy.

See [\[Context \(Application Signatures\)\]](#).

- **Micro-applications enhancements (SRX Series Firewalls and vSRX)**—Starting in Junos OS Release 23.4R1, we've enhanced the detection of micro-applications. Application identification (AppID) now uses string-based attributes of the application for matching micro-applications in addition to using the integer-based attributes of application.

You can now manage applications with a finer level of control at the sub-function level.

See [\[Application Identification Support for Micro-Applications\]](#).

Authentication and Access Control

- **Dynamic filter IPv6 support**—Starting in Junos OS Release 23.4R1, you can install filters having destination IPv6 as a match condition. Both IPv4 and IPv6 match conditions can be specified within the same filter.

[See [User Access and Authentication Administration Guide for Junos OS](#) .]

- **Support for firewall users log off, custom logo and banner (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, firewall users can log off using the logoff button displayed in captive portal after a successful login.

SRX and NFX administrators can set custom logo for captive portal. SRX and NFX administrators can configure custom login-success, login-fail banner messages in captive-portal. You can configure logo option under `set access firewall-authentication web-authentication hierarchy level` for custom-logo. You can configure banner option under `set access firewall-authentication web-authentication hierarchy level` for banner messages.

[See [firewall-authentication](#).]

- **Support for client/server certificate validation using TLS protocol mutual authentication (SRX Series Firewalls, vSRX3.0, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, a client can authenticate without password based on client/server certificate validation using Mutual-TLS authentication. You can configure `mtls-profile` option at the `set security firewall-authentication hierarchy level`.

[See [firewall-authentication \(Security\)](#).]

- **Support for destination identity in firewall policy (SRX Series Firewalls, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, you can control network access based on destination identity in security policy. You can match the traffic based on destination identity information. You can configure `destination-identity-context` option at the set security policies from-zone *zone-name* to-zone *zone-name* match hierarchy level.

You can configure `identity-context-profile` *profile-name* option at the set user-identification device-information hierarchy level. You can configure `destination-identity-context-profile` option at the set security policies from-zone *zone-name* to-zone *zone-name* match hierarchy level.

[See [user-identification \(Services\)](#), [match \(Security Policies\)](#), [identity-context-profile](#), [destination-identity-context](#), and [destination-identity-context-profile](#).]

Content Security

- **URL feed support for Content Security (SRX Series and vSRX)**—Starting in Junos OS Release 23.4R1, we introduce URL feed for Content Security. The URL feed reduces your effort to add multiple URLs into a single URL pattern automatically. You should add the URLs that need to be added in the URL pattern to the URL feed file saved in the HTTPS server. When you configure the URL feed, the system downloads the file from the HTTPS server and creates the URL pattern automatically.

[See [url-feed](#), [request security utm custom-objects url-feed update feed-name](#), [request security utm custom-objects url-feed update feed-name force](#), and [show security utm custom-objects url-feed status feed-name](#).]

Device Security

- **Pre-ID default policy enhancements (SRX Series Firewalls and vSRX Virtual Firewall)**—Starting in Junos OS Release 23.4R1, the Pre-ID default policy (`pre-id-default-policy`) denies the flow before performing application identification (AppID) when there are no potential policies to permit the flow.

When the device receives the first packet of a traffic flow, it performs a basic 5-tuple matching and checks the defined potential policies to determine how to treat the packet. If all potential policies have action as "deny", and the default policy action is also set to "deny", then the device denies the traffic and does not perform application identification.

If any policy has action other than "deny", then the device performs deep packet inspection (DPI) to identify the application.

The device checks for potential policies on both zone context and global context.

See [[Pre-id-default-policy](#)].

- **Security Policy Support for Explicit Web Proxy (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support explicit web proxy profile security policy. The

Juniper Networks® SRX Series Firewalls apply security enforcement based on the rules created in the explicit web proxy profile policy.

The explicit proxy profile policy can enforce fine-grained rules to filter and inspect the web traffic.

See [\[Explicit Web Proxy\]](#).

- **User authentication for Explicit Proxy (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support firewall LDAP-based user authentication to control user access to the network for explicit web-proxy deployments. We support web authentication with web redirection and usage of captive portals.

With explicit web proxy authentication in place, when a user first connects to the proxy server, the browser is prompted to provide their credentials. The explicit proxy then verifies the username and password with the LDAP server. If the credentials are valid, the proxy grants access to the client and stores their information in the database.

See [\[Explicit Web Proxy\]](#).

- **Explicit Web Proxy support is available for on-premises deployment (SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, Explicit Web Proxy support is available for on-premises deployment use cases on the following platforms:

SRX1500

SRX4100

SRX4200

SRX4600

vSRX3.0

The Explicit Web Proxy feature and the configurations are available by default.

SSL proxy support is required to enable SSL decryption service for explicit proxy sessions.

Flow-based and Packet-based Processing

- **Support drop-flow to prevent security attack - (SRX Series Firewall, vSRX3.0, cSRX, NFX150, NFX250, and NFX350)**—Starting in Junos OS Release 23.4R1, we support a new feature drop-flow to prevent security attack. You can control and limit the number of max-session for the drop-flow. The session in the drop-flow is valid for 4 seconds by default. During a drop-flow, the session state displays as Drop, but in the flow, the state remains as Valid.

The drop-flow feature is enabled by default. To disable the feature, use the `set security flow drop-flow max-sessions 0` command. To delete only the drop-flow feature, use the `run clear security flow session drop-flow` command.

To view the current drop-flow configuration, use the `show security flow drop-flow` command, and the view all the available drop-flow, use the `show security flow session drop-flow` command.

[See [Flow Based Session](#).]

J-Web

- **Support for Juniper NextGen Web Filtering (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, Juniper NextGen is available at **Security Services > Content Security**:
 - In **Default Configuration**, under **Web Filtering**.
 - In **Web Filtering Profiles > Create Web Filtering Profiles**, under **Engine Type**.

Juniper NextGen intercepts the HTTP and HTTPS traffic and sends URL or destination IP address information to the Juniper NextGen Web Filtering (NGWF) Cloud. The Juniper Networks® SRX Series Firewalls (SRX Series) use URL categorization and site reputation information from the NGWF Cloud to act on traffic.

[See [About the Default Configuration Page](#) and [Add a Web Filtering Profile](#).]

- **Support for migrating to Juniper NextGen (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Migrate to Juniper NextGen** in **Security Services > Content Security > Web Filtering Profiles**. You can use this option to migrate from Juniper Enhanced Web Filtering profile to Juniper NextGen Web Filtering profile.

[See [About the Web Filtering Profiles Page](#).]

- **Support for Juniper NextGen base filter (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **ng-default-filter** base filter in **Device Administration > Security Package Management > URL Categories**. You can click on **ng-default-filter** to view the available Juniper NextGen base filter categories.

[See [About the Security Package Management Page](#).]

- **Support for URL categorization (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports:
 - **Manage URL Categorization** under **URL Categorization** in **Device Administration > Security Package Management > URL Categories**. You can use this page to add a new URL to a category or change the category of an existing URL.
 - **Check URL Categorization Status** under **URL Categorization** in **Device Administration > Security Package Management > URL Categories**. You can use this page to check the URL recategorization status.

[See [Manage URL Categorization](#) and [Check URL Recategorization Status](#).]

- **Support for internal SA encryption algorithm (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added **Algorithm** under **Internal SA Encryption** in **Network > VPN > IPsec VPN > Global Settings**. The 3DES-CBC algorithm specifies the encryption algorithm for the internal Routing-Engine-to-Routing-Engine IPsec SA configuration. The AES-128-CBC algorithm specifies the encryption algorithm for high availability encryption link.

[See [IPsec VPN Global Settings](#).]

- **Support for IKE HA link (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added **IKE HA Link** under **Internal SA Encryption** in **Network > VPN > IPsec VPN > Global Settings**. You can use this to enable or disable HA link encryption IKE internal messages for chassis cluster devices.

[See [IPsec VPN Global Settings](#).]

- **Support for installation or uninstallation of IKE package (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, you can install or uninstall IKE package on your Juniper Networks® SRX Series Firewall using **Install IKE package** or **Uninstall IKE package**. This option is available in **Network > VPN > IPsec VPN > Global Settings**.

[See [IPsec VPN Global Settings](#).]

- **Support for SNMP Traps (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've added the following fields under **General** in **Network > VPN > IPsec VPN > Global Settings**.
 - **IKE SNMP trap**—Controls the sending of SNMP traps.
 - **Tunnel Down**—Generates traps for IPsec tunnel going down only when the associated peer IKE SA is up.
 - **Peer Down**—Generates traps when peer goes down.

[See [IPsec VPN Global Settings](#).]

- **Support for Internet Control Message Protocol (ICMP) Big Packet Warning (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for **junos-ike package** installed devices, J-Web supports **ICMP big packet warning** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. You can use this option to enable or disable sending ICMP packet too big notifications for IPv6 packets.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for Tunnel MTU (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for `junos-ike` package installed devices, J-Web supports **Tunnel MTU** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. Tunnel MTU specifies the maximum transmit packet size for IPsec tunnels.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for Extended Sequence Number (ESN) (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, for `junos-ike` package installed devices, J-Web supports **ESN** under **IPsec Settings Advanced Configuration** for **Site-Site to VPN**, **NCP Exclusive Client** and **Juniper Secure Connect**. ESN allows IPsec to use 64-bit sequence number. If ESN is not enabled, 32-bit sequence number is used by default.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **IKE settings enhancements (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the `junos-ike` package installed devices:
 - **SHA 512-bit IKE authentication algorithm under IKE Settings for Site-Site to VPN, NCP Exclusive Client and Juniper Secure Connect.** Juniper Networks® SRX Series Firewalls use these authentication algorithms to verify the authenticity and integrity of a packet.
 - **Group 15, group 16, and group 21 DH groups under IKE Settings for Site-Site to VPN, NCP Exclusive Client and Juniper Secure Connect.** A Diffie-Hellman (DH) exchange allows the participants to produce a shared secret value.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **IPsec settings enhancements (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the `junos-ike` package installed devices:
 - **HMAC-SHA 384 and HMAC-SHA 512 IPsec authentication algorithm under IPsec Settings for IKE Settings for Site-Site to VPN, NCP Exclusive Client and Juniper Secure Connect.** SRX Series Firewall uses these authentication algorithms to verify the authenticity and integrity of a packet.
 - **Group 15, group 16, and group 21 IPsec perfect forward secrecy keys under IPsec Settings for IKE Settings for Site-Site to VPN, NCP Exclusive Client and Juniper Secure Connect.** The Juniper Networks® SRX Series Firewalls use this method to generate the encryption key.

[See [Create a Remote Access VPN—Juniper Secure Connect](#), [Create a Remote Access VPN—NCP Exclusive Client](#), and [Create a Site-to-Site VPN](#).]

- **Support for IPv6 address (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports the following for the junos-ike package installed devices:
 - External Interface supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway**.
 - Global Address supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway > Protected Networks > Add**.
 - Address assignment supports IPv6 address in **Network > VPN > IPsec VPN > Juniper Secure Connect > Local Gateway > User Authentication > Add**.
 - Source Interface supports IPv6 address in **Security Services > Firewall Authentication > Access Profile > Create Access Profile**.

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

- **Support for excluded address ranges (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Excluded Address Ranges** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to exclude a single address or range of addresses.

[See [Add an Address Pool](#).]

- **Support for static address binding (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Static Address Binding** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to assign a specific IP address to a username or MAC address.

[See [Add an Address Pool](#).]

- **Support for linked address pool (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **Linked Address Pool** in **Security Services > Firewall Authentication > Address Pools > Create Address Pool**. You can use this option to create a secondary assignment pool and link it to a primary address assignment pool. The secondary pool provides a backup pool for local address assignment.

[See [Add an Address Pool](#).]

- **Support for LDAP traffic over Secure Sockets Layer/Transport Layer Security (SSL/TLS) technology (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, J-Web supports **LDAP over TLS/SSL** in **Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create LDAP Server**. You can set LDAP traffic to be confidential and secure by using Secure Sockets Layer/Transport Layer Security (SSL/TLS) technology.

[See [Add an Access Profile](#).]

Juniper Advanced Threat Prevention Cloud (ATP Cloud)

- **Flow-based antivirus solution (SRX Series and vSRX)**—Starting in Junos OS Release 23.4R1, you can use the flow-based antivirus solution to scan your network traffic and prevent threats in real time using a unified pattern-matching engine. With the flow-based antivirus solution, you can:
 - Implement explicit byte-pattern matching on the firewall device to improve the performance and efficiency of your network traffic.
 - Enable inline-blocking capability based on threat intelligence and recent threat detection events.

To enforce flow-based antivirus solution, you must install the Juniper Antivirus license, *Juniper AV* and enable the antivirus policy. Use the `set services anti-virus policy <policy-name>` command to enable the antivirus policy. Apply the antivirus policy to a network firewall policy using the `set security policies from-zone from-zone to-zone to-zone policy policy-name then permit application-services anti-virus-policy av-policy` command.

To query the antivirus scan statistics, use the `show services anti-virus statistics` command.

By default, the latest antivirus signature pack is automatically downloaded from the Juniper Networks content delivery network (CDN) server to your firewall device every five minutes. You can also customize the setting by using the `set services anti-virus update automatic interval <5...60>` command.

[See [Example: Configure Flow-based Antivirus Policy](#), [anti-virus](#), [request services anti-virus update](#), and [show services anti-virus statistics](#).]

Network Address Translation (NAT)

- **Enhanced persistent NAT binding support (SRX4100, SRX4200, and vSRX)**—Starting in Junos OS release 23.4R1, we've increased the number of persistent NAT bindings supported. The increased persistent NAT binding support is based on the available memory and sessions.

The internal host must have previously sent a packet to the external host's IP address. All requests from a specific internal IP address and port are mapped to the same reflexive transport address. Any external host can send a packet to the internal host by sending the packet to the reflexive transport address.

[See [Persistent NAT and NAT64](#).]

- **NAT PBA monitoring (MX240, MX480, MX960, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, we've added the following enhancements:
 - Support for port overloading and index-based port utilization in SNMP MIB table. `jnxJsNatPortOverloadUtilTable`.

- Support for pool based port utilization MIB object **jnxJsNatPoolUtil** on MX-SPC3.
- A new trap in the MIB table **jnxJsSrcNatOverloadedPoolThresholdStatus** to alert when the port is overloaded.
- Support for source NAT PBA table **jnxJsNatPbaStatsTable** in SRX Series Firewall.
- Display sessions filters:
 - On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.
 - On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm raise-threshold <value>` command.
 - On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm raise-threshold <value>` command.
 - On MX-SPC3, use the `set services nat source port-overloading-usage-alarm raise-threshold <value>` command.
- Clear sessions filters:
 - On SRX Series Firewall devices at source NAT, use the `set security nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
 - On SRX Series Firewall devices, use the `set security nat source port-overloading-usage-alarm clear-threshold <value>` command.
 - On MX-SPC3 at source NAT, use the `set services nat source pool <pool_name> port port-overloading-usage-alarm clear-threshold <value>` command.
 - On MX-SPC3, use the `set services nat source port-overloading-usage-alarm clear-threshold <value>` command.

[See [show security flow session](#), [clear services sessions](#), [show services sessions](#), [clear security flow session](#), [pool \(Security Source NAT\)](#) and [port \(Security Source NAT\)](#).]

Platform and Infrastructure

- **Support for AMD processor (vSRX 3.0)**—Starting in Junos OS Release 23.4R1, vSRX 3.0 supports AMD-based instances on on-prem servers running AMD based processors.

AMD processors provide better performance with scale out benefits compared to other processors and reduce the Total Cost of Ownership (TCO) with higher performance on AMD 64 core.

[See [Requirements for vSRX Virtual Firewall on AWS](#) and [AMD vs Intel Market Share](#).]

- **Support for RHEL 9 (vSRX 3.0)**—Starting in Junos OS Release 23.4R1, vSRX 3.0 supports RHEL 9. You can launch vSRX 3.0 on RHEL 9 using libvirt or kubevirt.

Deploying vSRX using “kubevirt” simplifies security deployments and operations on K8S-based infrastructures. Also, you can manage or orchestrate vSRX 3.0 using “kubevirt” in K8s environment and enable variety of Life Cycle Management (LCM) use cases.

[See [Requirements for vSRX Virtual Firewall on KVM | vSRX | Juniper Networks.](#)]

Public Key Infrastructure (PKI)

- **Support for dynamic update of trusted CA bundle for SSL proxy (SRX Series, cSRX, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support dynamic update of default trusted CA certificates for SSL proxy. Earlier in Junos OS Release 23.2R1, we introduced dynamic update of default trusted CA certificates for Junos OS devices. In the current release, we've made the following enhancements:
 - The Juniper content delivery network (CDN) server (<http://signatures.juniper.net/cacert>) is up to date with the latest copy of trusted CA certificates.
 - The SSL proxy on your SRX Series Firewall uses the latest trusted CA certificate from the default trusted CA bundle downloaded to your device from the CDN server.

With this feature, we ensure authenticity, confidentiality, and integrity of SSL proxy-based communication.

[See [Configuring a Trusted CA Profile Group.](#)]

VPNs

- **Support for ADVPN with ike process (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4300, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support the Auto Discovery VPN (ADVPN) configuration on firewalls that run the ike process for the IPsec VPN service. With the ike process, you can continue to configure advpn at the [edit security ike gateway *gateway-name*] hierarchy level.

[See [Auto Discovery VPNs.](#)]

- **Support for lifetime-kilobytes, install-interval, and idle-time options with ike process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support the idle-time, install-interval, and lifetime-kilobytes options on firewalls that run the ike process for the IPsec VPN service.

You can continue to configure the following options:

- lifetime-kilobytes at the [edit security ipsec proposal *proposal-name*] hierarchy level.
- idle-time and install-interval at the [edit security ipsec vpn *vpn-name*] hierarchy level.

[See [ike \(Security IPsec VPN\)](#) and [proposal \(Security IPsec\)](#).]

- **Support for multiple peer addresses in DPD configuration with ike process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, when your firewall runs the ike process for the IPsec VPN service, the IKE connection supports multiple peer addresses per gateway, ensuring DPD failover. You must configure the dead-peer-detection option at the [edit security ike gateway *gateway-name*] hierarchy level before configuring multiple peer addresses. You can use the address option at the same hierarchy level to configure multiple peer addresses.

Note the following behavior with the DPD failover feature:

- You can configure one active peer and up to four backup peer addresses.
- If the first peer address, which is the active peer, is not reachable, the IKE protocol negotiates with the next available peer based on the order of peer address configuration. You'll notice traffic disruption when DPD failover is in progress with the current active peer unreachable.

[See [gateway \(Security IKE\)](#), [dead-peer-detection](#), and [Dead Peer Detection](#).]

- **Support for robust protection against DDoS attacks on IKE protocol with ike process (MX240, MX480, and MX960 with SPC3, SRX1500, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, you can efficiently monitor and mitigate DDoS attacks on IKEv1 and IKEv2 protocols when your firewall runs the ike process for the IPsec VPN service.

To support the feature, we introduce the following configuration statements at the [edit security ike] hierarchy level:

- **session**—Tune parameters to manage the behavior of negotiations with the remote peers to protect the security associations. Configure the parameters at the [edit security ike session half-open] and [edit security ike session full-open] hierarchy levels.
- **blocklists**—Define multiple blocklists and their associated rules for blocking an IKE ID. Configure the blocklists at the [edit security ike session blocklists] hierarchy level. You must attach a blocklist to one or more IKE policies at the [edit security ike policy *policy-name* blocklist *blocklist-name*] hierarchy level.

Use the following commands to view and clear statistics and other details about the in-progress, failed, blocked, and backoff peers:

- `show security ike peer statistics` and `show security ike peer`.
- `clear security ike peers statistics` and `clear security ike peers`.

[See [IKE Protection from DDoS Attacks](#), [session \(Security IKE\)](#), [blocklists \(Security IKE\)](#), [show security ike peers statistics](#), [show security ike peers](#), [clear security ike peers statistics](#), and [clear security ike peers](#).]

- **Support for VPN monitoring and datapath verification with the iked process (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 23.4R1, we support VPN monitoring and datapath verification on firewalls that run the iked process for the IPsec VPN service. With the iked process, you can continue to configure `vpn-monitor` and `verify-path` at the `[edit security ipsec vpn vpn-name]` hierarchy level.

We provide the following enhancements with the feature:

- Configuration and deletion of VPN monitoring functionality on an active tunnel does not cause any service disruption.
- After you've configured VPN monitoring, the functionality is active only after the tunnel is up.
- Configuration of `verify-path` on an active tunnel causes service disruption and performs renegotiation after the tunnel is down.

[See [vpn-monitor](#), [verify-path](#), and [VPN Tunnel Monitoring](#).]

What's Changed

IN THIS SECTION

- [J-Web](#) | [221](#)
- [Junos XML API and Scripting](#) | [221](#)
- [Network Management and Monitoring](#) | [222](#)
- [VPNs](#) | [222](#)

Learn about what changed in this release for vSRX Virtual Firewall.

J-Web

- **Updated Security Package URL (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we've updated the security package URL in **Device Administration > Security Package Management > URL Categories Settings**. You can use this URL to download Juniper NextGen or Juniper Enhanced Web Filtering package.

[See [URL Categories Settings](#).]

- **Internal SA is now called Internal SA Encryption (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Internal SA** to **Inter SA Encryption** and **Internal SA Keys** to **Key** in **Network > VPN > IPsec VPN > Global Settings**.

[See [IPsec VPN Global Settings](#).]

- **Name is now called Identifier (SRX1500, SRX1600, SRX2300, SRX4100, SRX4200, SRX4600, SRX5400, SRX5800, and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Name** to **Identifier** and **Network Address** to **Subnet** in **Security Services > Firewall Authentication > Address Pools**.

[See [About the Address Pools Page](#).]

- **Address Range is now called Named Address Ranges (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Address Range** to **Named Address Ranges** in **Security Services > Firewall Authentication > Address Pools**.

[See [About the Address Pools Page](#).]

- **Routing Instance is now called Source Virtual Router (SRX Series Firewalls and vSRX3.0)**—Starting in Junos OS Release 23.4R1, in J-Web, we have renamed **Routing Instance** to **Source Virtual Router** and **Source Address** to **Source Interface** in **Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create Radius Server and Security Services > Firewall Authentication > Access Profile > Create Access Profile > Create LDAP Server**.

[See [Add an Access Profile](#).]

Junos XML API and Scripting

- **XML output tags changed for request-commit-server-pause and request-commit-server-start (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—We've changed the XML output for the request system commit server pause command (request-commit-server-pause RPC) and the request system commit server

start command (request-commit-server-start RPC). The root element is <commit-server-operation> instead of <commit-server-information>, and the <output> tag is renamed to <message>.

Network Management and Monitoring

- **NETCONF <copy-config> operations support a file:// URI for copy to file operations (ACX Series, EX Series, MX Series, QFX Series, SRX Series, and vSRX)**—The NETCONF <copy-config> operation supports using a file:// URI when <url> is the target and specifies the absolute path of a local file.

[See [<copy-config>](#).]

VPNs

- **Introduction of extensive option for IPsec security associations (MX Series, SRX Series and vSRX 3.0)**—We've introduced the extensive option for the show security ipsec security-associations command. Use this option to display IPsec security associations with all the tunnel events. Use the existing detail option to display upto ten events in reverse chronological order.

See [show security ipsec security-associations](#).
- On vSRX instances in GCP deployments with cloud-hosted Hardware Security Module (HSM), if you lose GCP HSM connectivity, then the show security hsm status command might take up to 2 minutes to work.
- **Enhancement to the output of clear and regenerate key pair commands (vSRX 3.0)**--We've modified the output of the following commands when you clear and regenerate the same key pair to manage the secure data using hardware security module (HSM).

Starting in Junos OS 23.4R1 release, the command:

- clear security pki key-pair certificate-id *certificate-id-name* displays the message Key pair deleted successfully from the device. Key pair will be purged from the keyvault based on it's own preferences, as opposed to the message Key pair deleted successfully displayed in previous releases.
- request security pki generate-key-pair certificate-id certificate-id-name displays the message error: Failed to generate key pair. If the keypair was created and deleted before, please ensure that the keypair has been purged from the keyvault as opposed to the message error: Failed to generate key pair displayed in previous releases.

We made these changes to align with the cloud provider's restriction on key pair deletion, if any.

- **Enhancements to address CA certificate validation failure (SRX Series and vSRX 3.0)**–For the CA certificates, the certificate validation fails with the Lets Encrypt server when using the configuration statement `set security pki ca-profile ISRG revocation-check crl url` as PKI sends the OCSP request on HTTP 1.0 with the *requestorName*. We made modifications to the behaviour in order to send the OCSP request using HTTP 1.1 without the *requestorName* by default.
- To send the *requestorName* when using HTTP 1.1, use the hidden option `add-requestor-name-payload` at the edit `security pki ca-profile ca-profile-name revocation-check ocsp` hierarchy level.
- To send the OCSP request using the HTTP 1.0, use the hidden option `use-http-1.0` at the edit `security pki ca-profile ca-profile-name revocation-check ocsp` hierarchy level to ensure backward compatibility.

[See [revocation-check \(Security PKI\)](#).]

- **Enhancements to the output of `show security ipsec security-associations detail` command (SRX Series and vSRX 3.0)**–We've enhanced the output of `show security ipsec security-associations detail` when you enable `vpn-monitor` at the edit `security ipsec vpn vpn-name` hierarchy level, when your firewall runs IPsec VPN services with the new `iked` process. The output displays threshold and interval values in the command output. Starting in Junos OS Release 23.4R1, you'll notice these changes.

[See [show security ipsec security-associations](#).]

- **Modification to the XML tags for `show security ipsec` commands (SRX Series and vSRX 3.0)**–We've changed the XML tags for the following commands at `show security ipsec`.

Command	New XML Tag	Old XML Tag
<code>show security ipsec tunnel-events-statistics display xml validate</code>	<code>ipsec-tunnel-event-statistics</code>	<code>usp-ipsec-tunnel-event-statistics-information</code>
<code>show security ipsec inactive-tunnels detail display xml validate</code>	<code>ipsec-unestablished-tunnel-information</code>	<code>ipsec-security-association-information</code>

Starting in Junos OS Release 23.4R1, with the new XML tags, you'll notice that the `show security ipsec commands` emits valid XML.

Known Limitations

IN THIS SECTION

- [Network Address Translation \(NAT\) | 224](#)

Learn about known limitations in this release for vSRX Virtual Firewall.

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)

- Sessions drop observed under a timing scenario and traffic profile with persistent NAT configured. [PR1762417](#)

Open Issues

There are no known issues in hardware or software in this release for vSRX Virtual Firewall.

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

- [Flow-Based and Packet-Based Processing | 225](#)
- [General Routing | 225](#)
- [J-Web | 225](#)

- [Layer 2 Ethernet Services | 226](#)
- [User Interface and Configuration | 226](#)

Learn about the issues fixed in this release for vSRX Virtual Firewall.

Flow-Based and Packet-Based Processing

- Virtual routing instance configured on ingress interface will drop the ICMP traffic. [PR1742739](#)
- Buffer leak when PMI sends out packet on egress interface with MTU smaller than the packet length. [PR1758208](#)
- In NAT46 or NAT64 scenario, the packet that trigger NDP or ARP learning might get dropped. [PR1759202](#)
- Multicast packets of specific size between 663 to 676 bytes getting dropped. [PR1761891](#)

General Routing

- Traffic drop caused by Packet Forwarding Engine memory leak on SRX Series Firewall devices. [PR1738656](#)
- Memory leak in PKID. [PR1739342](#)
- Add FQDN-name counter in the show services user-identification identity-management status output. [PR1745588](#)
- Junos OS: SRX Series and EX Series: Multiple vulnerabilities in J-Web can be combined to allow a preAuth Remote Code Execution [PR1758332](#)

J-Web

- Junos OS: EX and SRX Series: A PHP vulnerability in J-Web allows an unauthenticated to control important environment variables (CVE-2023-36845) [PR1736942](#)

- J-Web certificate management issues. [PR1738316](#)
- J-Web gets stuck with loading message 'Please wait, syncing data from device'. [PR1756252](#)

Layer 2 Ethernet Services

- Delay in getting IP through DHCP cause traffic loss. [PR1752804](#)

User Interface and Configuration

- The load replace operation might result in mustd and mgd process pause. [PR1740289](#)

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 232](#)

This section contains information about how to upgrade Junos OS for vSRX Virtual Firewall 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 23.4R1 for vSRX Virtual Firewall using J-Web (see [J-Web](#)) or the Junos Space Network Management Platform (see [Junos Space](#)).

Direct upgrade of vSRX Virtual Firewall 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 Virtual Firewall 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 Virtual Firewall and vSRX Virtual Firewall 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 Firewall virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX Virtual Firewall to the newer and more recommended vSRX Virtual Firewall 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 Virtual Firewall 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 Virtual Firewall instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 23.4R1 for vSRX .tgz** file from the [Juniper Networks website](#). Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX Virtual Firewall instance to upload the new software image.

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

/dev/md0	1.3G	1.3G	0B	100%	/junos
/cf	694M	433M	206M	68%	/junos/cf
devfs	1.0K	1.0K	0B	100%	/junos/dev/
procfs	4.0K	4.0K	0B	100%	/proc
/dev/vtbd1s1e	302M	22K	278M	0%	/config
/dev/vtbd1s1f	2.7G	69M	2.4G	3%	/var
/dev/vtbd3s2	91M	782K	91M	1%	/var/host
/dev/md1	302M	1.9M	276M	1%	/mfs
/var/jail	2.7G	69M	2.4G	3%	/jail/var
/var/jails/rest-api	2.7G	69M	2.4G	3%	/web-api/var
/var/log	2.7G	69M	2.4G	3%	/jail/var/log
devfs	1.0K	1.0K	0B	100%	/jail/dev
192.168.1.1:/var/tmp/corefiles	4.5G	125M	4.1G	3%	/var/crash/ corefiles
192.168.1.1:/var/volatile	1.9G	4.0K	1.9G	0%	/var/log/host
192.168.1.1:/var/log	4.5G	125M	4.1G	3%	/var/log/hostlogs
192.168.1.1:/var/traffic-log	4.5G	125M	4.1G	3%	/var/traffic-log
192.168.1.1:/var/local	4.5G	125M	4.1G	3%	/var/db/host
192.168.1.1:/var/db/aamwd	4.5G	125M	4.1G	3%	/var/db/aamwd
192.168.1.1:/var/db/secinteld	4.5G	125M	4.1G	3%	/var/db/secinteld

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

```

root@vsrx> request system storage cleanup
List of files to delete:
Size Date      Name
11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
494B Sep 25 14:15 /var/log/interactive-commands.0.gz
20.4K Sep 25 14:15 /var/log/messages.0.gz
27B Sep 25 14:15 /var/log/wtmp.0.gz
27B Sep 25 14:14 /var/log/wtmp.1.gz
3027B Sep 25 14:13 /var/tmp/BSD.var.dist
0B Sep 25 14:14 /var/tmp/LOCK_FILE
666B Sep 25 14:14 /var/tmp/appidd_trace_debug
0B Sep 25 14:14 /var/tmp/eedebug_bin_file
34B Sep 25 14:14 /var/tmp/gksdchk.log
46B Sep 25 14:14 /var/tmp/kmdchk.log
57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
42B Sep 25 14:13 /var/tmp/pfe_debug_commands
0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
30B Sep 25 14:14 /var/tmp/policy_status

```

```

0B Sep 25 14:14 /var/tmp/rtbdb/if-rtbdb
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 Virtual Firewall to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.1R1 for vSRX Virtual Firewall .tgz file to `/var/crash/corefiles/` on the local file system of your vSRX Virtual Firewall VM. For example:

```

root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsr-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-vsr-x
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsr-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-vsr-x-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 21.1R1 for vSRX Virtual Firewall.



NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX Virtual Firewall 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 Virtual Firewall .ova image and need to validate it, see [Validating the vSRX .ova File for VMware](#).

Note that only .ova (VMware platform) vSRX Virtual Firewall images can be validated. The .qcow2 vSRX Virtual Firewall 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.

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

Table 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](#).

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 | 235
- Creating a Service Request with JTAC | 236

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>

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

Creating a Service Request with JTAC

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

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

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

Revision History

17 January 2025—Junos OS Release 23.4R1.

29 October 2024—Junos OS Release 23.4R1.

29 August 2024—Junos OS Release 23.4R1.

22 August 2024—Junos OS Release 23.4R1.

25 July 2024—Junos OS Release 23.4R1.

19 July 2024—Junos OS Release 23.4R1.

4 July 2024—Junos OS Release 23.4R1.

27 June 2024—Junos OS Release 23.4R1.

17 June 2024—Junos OS Release 23.4R1.

23 May 2024—Junos OS Release 23.4R1.

2 May 2024—Junos OS Release 23.4R1.
29 April 2024—Junos OS Release 23.4R1.
4 April 2024—Junos OS Release 23.4R1.
28 March 2024—Junos OS Release 23.4R1.
5 March 2024—Junos OS Release 23.4R1.
22 February 2024—Junos OS Release 23.4R1.
8 February 2024—Junos OS Release 23.4R1.
2 February 2024—Junos OS Release 23.4R1.
18 January 2024—Junos OS Release 23.4R1.
11 January 2024—Junos OS Release 23.4R1.
18 December 2023—Junos OS Release 23.4R1.

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 © 2025 Juniper Networks, Inc. All rights reserved.