

# Release Notes

Published  
2021-12-16

## Junos® OS Release 21.4R1

### SUPPORTED PLATFORMS

ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX

### KEY FEATURES

- Refer to Key Features in Junos OS Release 21.4 to quickly learn about the most important Junos OS features and how you can deploy them in your network.

### HARDWARE HIGHLIGHTS

- High-capacity second-generation AC PSM for SRX5800 Services Gateway

### SOFTWARE HIGHLIGHTS

- Interconnecting an EVPN-VXLAN Data Center with EVPN-MPLS in WAN using Inter-AS without a Logical Tunnel interface (MX-Series-All, EX9200, EX9252, EX9253)
- Hybrid Mode (SyncE and PTP) over LAG supports PTPoIPv4 and PTPoE (MX204 and MX10003)
- *Support for UPF N9 Uplink Classifier (MX240, MX480, MX960)*
- Support for GeoIP Filtering, Global Allowlist, and Global Blocklist (MX240, MX480, and MX960 routers )
- Support for Precision Time Protocol (PTP) over Ethernet in hybrid mode over link aggregation group (LAG) (MX10008 with JNP10K-LC2101 MPC line card)
- DHCP relay in an EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, QFX10002, QFX10008, and QFX10016)

- EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)
- Inband Flow Analyzer (IFA) 2.0 (QFX5120-48Y and QFX5120-32C)
- Support for firewall filters on EVPN-VXLAN with IPv6 underlays (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, and QFX5120-48YM)
- Increase in AC redundancy mode to 2+2 for high capacity high line PEMs (SRX5400)
- Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)
- UTM Content Filtering Based on File Content (SRX Series and vSRX)
- Support for FPC major alarm (SRX5400, SRX5600, and SRX5800)
- Support for FAT flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)
- EVPN-VXLAN additional features

## Day One+

- Use this [new setup guide](#) to get your Junos OS up and running in three quick steps.

# Table of Contents

**Introduction | 1**

**Key Features in Junos OS Release 21.4 | 1**

**Junos OS Release Notes for ACX Series**

**What's New | 6**

What's New in 21.4R1 | 6

Routing Protocols | 6

Additional Features | 7

**What's Changed | 7**

What's Changed in Release 21.4R1 | 7

**Known Limitations | 8**

**Open Issues | 9**

**Resolved Issues | 10**

Resolved Issues: 21.4R1 | 10

**Documentation Updates | 12**

**Migration, Upgrade, and Downgrade Instructions | 12**

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life  
Releases | 13

**Junos OS Release Notes for cRPD**

**What's New | 14**

What's New in 21.4R1 | 14

Additional Features | 14

**What's Changed | 15**

**Known Limitations | 15**

**Open Issues | 15**

**Resolved Issues | 16**

| Resolved Issues: 21.4R1 | 16

**Documentation Updates | 16**

## **Junos OS Release Notes for cSRX**

**What's New | 17**

| What's New in 21.4R1 | 17

**What's Changed | 18**

**Known Limitations | 18**

**Open Issues | 18**

**Resolved Issues | 18**

**Documentation Updates | 18**

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

**What's New | 19**

What's New in 21.4R1 | 20

| Authentication and Access Control | 20

| Dynamic Host Configuration Protocol | 20

| EVPN | 21

| High Availability | 22

| Junos Telemetry Interface (JTI) | 22

| Services Applications | 23

| Additional Features | 23

**What's Changed | 24**

| What's Changed in Release 21.4R1 | 24

**Known Limitations | 25**

**Open Issues | 27**

**Resolved Issues | 28**

| Resolved Issues: 21.4R1 | 29

**Documentation Updates | 33**

**Migration, Upgrade, and Downgrade Instructions | 33**

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 33

## Junos OS Release Notes for JRR Series

What's New | 34

What's Changed | 35

Known Limitations | 35

Open Issues | 35

Resolved Issues | 35

Resolved Issues: 21.4R1 | 36

Documentation Updates | 36

Migration, Upgrade, and Downgrade Instructions | 36

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 37

## Junos OS Release Notes for Juniper Secure Connect

What's New | 38

What's New in 21.4R1 | 38

Authentication and Access Control | 38

What's Changed | 39

Known Limitations | 39

Open Issues | 39

Resolved Issues | 39

Resolved Issues: 21.4R1 | 39

Documentation Updates | 40

## Junos OS Release Notes for Junos Fusion for Enterprise

What's New | 40

What's Changed | 41

Known Limitations | 41

**Open Issues | 41**

**Resolved Issues | 41**

**Documentation Updates | 41**

**Migration, Upgrade, and Downgrade Instructions | 42**

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

**What's New | 48**

**What's Changed | 48**

**Known Limitations | 48**

**Open Issues | 49**

**Resolved Issues | 49**

**Documentation Updates | 49**

**Migration, Upgrade, and Downgrade Instructions | 49**

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

**What's New | 59**

What's New in 21.4R1 | 59

Architecture | 60

EVPN | 60

High Availability | 61

IP Tunneling | 61

Junos Telemetry Interface (JTI) | 61

Layer 2 VPN | 62

MPLS | 62

Multicast | 62

Network Address Translation (NAT) | 62

Operation, Administration, and Maintenance (OAM) | 62

Platform and Infrastructure | 63

Routing Protocols | 64

Services Applications | 64

Software Defined Networking (SDN) | 65

Source Packet Routing in Networking (SPRING) or Segment Routing | 65

Subscriber Management and Services	65
VPNs	67
Additional Features	68

## **What's Changed | 69**

What's Changed in Release 21.4R1	70
----------------------------------	----

## **Known Limitations | 72**

## **Open Issues | 75**

## **Resolved Issues | 85**

Resolved Issues: 21.4R1	85
-------------------------	----

## **Documentation Updates | 103**

## **Migration, Upgrade, and Downgrade Instructions | 104**

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

## **What's New | 112**

What's New in 21.4R1	112
Network Management and Monitoring	112
Routing Policy and Firewall Filters	112

## **What's Changed | 114**

## **Known Limitations | 114**

## **Open Issues | 114**

## **Resolved Issues | 115**

Resolved Issues: 21.4R1	116
-------------------------	-----

## **Documentation Updates | 117**

## **Migration, Upgrade, and Downgrade Instructions | 117**

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

## **What's New | 119**

What's New in 21.4R1	120
Juniper Extension Toolkit (JET)	120
Operation, Administration, and Maintenance (OAM)	120

Routing Protocols | 121

Source Packet Routing in Networking (SPRING) or Segment Routing | 122

Additional Features | 122

## **What's Changed | 122**

What's Changed in Release 21.4R1 | 123

## **Known Limitations | 124**

## **Open Issues | 125**

## **Resolved Issues | 127**

Resolved Issues: 21.4R1 | 127

## **Documentation Updates | 130**

## **Migration, Upgrade, and Downgrade Instructions | 130**

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

## **What's New | 135**

EVPN | 135

High Availability | 137

Juniper Extension Toolkit (JET) | 137

Junos Telemetry Interface (JTI) | 137

Licensing | 138

MPLS | 138

Network Management and Monitoring | 138

Operation, Administration, and Maintenance (OAM) | 139

Routing Policy and Firewall Filters | 139

Routing Protocols | 140

Services Applications | 142

Additional Features | 142

## **What's Changed | 143**

What's Changed in Release 21.4R1 | 144



**Known Limitations | 145**

**Open Issues | 146**

**Resolved Issues | 149**

Resolved Issues: 21.4R1 | 150

**Documentation Updates | 155**

**Migration, Upgrade, and Downgrade Instructions | 155**

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

**What's New | 169**

Application Identification (AppID) | 169

Authentication and Access Control | 170

Chassis | 170

Chassis Cluster-specific | 170

Flow-Based and Packet-Based Processing | 171

Hardware | 171

J-Web | 171

Network Address Translation (NAT) | 173

Platform and Infrastructure | 173

Routing Policy and Firewall Filters | 174

Software Installation and Upgrade | 175

Unified Threat Management (UTM) | 175

Additional Features | 175

**What's Changed | 176**

What's Changed in Release 21.4R1 | 176

**Known Limitations | 179**

**Open Issues | 179**

**Resolved Issues | 182**

| Resolved Issues: 21.4R1 | 182

**Documentation Updates | 188**

**Migration, Upgrade, and Downgrade Instructions | 188**

| Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life  
Releases | 188

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

**What's New | 190**

| Licensing | 190

| Operation, Administration, and Maintenance (OAM) | 190

**What's Changed | 191**

| What's Changed in Release 21.4R1 | 191

**Known Limitations | 192**

**Open Issues | 192**

**Resolved Issues | 193**

| Resolved Issues: 21.4R1 | 193

**Documentation Updates | 193**

**Upgrade Instructions | 193**

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

**What's New | 194**

**What's Changed | 194**

**Known Limitations | 194**

**Open Issues | 195**

**Resolved Issues | 195**

| Resolved Issues: 21.4R1 | 196

**Documentation Updates | 196**

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

**What's New | 197**

- Application Identification (AppID) | 197
- Authentication and Access Control | 198
- Flow-Based and Packet-Based Processing | 198
- Interfaces | 198
- Licensing | 198
- Platform and Infrastructure | 199
- Unified Threat Management (UTM) | 199
- Additional Features | 200

**What's Changed | 201**

- What's Changed in Release 21.4R1 | 201

**Known Limitations | 202****Open Issues | 202****Resolved Issues | 205**

- Resolved Issues: 21.4R1 | 205

**Documentation Updates | 207****Migration, Upgrade, and Downgrade Instructions | 207**

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 214

**Licensing | 214****Finding More Information | 215****Documentation Feedback | 215****Requesting Technical Support | 216****Revision History | 218**

# Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

These release notes accompany Junos OS Release 21.4R1 for the ACX Series, Containerized Routing Protocol Process (cRPD), cSRX Container Firewall (cSRX), EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise, Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX). They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

## Key Features in Junos OS Release 21.4

Start here to learn about the key features in Junos OS Release 21.4. For more information about a feature, click the link in the feature description.

- **DHCP relay in an EVPN-VXLAN fabric with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, EVPN-VXLAN fabrics with an IPv6 underlay support DHCP relay. You can configure the DHCP relay agent in centrally routed and edge-routed bridging overlays. Support for DHCP relay includes support for DHCPv4 and DHCPv6. This feature was introduced in Junos OS Release 21.2R2.

[See [DHCP Relay Agent over EVPN-VXLAN](#).]

- **Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)**—Starting in Junos OS Release 21.4R1, we've increased the source NAT pool IP address range from 8 IP addresses to 64 IP addresses.

We've also increased the configurable length of the source NAT pool name, destination NAT pool name, source NAT rule name, destination NAT rule name, static NAT rule name, and rule set name from 31 characters to 63 characters.

[See [show security nat source rule](#), [show security nat destination rule](#), and [show security nat static rule](#).]

- **EVPN-VXLAN support (QFX5120-48YM):**
  - EVPN-VXLAN with MAC-VRF routing instances

- Filter-based forwarding in EVPN-VXLAN
- IPv6 data traffic support through an EVPN-VXLAN overlay network
- IPv6 support for firewall filtering and policing on EVPN-VXLAN traffic
- Port mirroring and analyzers on EVPN-VXLAN
- Storm control on EVPN-VXLAN

[See [EVPN User Guide](#).]

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure an 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, configure the underlay VXLAN tunnel endpoint (VTEP) source interface in the MAC-VRF instance as an IPv6 address. However, you must use the IPv4 loopback address as the router ID for BGP handshaking to work.

This feature was introduced in Junos OS Release 21.2R2.

[See [EVPN-VXLAN with an IPv6 Underlay](#) and [Understanding EVPN with VXLAN Data Plane Encapsulation](#).]

- **Hybrid mode (Synchronous Ethernet and Precision Time Protocol) over LAG supports PTP over IPv4 and PTP over Ethernet (MX204 and MX10003)**

[See [PTP Overview](#) and [Hybrid Mode Overview](#).]

- **Inband Flow Analyzer (IFA) 2.0 (QFX5120-48Y and QFX5120-32C)**—In Junos OS Release 21.4R1, we've introduced support for IFA 2.0 on QFX Series switches. IFA 2.0 monitors and analyzes packets entering and exiting the network. You can use IFA 2.0 to monitor the network for faults and performance issues. IFA 2.0 supports both Layer 3 and VXLAN flows.

With IFA 2.0, you can collect various flow-specific information from the data plane, without the involvement of the control plane or the host CPU. IFA collects data on a per-hop basis across the network. You can export this data to external collectors to perform localized or end-to-end analytics.

IFA 2.0 contains three different processing nodes:

- IFA initiator node
- IFA transit node
- IFA terminating node

[See [Inband Flow Analyzer \(IFA\) 2.0 Probe for Real-Time Performance Monitoring](#), [inband-flow-telemetry](#), [show services inband-flow-telemetry](#), and [clear inband-flow-telemetry stats](#).]

- **Increase in AC redundancy mode to 2+2 for high-capacity high-line PEMs (SRX5400)**—Starting in Junos OS Release 21.4R1, the SRX5400 device supports 2+2 AC redundancy mode on high-capacity high-line power entry modules (PEMs). The support for 2+2 redundancy mode increases the PEM's capacity from 2050 W to 4100 W.

[See [SRX5400 Services Gateway AC Power Supply Specifications](#).]

- **Interconnecting EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes (MX-Series, EX9200, EX9252, EX9253)**—Starting in Junos OS Release 21.4R1, you can interconnect EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes, but without using logical tunnel interfaces. In Release 21.4R1, you can interconnect only those BDs/VLANs that are on the interconnected VLAN list. Note that the gateway nodes in one data center will have connectivity by means of virtual tunnel end points (VTEPs), whereas gateway nodes must be able to handle EVPN-VXLAN encapsulation on the data center side and EVPN-MPLS on the WAN (data center interconnect) side.

EVPN interconnect CLI commands:

```
set routing-instances <instance-name> protocols evpn interconnect interconnected-vlan-list
[ <vlan-id1> <vlan-id2>]
```

```
set routing-instances <instance-name> protocols evpn interconnect encapsulation mpls
```

[See [Technology Overview of VXLAN-EVPN Integration for DCI](#).]

- **Support for firewall filters on EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, and QFX5120-48YM)**—Starting in Junos OS Release 21.4R1, QFX5120 switches support firewall filters for ingress and egress traffic on EVPN-VXLAN with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation](#).]

- **Support for fat flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support fat flow technology to improve the firewall and NAT throughput value up to 10 times of the current value.

[See [Understanding Symmetric Fat IPsec Tunnel](#).]

- **Support for FPC major alarm (SRX5400, SRX5600, and SRX5800 with SPC3)**—In Junos OS Release 21.4R1, we've enhanced the following commands to show more details about the FPC major alarm:

- `show chassis error active`
- `show chassis error active detail`
- `show chassis error active fpc-slot slot-number`
- `show chassis error active detail fpc-slot slot-number`

You can use these commands to identify and troubleshoot the hardware issues.

[See [show chassis errors active](#).]

- **Support for UPF N9 uplink classifier (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, you can use the uplink classifiers functionality supported by the control and user plane separation (CUPS)-enabled UPF (User Plane Functions) to do the following selectively on the link connected to your devices:

- Forward uplink traffic towards different protocol data unit (PDU) session anchors.
- Merge downlink traffic from the different PDU session anchors.

[See [Junos Multi-Access User Plane Overview](#) and [CUPS Session Creation and Data Flow with Junos Multi-Access User Plane](#).]

- **Support for GeoIP filtering, global allowlist, and global blocklist (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, you can configure the Security Intelligence process ipfd on the listed MX Series routers to fetch GeoIP feeds from Policy Enforcer. The GeoIP feeds help prevent devices from communicating with IP addresses belonging to specific countries.

You can define:

- A profile to dynamically fetch GeoIP feeds. Include the `geo-ip rule match country country-name` statement at the `[edit services web-filter profile profile-name security-intelligence-policy]` hierarchy level.
- A template to dynamically fetch GeoIP feeds. Include the `geo-ip rule match group group-name` statement at the `[edit services web-filter profile profile-name url-filter-template template-name security-intelligence-policy]` hierarchy level.

You can define a global allowlist by configuring the `white-list (IP-address-list | file-name)` statement at the `edit services web-filter profile profile-name security-intelligence-policy` hierarchy level. You can define a global blocklist by configuring the `black-list (IP-address-list | file-name)` statement at the `edit services web-filter profile profile-name security-intelligence-policy` hierarchy level. Here, *IP-address-list* refers to the name of the list specified at the `[edit services web-filter]` hierarchy level. The *file-name* option refers to the name of the file where the list of the IP addresses to be allowed or blocked is specified. The file must be in the `/var/db/url-filterd` directory and must have the same name as in the configuration.

[See [Integration of Juniper ATP Cloud and Web filtering on MX Routers](#) .]

- **Support for Precision Time Protocol (PTP) over Ethernet in hybrid mode over link aggregation group (LAG)** (MX10008 with JNP10K-LC2101 MPC line card)

[See [Precision Time Protocol Overview](#) and [Hybrid Mode Overview](#).]

- **Content filtering based on file content (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, unified threat management (UTM) performs content filtering to determine the file type based on the file content and not on file extensions. This feature complements application identification (App ID) by enabling you to configure the firewall to identify and to control access to the Web (HTTP and HTTPS) traffic and to protect your network from attacks.

This content filtering improvement replaces the existing content filtering based on filename extensions and profile-based filtering on application profiles.

Use the **show security utm content-filtering statistics** command to view the content-filtering system statistics and errors.

With this feature implementation, we do not support content filtering based on MIME type, content type, and protocol commands.

The legacy content-filtering configurations are deprecated and are hidden. You will receive system logs and error messages if you try to configure the legacy content filtering options. You can use the legacy functionality if you don't want to migrate to this improved functionality.

[See [Content Filtering](#), [content-filtering \(Security UTM Policy\)](#), [utm](#), and [utm default-configuration](#).]

## Junos OS Release Notes for ACX Series

### IN THIS SECTION

- [What's New | 6](#)
- [What's Changed | 7](#)
- [Known Limitations | 8](#)
- [Open Issues | 9](#)
- [Resolved Issues | 10](#)
- [Documentation Updates | 12](#)
- [Migration, Upgrade, and Downgrade Instructions | 12](#)



These release notes accompany Junos OS Release 21.4R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [What's New in 21.4R1 | 6](#)

Learn about new features introduced in the Junos OS main and maintenance releases for ACX Series routers.

## What's New in 21.4R1

### IN THIS SECTION

- [Routing Protocols | 6](#)
- [Additional Features | 7](#)

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

### Routing Protocols

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by the Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

[See [How to Enable Link Delay Measurement and Advertising in OSPF](#).]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

[See [What is Flexible Algorithm Definition \(FAD\)](#).]

## Additional Features

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

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

- **G.8275.1 Telecom profile support** (ACX5448)

[See [G.8275.1 Telecom profile support](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1 | 7](#)

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

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [EVPN | 8](#)
- [Network Management and Monitoring | 8](#)

## EVPN

- **Output for the show Ethernet switching flood extensive command**—The output for the `show ethernet-switching flood extensive` command now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as `unilist`. Previously, the output for the `show ethernet-switching flood extensive` command would misidentify the next-hop type as `composite`.

## Network Management and Monitoring

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

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

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 9

Learn about known limitations in Junos OS Release 21.4R1 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 ACX5448 routers, latency appears for the host-generated ICMP traffic. [PR1380145](#)

## Open Issues

### IN THIS SECTION

- [General Routing | 9](#)
- [Routing Protocols | 10](#)

Learn about open issues in Junos OS Release 21.4R1 for ACX Series routers.

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

## General Routing

- The ACX710 routers with the console cable plugged in might find interruption in the system boot. [PR1513553](#)
- On ACX5448 routers, ping stops working even though the ARP entry is present during continuous script executions. [PR1533513](#)
- When you configure the multihop BFD, the delegated BFD sessions do not come up. [PR1633395](#)
- On ACX VM host-based platforms, starting in Junos OS Release 21.4R1 and later, ssh and root login are required for copying line card image from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use the `deny-password` instead of `deny` as default root-login

option under ssh configuration to allow internal trusted communication. Alternatively, once installed, it can be disabled in the configurations. Refer to <https://kb.juniper.net/TSB18224>. [PR1629943](#)

## Routing Protocols

- FIPS mode enabling fails with self-test failure and kernel crash. [PR1623128](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | 10

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.

### Resolved Issues: 21.4R1

### IN THIS SECTION

- [General Routing](#) | 10

## General Routing

- On ACX5448 routers, the BFD session status goes in the Init state after the system reboots when you have both CFM and BFD configured on the system. [PR1552235](#)
- Packet buffer allocation failed messages might be generated when you use the scaled-CFM sessions with minimum DM or SLM cycle-time along with enhanced-sla-iterator. [PR1574754](#)
- On ACX5448 routers, the asynchronous-notification for 1G interface fails. [PR1580700](#)

- On ACX5448 routers, IPv4 traffic loss with packet size more than 1410 occurs. [PR1584509](#)
- On ACX710 routers, PTP might get stuck and not function properly in a certain condition. [PR1587990](#)
- On ACX710 and ACX5400 routers, traffic might get forwarded through the member links in the Down state after the new member links gets added to the aggregated Ethernet interface. [PR1589168](#)
- On ACX5448 routers, high DMR out of sequence with iterator configuration occurs. [PR1596050](#)
- On ACX710 routers, the l2ald process generates core file at l2ald\_event\_process\_list\_id, l2ald\_event\_proc\_all\_lists, and l2ald\_event\_periodic () at `../../../../src/junos/usr/sbin/l2ald/l2ald_event.c:757`. [PR1596908](#)
- On ACX5448 and ACX710 routers, traffic drop in the EVPN VPWS flexible cross connect occurs. [PR1598074](#)
- On ACX710 and ACX5448 routers, traffic loss might be observed if you modify drop-profiles. [PR1598595](#)
- On ACX710 routers, the rpf-check-bytes,rpf-check-packets counters does not get updated properly to the flat file as expected. [PR1600513](#)
- On ACX5448 and ACX710 routers, MACsec traffic over Layer 2 circuit might not work. [PR1603534](#)
- On ACX5448 routers, FPC might restart when you execute the `show firewall`. [PR1605288](#)
- The optics\_mts\_010.robot script fails while verifying SNMP and matching the CLI values. [PR1605348](#)
- On ACX5448 and ACX710 routers running DHCP, relay does not process packets arriving over MPLS. [PR1605854](#)
- On ACX1100 routers, the FEB (Forwarding Engine Board) might crash. [PR1606424](#)
- On ACX710 and ACX5448 routers, the DHCP packets might not be relayed. [PR1608125](#)
- On ACX5096 routers, the pps traffic output appears on the deactivated interfaces. [PR1608827](#)
- On ACX710 routers running Junos OS Release 21.2R1 and later might experience kernel crash. [PR1608852](#)
- The routing protocol engine CPU becomes nonresponsive at 100 percent. [PR1612387](#)
- Interface state gets reset after the Packet Forwarding Engine restarts. [PR1613314](#)
- On ACX5448 routers, unknown SMART attributes for StorFly VSFBM6CC100G-JUN1 SSD might occur. [PR1614068](#)

- On ACX5448 and ACX710 routers with Layer 3 VPN scenarios, error messages might be generated after multiple core link or protocol flaps. [PR1621425](#)
- On ACX5448 routers, CFM does not appear to be in the 0k state after the router reboots. [PR1602489](#)
- On ACX5448 and ACX710 routers, traffic towards the CE device through the default route might be dropped in VRF. [PR1611651](#)
- Traffic might get equally load-balanced irrespective of the scheduler configuration. [PR1620137](#)
- Six to eight seconds of delay occurs when the receiver switches in between groups. [PR1620685](#)
- Traffic does not get forwarded to one of the the single homed PE device after you change the VLAN-ID under the routing instance. [PR1621036](#)
- On ACX5448 routers, the smartd configurations do not get applied. [PR1623359](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for ACX Series.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 13

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](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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.4.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of 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 | 14](#)
- [What's Changed | 15](#)
- [Known Limitations | 15](#)
- [Open Issues | 15](#)
- [Resolved Issues | 16](#)
- [Documentation Updates | 16](#)



These release notes accompany Junos OS Release 21.4R1 for the containerized routing protocol process (cRPD) container. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [What's New in 21.4R1 | 14](#)

Learn about new features introduced in this release for Containerized Routing Protocol Daemon.

### What's New in 21.4R1

### IN THIS SECTION

- [Additional Features | 14](#)

Learn about new features or enhancements to existing features in this release for cRPD.

#### Additional Features

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

- **Support for Advanced RISC Machines (ARM)64 (cRPD)** cRPD is packaged as a Docker container to run on a 64-bit ARM platform.

cRPD on ARM64 does not support the following features:

- **Sharding and updateIO.** The set system processes routing bgp rib-sharding *number-of-shard* and set system processes routing bgp update-threading *number-of-threads* commands are not supported.
- SRv6

[See [Server Requirements](#) .]

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for Containerized Routing Protocol Daemon.

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 15

Learn about known limitations in Junos OS Release 21.4R1 for Containerized Routing Protocol Daemon.

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

## General Routing

- The configuration results in unexpected behaviour set routing-options forwarding-table channel vrouter protocol protocol-type netlink-fpm. [PR1603055](#)

## Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R1 for Containerized Routing Protocol Daemon.

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

- [Resolved Issues: 21.4R1 | 16](#)

Learn about the issues fixed in this release for Containerized Routing Protocol Daemon.

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

### Resolved Issues: 21.4R1

### IN THIS SECTION

- [MPLS | 16](#)

## MPLS

- Deactivating or reacting routing-instance configuration could result in permanent traffic loss for remote destinations when using MPLSoUDP or MPLSoGRE tunnels. [PR1595071](#)
- LDPv6 routes preference is not updated after modifying LDP route preference. [PR1618785](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for Containerized Routing Protocol Daemon.

# Junos OS Release Notes for cSRX

## IN THIS SECTION

- What's New | 17
- What's Changed | 18
- Known Limitations | 18
- Open Issues | 18
- Resolved Issues | 18
- Documentation Updates | 18

These release notes accompany Junos OS Release 21.4R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- What's New in 21.4R1 | 17

There are no new features or enhancements to existing features in Junos OS Release 21.4R1 for cSRX Container Firewall.

### What's New in 21.4R1

There are no new features for cSRX in Junos OS Release 21.4R1.

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for cSRX Container Firewall.

## Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R1 for cSRX Container Firewall.

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

## Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R1 for cSRX Container 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

There are no resolved issues in Junos OS Release 21.4R1 for cSRX Container Firewall.

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

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for cSRX Container Firewall.

# Junos OS Release Notes for EX Series

## IN THIS SECTION

- What's New | 19
- What's Changed | 24
- Known Limitations | 25
- Open Issues | 27
- Resolved Issues | 28
- Documentation Updates | 33
- Migration, Upgrade, and Downgrade Instructions | 33

These release notes accompany Junos OS Release 21.4R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

## IN THIS SECTION

- What's New in 21.4R1 | 20

Learn about new features introduced in the Junos OS main and maintenance releases for EX Series switches.

## What's New in 21.4R1

### IN THIS SECTION

- Authentication and Access Control | 20
- Dynamic Host Configuration Protocol | 20
- EVPN | 21
- High Availability | 22
- Junos Telemetry Interface (JTI) | 22
- Services Applications | 23
- Additional Features | 23

Learn about new features or enhancements to existing features in this release for EX Series switches.

### Authentication and Access Control

- **RADIUS reachability to reauthenticate server fail sessions (EX2300, EX3400, EX4300, and EX4400)**—Starting in Junos OS Release 21.4R1, you can configure the RADIUS reachability feature to enable the switch to trigger reauthentication when the server is reachable, without waiting for the reauthentication timer to expire.

[See [Configuring RADIUS Reachability to Reauthenticate Server Fail Sessions](#).]

### Dynamic Host Configuration Protocol

- **Support for DHCP security features with service provider style of configuration (EX2300, EX3400, EX4300, EX4300-MP, EX4400, and EX4400-MP)**—Starting in Junos OS Release 21.4R1, you can configure the following DHCP security features with a service provider style of configuration:
  - DHCPv4 snooping
  - DHCPv6 snooping
  - Dynamic ARP inspection
  - Neighbor discovery inspection
  - DHCP option 82
  - DHCPv6 option 18

- DHCPv6 option 37
- Lightweight DHCPv6 relay agent

You can combine service provider and enterprise styles of configuration on the same physical interface using flexible Ethernet services encapsulation on EX2300, EX3400, EX4300-MP, EX4400 and EX4400-MP switches.

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

## EVPN

- **Support for EVPN-VXLAN group-based policies (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, EX4400-48T, EX4650, and EX4650-48Y-VC)**—Starting in Junos OS Release 21.4R1, EX4400 and EX4650 switches provide standards-based multi-level segmentation (also called group-based policy, or GBP) on the basis of Layer 3 virtual networks and group-based tags rather than IP-based filters. GBP supports an application-centric policy model that separates network access policies from the underlying network topology through the use of policy tags, thus allowing different levels of access control for endpoints and applications even within the same VLAN.

The EX4400 and EX4650 switches also provide GBP support for locally switched traffic on VXLAN access ports.

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

- **Dynamic overlay load balancing in an EVPN-VXLAN network (EX4400-24MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48MP, EX4400-48P, and EX4400-48T)** —Starting in Junos OS Release 21.4R1, EX4400 switches in an EVPN-VXLAN network (centrally routed and edge-routed bridging overlays) support dynamic load balancing on virtual tunnel endpoints (VTEPs). Juniper Networks switches have dynamic load balancing enabled by default.

[See [Dynamic Load Balancing in an EVPN-VXLAN Network](#).]

- **Interconnecting EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes (MX-Series, EX9200, EX9252, EX9253)**—Starting in Junos OS Release 21.4R1, you can interconnect EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes, but without using logical tunnel interfaces. In Release 21.4R1, you can interconnect only those BDs/VLANs that are on the interconnected VLAN list. Note that the gateway nodes in one data center will have connectivity by means of virtual tunnel end points (VTEPs), whereas gateway nodes must be able to handle EVPN-VXLAN encapsulation on the data center side and EVPN-MPLS on the WAN (data center interconnect) side.



EVPN interconnect CLI commands:

```
set routing-instances <instance-name> protocols evpn interconnect interconnected-vlan-list
[ <vlan-id1> <vlan-id2>]
```

```
set routing-instances <instance-name> protocols evpn interconnect encapsulation mpls
```

[See [Technology Overview of VXLAN-EVPN Integration for DCI](#).]

## High Availability

- **Unified ISSU support on EX4650**—Starting in Junos OS Release 21.4R1, EX4650 switches support unified in-service software upgrade (ISSU). The unified ISSU feature enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic.

Use the `request system software in-service-upgrade package-name.tgz` command to use unified ISSU. Use the `request system software validate in-service-upgrade package-name.tgz` command to verify that your device and target release are compatible.

**NOTE:** EX4650 switches provide unified ISSU support only if the Cancun versions of the chipset SDK are the same for the current version and the version you are upgrading to. See, "[High Availability](#)" on page 26.

[See [Getting Started with Unified In-Service Software Upgrade](#) and [Understanding In-Service Software Upgrade \(ISSU\)](#).]

## Junos Telemetry Interface (JTI)

- **Packet Forwarding Engine performance sensors (EX4650, QFX5110, QFX5120-48Y, QFX5200, and QFX5210)**—Starting in Junos OS Release 21.4R1, JTI streams NPU utilization statistics by means of remote procedure calls (gRPC), gRPC network management interface (gNMI), or UDP (native) transport from a device to an outside collector.

[See [sensor \(Junos Telemetry Interface\)](#), [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#), and [Telemetry Sensor Explorer](#).]

## Services Applications

- **Support for Two-Way Active Measurement Protocol (TWAMP) and hardware timestamping of RPM probe messages (EX9200 line of switches)**—Starting in Release 24.1R1, Junos OS supports TWAMP and hardware timestamping of real-time performance monitoring (RPM) probe messages on the EX9200 line of switches.

You can use TWAMP to measure IP performance between two devices in a network. By enabling hardware timestamping of RPM, you can account for the latency in the communication of probe messages and also generate more accurate timers in the Packet Forwarding Engine.

[See [Understand Two-Way Active Measurement Protocol](#) and [Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX, and MX Series Routers and QFX Switches](#) .]

## Additional Features

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

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
- **DHCP security** (EX9200, MX240, MX480, MX960, MX2010, MX2020). MPC10E line cards support the following DHCP security features:
  - DHCP snooping with Option 82.
  - DHCPv6 snooping with Option 16, Option 18, Option 37, and Option 79.
  - Lightweight DHCPv6 Relay Agent.

[See [DHCP Snooping](#).]

- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

[See [EVPN Type 2 and Type 5 Route Coexistence with EVPN-VXLAN](#).]

- **MACsec bounded delay protection** (EX4400 and SRX380)

[See [bounded-delay](#).]

- **Precision Time Protocol (PTP) transparent clock** (EX4300 and EX4300-48MP)

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

- **Support for OSPF, IS-IS, BGP, and static routing on IRB interfaces in EVPN-VXLAN networks** (EX4300-48MP and EX4400)

[See [Supported Protocols on an IRB Interface in EVPN-VXLAN](#).]

- **Support for IEEE 802.1ag CFM on service provider interfaces and Q-in-Q (point-to-point) interfaces** (EX2300, EX3400, EX4300, EX4300-48MP, and EX4400)

[See [Introduction to OAM Connectivity Fault Management \(CFM\)](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 24

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

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [EVPN](#) | 24
- [Interfaces and Chassis](#) | 25
- [Network Management and Monitoring](#) | 25

## EVPN

- **Output for show Ethernet switching flood extensive**—The output for show ethernet-switching flood extensive now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unicast. Previously, the output for show ethernet-switching flood extensive would misidentify the next-hop type as composite.

## Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

## Network Management and Monitoring

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

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

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 26
- [Infrastructure](#) | 26

Learn about known limitations in Junos OS Release 21.4R1 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

- When the device is up and running for a long time, there is a possibility FS gets bad blocks and it is accumulated. When any change done to it, it reloads and tries to recover the bad blocks from the FS. [PR910445](#)
- BUM (Broadcast, Unknown Unicast, and Multicast) traffic replication over VTEP is sending out more packets than expected and there seems to be a loop also in the topology. [PR1570689](#)

## Infrastructure

- Software versions 21.1 and lower are running FreeBSD version 11 whereas from version 21.2 onward, the FreeBSD version is 12. Software upgrade to 21.2 (or later) from 21.1 (or earlier) will mandatorily need cli knob 'no-validate' to be used during software image upgrade process. (For EX4400 platforms, this is applicable from version 21.3 onward. Hence, for EX4400 platforms, software upgrade to 21.3 (or later) from 21.2 (or earlier) will mandatorily need cli knob 'no-validate' to be used during software image upgrade process.) [PR1586481](#)

## High Availability

- Starting in Junos OS Release 21.4R1, EX4650 switches support unified in-service software upgrade (ISSU). However, EX4650 switches provide unified ISSU support only if the Cancun versions in the chipset SDK are the same in the current version and the version you are upgrading to. [PR1634695](#)

## Open Issues

### IN THIS SECTION

- [General Routing | 27](#)
- [Infrastructure | 28](#)
- [Platform and Infrastructure | 28](#)

Learn about open issues in Junos OS Release 21.4R1 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

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- When running the command, `show pfe filter hw filter-name <filter name>`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- On the EX4300-48MP device, 35 second delay is added in reboot time. [PR1514364](#)
- FPC might not be recognized after the power cycle (hard reboot). [PR1540107](#)
- On EX4400 family of devices, sometimes login prompt is not shown after the login session ends. [PR1582754](#)
- On EX series switches with vendor chip as Packet Forwarding Engine, if IS-IS is enabled on an integrated routing and bridging (IRB) interface and the maximum transmission unit (MTU) size of the IRB interface is configured with a value great than 1496 bytes, the IS-IS hello (IIH) PDUs with jumbo frame size (i.e., great than 1496 bytes) might be dropped and not sent to the IS-IS neighbors. The following is the product list of EX series switches with vendor chip as Packet Forwarding Engine. EX2300/EX3400/EX4300/EX4600/EX4650 [PR1595823](#)
- On EX4400 platforms, if image upgrade is attempted using non-stop software upgrade, an error message **error: syntax error: request-package-validate** will be reported as the CLI output. The error does not have any impact on the non-stop software upgrade process. [PR1596955](#)

- EX4400 platforms have a Cloud LED on the front panel to indicate onboarding of the device to cloud (day0) and management after onboarding (day1). If MIST is used as a management entity in cloud, then the cloud LED displays green in situations where device has lost connectivity to cloud. This is because, MIST is using outbound SSH for management. This behavior is not applicable to any other management entity that uses outbound https and LED that displays appropriate states to indicate the loss on connection to cloud. [PR1598948](#)

## Infrastructure

- A double free vulnerability in the software forwarding interface daemon (sfid) process of Juniper Networks Junos OS allows an adjacently-connected attacker to cause a Denial of Service (DoS) by sending a crafted ARP packet to the device. Please refer <https://kb.juniper.net/JSA11162> for more information. [PR1497768](#)

## Platform and Infrastructure

- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect ASIC programming. This issue only affects while running DHCP relay on EVPN and VXLAN environment. [PR1530160](#)
- When a EX4400 Virtual Chassis is scaled with different features configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a vmcore might be reported at that time. Once VM core is saved, device will continue to operate normally. [PR1599498](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | [29](#)

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.

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [General Routing | 29](#)
- [EVPN | 31](#)
- [Infrastructure | 32](#)
- [Interfaces and Chassis | 32](#)
- [Junos Fusion Enterprise | 32](#)
- [Layer 2 Ethernet Services | 32](#)
- [Platform and Infrastructure | 32](#)

## General Routing

- During flooding, MAC is learnt only on normal access port but not on the aggregated Ethernet interface trunk port. [PR1506403](#)
- CSPRNG is changed to the HMAC-DRBG and cannot be changed to either the FreeBSD Fortuna or the Juniper DYCE RNGs. [PR1529574](#)
- On EX Series line of switches Virtual Chassis (VC), Power over Ethernet (POE) might not be detected and hence might fail to work on VC members. [PR1539933](#)
- The Virtual Chassis Port (VCP) might not come up on EX4600 platform. [PR1555741](#)
- Some transmitting packets might get dropped due to the **disable-pfe** action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- The DHCP client might not obtain IP address when dhcp-security is configured. [PR1564941](#)
- On EX platforms, the new primary Routing Engine post switchover might go into DB mode (or crash). [PR1565213](#)
- The MAC address will point to incorrect interface after traffic is stopped and not aging out. [PR1565624](#)
- The fxpc process might crash and cause traffic loss in the IFBD scenario. [PR1572305](#)



- Private VLAN configuration might fail in certain scenario. [PR1574480](#)
- The dcpfe crash is observed on Junos OS EX Series line of switches. [PR1578859](#)
- On EX Series line of switches, some 40G ports might not be channelized successfully. [PR1582105](#)
- The upgrade of the PoE firmware might fail on EX2300 and EX3400. [PR1584491](#)
- Packet drops during VRRP primary reboot when 40XS linecard is present on some EX9204 platforms. [PR1586740](#)
- Process dot1xd crash might be seen and re-authentication might be needed on EX9208 platform. [PR1587837](#)
- Inconsistent statistics value seen on performing **slaac-snooping**. [PR1590926](#)
- The DHCP relay might not work if it connects with the server via type 5 route which with aggregated Ethernet interface as the underlay interface. [PR1592133](#)
- On the EX4300-48MP Virtual Chassis, the backup Routing Engines clear the reporting alarm for a PEM failure intermittently for a missing power source. [PR1593795](#)
- Clients authentication failure might occur due to dot1x daemon memory leak. [PR1594224](#)
- On a EX4400 VC, log messages related to fan settings will be observed in chassis traceoptions file. [PR1594446](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- The MAC/IP withdraw route may be suppressed by rpd in the EVPN scenario [PR1597391](#)
- The backup Virtual Chassis member might not learn MAC address on a primary after removing a VLAN unit from the SP style aggregated Ethernet interface which is part of multiple VLAN units. [PR1598346](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable [PR1599094](#)
- On EX4400 Virtual chassis, linecard member console might fail to redirect to Virtual Chassis primary. [PR1599625](#)
- Unable to disable the management port em1. [PR1600905](#)
- EX4400 PVIDB schema files not updated for the correct count of (lic\_ft\_cnt) Licensing feature. [PR1601449](#)
- On EX2300 and EX4650, if the system is upgraded from 20.2 or earlier release to 20.3 or later release, either using phone-home feature or when the system is in factory default state, the upgrade will fail with phone-home crash. [PR1601722](#)

- On EX2300 Virtual Chassis platforms ARP might not get resolved. [PR1602003](#)
- On a EX4400 Virtual Chassis, the Cloud LED will display pattern for **NO\_CLOUD\_RESPONSE** when there is no IP address present on IRB interface or no DNS is configured on the device. [PR1602664](#)
- On EX4400 dot1x authentication might not work on EVPN/xlan enabled endpoints. [PR1603015](#)
- The NSSU performed with MACsec configuration might result in fxpc core [PR1603602](#)
- MAC move might be seen between the ICL and MC-LAG interface if adding or removing VLANs on the ICL interface. [PR1605234](#)
- On a EX4400 POE supported device, PoE firmware upgrade should be done with bt-firmware CLI option only. [PR1606276](#)
- On EX Series switches, the fxpc process might crash and generate a core dump. [PR1607372](#)
- On EX4300 platform, the dcpfe process might crash and generate core. [PR1608306](#)
- DHCP packets might be received and then returned back to DHCP relay through the same interface on EX2300, EX3400, and EX4300 Virtual Chassis platforms. [PR1610253](#)
- Change in commit error message while configuring the same vlan-id with different vlan-name through openconfig CLI. [PR1612566](#)
- After performing zeroize factory default configuration does not show appropriate interface in the device. [PR1614098](#)
- SFP+-10G-T-DWDM-ZR support for EX3400. [PR1615246](#)
- Lowest acceptable PN not reflecting correct value when replay-window-size is more than zero. [PR1618598](#)
- EVPN type 5 routes might not be installed. [PR1620808](#)
- Traffic loss might be observed after configuring VXLAN over IRB interface. [PR1625285](#)

## EVPN

- Traffic loss might be seen under EVPN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- Traffic loss might be seen if aggregated Ethernet bundle interface with ESI is disabled on primary Routing Engine followed by a Routing Engine switchover. [PR1597300](#)

## Infrastructure

- For EX4400 product family, net installation (PXE) is not working. [PR1577562](#)
- EX2300, EX2300-MP, and EX3400 do not take kernel core file to internal storage on panic. [PR1600442](#)
- Upgrade might fail when upgrading from legacy release. [PR1602005](#)
- The fxpc process might crash and generate core. [PR1611480](#)

## Interfaces and Chassis

- ARP resolution failure might occur during VRRP failover. [PR1578126](#)
- SNMP\_TRAP\_LINK\_UP and SNMP\_TRAP\_LINK\_DOWN trap might be seen while activating and deactivating firewall filters. [PR1609838](#)

## Junos Fusion Enterprise

- Reverting mastership from RE1 to RE0 might lead to l2ald daemon crash and cause an outage. [PR1601817](#)

## Layer 2 Ethernet Services

- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)

## Platform and Infrastructure

- FPC crashes might be seen on EX92 platforms. [PR1579182](#)
- Broadcast traffic might be discarded when a firewall filter is applied to the loopback interface. [PR1597548](#)
- VLAN tagged traffic might be dropped with service provider style configuration. [PR1598251](#)
- The VRRP packets might not be forwarded when **mac-move-limit** configuration statement is configured. [PR1601005](#)
- Adding aggregated Ethernet configuration without child member might cause MAC or ARP learning issues. [PR1602399](#)
- The ZTP service might not work and the image installation fails. [PR1603227](#)

- Slaac-Snooping global address entry learnt over vtep interface does not RENEW sometimes after lease timer expiry. [PR1603269](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for EX Series switches.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 33

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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.4.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases

before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of 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 | 34](#)
- [What's Changed | 35](#)
- [Known Limitations | 35](#)
- [Open Issues | 35](#)
- [Resolved Issues | 35](#)
- [Documentation Updates | 36](#)
- [Migration, Upgrade, and Downgrade Instructions | 36](#)

These release notes accompany Junos OS Release 21.4R1 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

### What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R1 for JRR Series Route Reflectors.

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for JRR Series Route Reflectors.

## Known Limitations

There are no known limitations in hardware and software in Junos OS Release 21.4R1 for JRR Series Route Reflectors.

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

## Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R1 for JRR Series Route Reflectors.

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

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | 36

Learn which issues were resolved in the Junos OS main and maintenance releases for JRR Series.

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

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [General Routing | 36](#)

## General Routing

- On JRR200, incorrect Power Entry Module (PEM) load percentage is observed when you execute the `show chassis power` command. [PR1598728](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for JRR Series Route Reflectors.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 37](#)

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

For information about software installation and upgrade, see the [JRR200 Route Reflector Quick Start](#) and [Installation and Upgrade Guide](#).

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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.4.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of 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 | 38](#)
- [What's Changed | 39](#)
- [Known Limitations | 39](#)
- [Open Issues | 39](#)
- [Resolved Issues | 39](#)
- [Documentation Updates | 40](#)

These release notes accompany Junos OS Release 21.4R1 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.



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

## What's New

### IN THIS SECTION

- [What's New in 21.4R1](#) | 38

Learn about new features introduced in the Junos OS main and maintenance releases for the Juniper Secure Connect.

routers.

## What's New in 21.4R1

### IN THIS SECTION

- [Authentication and Access Control](#) | 38

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

### Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the `address-assignment` option at the `[edit access profile profile-name authentication-order ldap ldap-options]` hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

[See [ldap-options](#).]

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for Juniper Secure Connect.

## Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R1 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 and software in Junos OS Release 21.4R1 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

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | 39

There are no resolved issues in Junos OS Release 21.4R1 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: 21.4R1

There are no resolved issues in Junos OS Release 21.4R1 for Juniper Secure Connect.

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for Juniper Secure Connect.

# Junos OS Release Notes for Junos Fusion for Enterprise

### IN THIS SECTION

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

These release notes accompany Junos OS Release 21.4R1 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

There are no new features or enhancements to existing features in Junos OS release 21.4R1 for Junos fusion for enterprise.

## What's Changed

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

## Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in this release for Junos fusion for enterprise.

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

## Open Issues

There are no open issues in hardware and software in this release for Junos Fusion for enterprise.

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

## Resolved Issues

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

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

## Documentation Updates

There are no errata or changes in Junos OS Release 21.4R1 documentation for Junos Fusion for enterprise documentation.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- Basic Procedure for Upgrading Junos OS on an Aggregation Device | 42
- Upgrading an Aggregation Device with Redundant Routing Engines | 44
- Preparing the Switch for Satellite Device Conversion | 45
- Converting a Satellite Device to a Standalone Switch | 46
- Upgrade and Downgrade Support Policy for Junos OS Releases | 46
- Downgrading Junos OS | 47

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

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

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

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To

preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the [Junos OS Administration Library](#).

To download and install Junos OS:

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

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

Customers in the United States and Canada, use the following commands, where *n* is the spin number.

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

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

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

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

## Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

## Preparing the Switch for Satellite Device Conversion

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

For satellite device hardware and software requirements, see [Understanding Junos fusion for enterprise Software and Hardware Requirements](#).

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

## Converting a Satellite Device to a Standalone Switch

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

## Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3,

19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

## Downgrading Junos OS

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

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

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

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

# Junos OS Release Notes for Junos Fusion for Provider Edge

### IN THIS SECTION

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

- Documentation Updates | 49
- Migration, Upgrade, and Downgrade Instructions | 49

These release notes accompany Junos OS Release 21.4R1 for Junos Fusion for provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R1 for Junos fusion for provider edge.

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for Junos fusion for provider edge.

## Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R1 for Junos fusion for provider edge.

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

## Open Issues

There are no known issues in hardware and software in Junos OS Release 21.4R1 for Junos fusion for provider edge.

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

## Resolved Issues

There are no resolved issues in Junos OS Release 21.4R1 for Junos fusion for provider edge.

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

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for Junos fusion for provider edge.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading an Aggregation Device | 50](#)
- [Upgrading an Aggregation Device with Redundant Routing Engines | 52](#)
- [Preparing the Switch for Satellite Device Conversion | 53](#)
- [Converting a Satellite Device to a Standalone Device | 55](#)
- [Upgrading an Aggregation Device | 57](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 57](#)
- [Downgrading from Junos OS Release 21.4 | 58](#)

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

## Basic Procedure for Upgrading an Aggregation Device

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

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

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

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

The download and installation process for Junos OS Release 21.4R1 is different from that for earlier Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:  
<https://www.juniper.net/support/downloads/>
2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos fusion** to find the software that you want to download.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the page.
5. Select the **Software** tab.

6. Select the software package for the release.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new `jinstall` package on the aggregation device.

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

Customers in the United States and Canada, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.4R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.4R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.4R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.4R1.SPIN-
export-signed.tgz
```

Replace *source* with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

**NOTE:** After you install a Junos OS Release 21.4R1 *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.

## Upgrading an Aggregation Device with Redundant Routing Engines

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

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

## Preparing the Switch for Satellite Device Conversion

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

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

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

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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



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

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

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

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

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

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

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

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

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

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

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

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

## Converting a Satellite Device to a Standalone Device

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

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

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

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:  
<https://www.juniper.net/support/downloads>
2. Log in to the Juniper Networks authentication system by using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
3. Select **By Technology > Junos Platform > Junos fusion** from the drop-down list and select the switch platform series and model for your satellite device.
4. Select the Junos OS Release 14.1X53-D30 software image for your platform.
5. Review and accept the End User License Agreement.
6. Download the software to a local host.
7. Copy the software to the routing platform or to your internal software distribution site.
8. Remove the satellite device from the automatic satellite conversion configuration.

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

[edit]

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

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

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

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

## 9. Commit the configuration.

To commit the configuration to both Routing Engines:

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

Otherwise, commit the configuration to a single Routing Engine:

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

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

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

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

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

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

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

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

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

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

## Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 21.4R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

## Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

## Downgrading from Junos OS Release 21.4

To downgrade from Release 21.4 to another supported release, follow the procedure for upgrading, but replace the 21.4 jinstall package with one that corresponds to the appropriate release.

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

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

# Junos OS Release Notes for MX Series

### IN THIS SECTION

- [What's New | 59](#)
- [What's Changed | 69](#)
- [Known Limitations | 72](#)
- [Open Issues | 75](#)
- [Resolved Issues | 85](#)
- [Documentation Updates | 103](#)
- [Migration, Upgrade, and Downgrade Instructions | 104](#)

These release notes accompany Junos OS Release 21.4R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [What's New in 21.4R1 | 59](#)

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

## What's New in 21.4R1

### IN THIS SECTION

- [Architecture | 60](#)
- [EVPN | 60](#)
- [High Availability | 61](#)
- [IP Tunneling | 61](#)
- [Junos Telemetry Interface \(JTI\) | 61](#)
- [Layer 2 VPN | 62](#)
- [MPLS | 62](#)
- [Multicast | 62](#)
- [Network Address Translation \(NAT\) | 62](#)
- [Operation, Administration, and Maintenance \(OAM\) | 62](#)
- [Platform and Infrastructure | 63](#)
- [Routing Protocols | 64](#)
- [Services Applications | 64](#)
- [Software Defined Networking \(SDN\) | 65](#)
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 65](#)
- [Subscriber Management and Services | 65](#)

●	<a href="#">VPNs   67</a>
●	<a href="#">Additional Features   68</a>

Learn about new features or enhancements to existing features in this release for the MX Series routers.

## Architecture

- **Support for UPF N9 uplink classifier (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, you can use the uplink classifiers functionality supported by the control and user plane separation (CUPS)-enabled UPF (User Plane Functions) to do the following selectively on the link connected to your devices:
  - Forward uplink traffic towards different protocol data unit (PDU) session anchors.
  - Merge downlink traffic from the different PDU session anchors.

[See [Junos Multi-Access User Plane Overview](#) and [CUPS Session Creation and Data Flow with Junos Multi-Access User Plane](#).]

## EVPN

- **Support for EVPN routing policies on the MPC10E and MPC11E (MX240, MX480, MX960, MX2010, and MX2020)**—Starting in Junos OS Release 21.4R1, Junos OS supports policy filter configurations for EVPN routes on the MX240, MX480, and MX960 routers with the MPC10E line cards and on the MX2010 and MX2020 routers with the MPC11E line cards. You can create policies and apply policy filters to import and export EVPN routes at a specific EVPN routing-instance level or at the BGP level if you want to apply the policy to all EVPN routing instances.

[See [Routing policies for EVPN](#).]

- **Interconnecting EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes (MX-Series, EX9200, EX9252, EX9253)**—Starting in Junos OS Release 21.4R1, you can interconnect EVPN-VXLAN data centers with EVPN-MPLS in a WAN using gateway nodes, but without using logical tunnel interfaces. In Release 21.4R1, you can interconnect only those BDs/VLANs that are on the interconnected VLAN list. Note that the gateway nodes in one data center will have connectivity by means of virtual tunnel end points (VTEPs), whereas gateway nodes must be able to handle EVPN-VXLAN encapsulation on the data center side and EVPN-MPLS on the WAN (data center interconnect) side.

EVPN interconnect CLI commands:

```
set routing-instances <instance-name> protocols evpn interconnect interconnected-vlan-list
[ <vlan-id1> <vlan-id2>]
```

```
set routing-instances <instance-name> protocols evpn interconnect encapsulation mpls
```

[See [Technology Overview of VXLAN-EVPN Integration for DCI.](#)]

## High Availability

- **Unified ISSU with enhanced mode supported on MPC11E sub-line cards (MX2010 and MX2020)**—Starting in Junos OS Release 21.4R1, MX Series routers with MPC11E sub-line cards installed can use the enhanced mode ISSU option. Enhanced mode eliminates packet loss during the unified ISSU process.

Use the request system software in-service-upgrade *package-name.tgz* enhanced-mode command to use unified ISSU with enhanced mode. Use the request system software validate in-service-upgrade *package-name.tgz* enhanced-mode command to verify that your device and target release are compatible with enhanced mode.

[See [How to Use Unified ISSU with Enhanced Mode](#) and [Sub Line Card Overview.](#)]

## IP Tunneling

- **Support for unicast IP-over-IP (IP-IP) tunneling for IPv4 and IPv6 traffic signaled by BGP (MX960 and MX2008)**—Starting in Junos OS Release 21.4R1, we support an IP-IP encapsulation to facilitate IP overlay construction over an IP transport network.

[See [Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation](#)]

## Junos Telemetry Interface (JTI)

- **Streaming queue statistics for static demux interfaces over aggregated Ethernet interfaces (MX Series)**—Starting in Junos OS Release 21.4R1, we support streaming of quality-of-service (QoS) queue statistics using JTI for statically configured demux interfaces over aggregated Ethernet interfaces.

[See [Enabling Export of Subscriber Statistics and Queue Statistics for Dynamic Interfaces and Interface-Sets](#) .]



## Layer 2 VPN

- **Support for VPLS over transport class tunnels ( MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, and vMX)**—Starting in Junos OS Release 21.4R1, you can configure VPLS (FEC129, BGP, and LDP) services on segment routing–traffic engineering (SR-TE), RSVP-TE, flexible algorithm, and BGP Labeled Unicast (BGP-LU) traffic tunnels. Junos OS supports both colored and non-colored routing configurations.

[See [Introduction to Configuring VPLS](#) and [BGP Classful Transport Planes Overview](#).]

## MPLS

- **Support for new statement `no-normalize-same-members` to resize member LSPs (MX Series and PTX Series)**—In Junos OS Release 21.4R1, we've added the `no-normalize-same-members` statement to the container LSP normalization configuration under the `[edit protocols mpls container-label-switched-path NAME splitting-merging]` hierarchy. When you enable the `no-normalize-same-members` configuration, you only resize the existing member LSPs with equal bandwidth. In earlier Junos OS releases, if normalization does not need to create or delete any member LSPs, you resignal the member LSPs with equal bandwidth.

[See [splitting-merging](#).]

## Multicast

### Network Address Translation (NAT)

- **Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)**—Starting in Junos OS Release 21.4R1, we've increased the source NAT pool IP address range from 8 IP addresses to 64 IP addresses.

We've also increased the configurable length of the source NAT pool name, destination NAT pool name, source NAT rule name, destination NAT rule name, static NAT rule name, and rule set name from 31 characters to 63 characters.

[See [show security nat source rule](#), [show security nat destination rule](#), and [show security nat static rule](#).]

### Operation, Administration, and Maintenance (OAM)

- **Enhancements to BFD-triggered FRR for unicast next hops and forwarding-table session-id-change-limiter-indirect to address issue of traffic being silently discarded (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002,**

**QFX10008, QFX10016, and vMX**—In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and forwarding-table session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

To align the traffic by creating session-id-change-limiter indirect next hop, set the `set routing-options forwarding-table session-id-change-limiter-indirect` configuration statement at the `[edit routing-options forwarding-table]` hierarchy level.

[See [Bidirectional Forwarding Detection \(BFD\) for MPLS](#).]

## Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:
  - View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name group-name` command. See [request security pki ca-profile-group-status](#).
  - Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` command. See [auto-re-enrollment](#).
  - View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <cert_id> detail` command. See [show security pki local-certificate \(View\)](#).
  - View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See [show security pki ca-certificate \(View\)](#).
  - View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See [request security pki ca-certificate verify \(Security\)](#) and [request security pki local-certificate verify \(Security\)](#).
  - View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See [show security pki statistics](#) and [clear security pki statistics](#).
- **Support for optics (MX10008 and MX10016)**—Starting in Junos OS Release 21.4R1, we've added SFP+-10G-T-DWDM-ZR in supported list of optics on the MX10K-LC480 line card.

[See [Hardware Compatibility Tool](#).]

## Routing Protocols

- **Support for accepting BGP routes with `accept-own` community (MX480 and MX960)**—Starting in Junos OS Release 21.4R1, MX480 and MX960 routers accept BGP routes with the `accept-own` community, defined by *RFC 7611, BGP ACCEPT\_OWN Community Attribute*.

The feature enhances the interoperability of a Juniper router by enabling it to accept routes whose `ORIGINATOR_ID` or `NEXT_HOP` value matches that of the receiving BGP speaker. For example, when a provider edge (PE) device advertises routes with the route distinguisher of a source VRF, the route reflector attaches the `accept-own` community and re-advertises the routes back to the originator. The provider edge (PE) device can then import the routes into the other destination VRFs, excluding its own.

[See [BGP accept-own Community](#) and [accept-own](#).]

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by the Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

[See [How to Enable Link Delay Measurement and Advertising in OSPF](#).]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

[See [What is Flexible Algorithm Definition \(FAD\)](#).]

## Services Applications

- **Support for GeoIP filtering, global allowlist, and global blocklist (MX240, MX480, and MX960 )**—Starting in Junos OS Release 21.4R1, you can configure the Security Intelligence process `ipfd` on the listed MX Series routers to fetch GeoIP feeds from Policy Enforcer. The GeoIP feeds help prevent devices from communicating with IP addresses belonging to specific countries.

You can define:

- A profile to dynamically fetch GeoIP feeds. Include the geo-ip rule match country *country-name* statement at the [edit services web-filter profile *profile-name* security-intelligence-policy] hierarchy level.
- A template to dynamically fetch GeoIP feeds. Include the geo-ip rule match group *group-name* statement at the [edit services web-filter profile *profile-name* url-filter-template *template-name* security-intelligence-policy] hierarchy level.

You can define a global allowlist by configuring the white-list (IP-address-list | *file-name*) statement at the edit services web-filter profile *profile-name* security-intelligence-policy hierarchy level. You can define a global blocklist by configuring the black-list (IP-address-list | *file-name*) statement at the edit services web-filter profile *profile-name* security-intelligence-policy hierarchy level. Here, *IP-address-list* refers to the name of the list specified at the [edit services web-filter] hierarchy level. The *file-name* option refers to the name of the file where the list of the IP addresses to be allowed or blocked is specified. The file must be in the **/var/db/url-filterd** directory and must have the same name as in the configuration.

[See [Integration of Juniper ATP Cloud and Web filtering on MX Routers](#) .]

## Software Defined Networking (SDN)

- **New CLI command to view load-balancing statistics for af interfaces (MX480, MX960, MX2008, MX2010, and MX2020)**—Starting in Junos OS Release 21.4R1, use the show interfaces lb-stats *af-interface-name* command at the guest network function (GNF) level to view the information about the load balancing of transmit traffic on each peer Packet Forwarding Engine of an abstracted fabric (af) interface. You can also view the statistics of the transmit traffic on the fabric queues (high and low queues) for each peer Packet Forwarding Engine on an af interface. In Junos OS releases earlier than Release 21.4R1, you use the show interface *af-name* command to display the load-balancing information.

[See [show interfaces lb-stats af](#).]

## Source Packet Routing in Networking (SPRING) or Segment Routing

- **Support for SRv6 LSPs in PCEP (MX Series)**—Support for SRv6 LSP in PCEP (MX Series)- Starting Junos OS Release 21.4R1, all types of SRv6 LSPs, such as PCE-Initiated, locally created, and delegated SRv6 LSPs are supported in the Path Computation Element Protocol (PCEP).

[See [SRv6 LSPs in PCEP](#).]

## Subscriber Management and Services

- **Support for subscriber service redundancy on DHCP server (MX Series)**—Starting in Junos OS Release 21.4R1, you can enable M:N subscriber service redundancy using active leasequery for the

DHCP server running on an MX Series broadband network gateway (BNG). The subscriber service redundancy on the DHCP server ensures uninterrupted subscriber services when you reboot or replace the primary server, or when the primary server has any hardware failures such as access link failures, access line-card failure, or chassis failure.

[See [Subscriber Redundancy on DHCP Server](#).]

- **Subscriber service reauthentication on actual data rate change (MX Series)**—Starting in Junos OS Release 21.4R1, the DHCP server reauthenticates the subscriber service when the actual data rate changes. This reauthentication is an alternative to RADIUS change of authorization (CoA) to change subscriber session characteristics based on the actual data rate change without interrupting the subscriber service.

You can enable the reauthentication feature using the `actual-data-rate-change` statement at the `[edit system services dhcp-local-server reauthenticate]` hierarchy level. You can also configure a threshold value for the `actual-data-rate-change` downstream and upstream DSL attributes at the `[edit system services dhcp-local-server reauthenticate actual-data-rate-change]` hierarchy level.

[See [reauthenticate \(DHCP Local Server\)](#), [show subscribers](#), and [show network-access aaa statistics re-authentication](#).]

- **Load-balancing support for subscriber traffic on pseudowire service interface (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.4R1, we support load balancing for subscriber sessions on the pseudowire service interface over multiple logical tunnel child member links of a redundant logical tunnel (RLT) interface at the same time. The load balancing property of the RLT interface allows subscriber traffic on the pseudowire service interface to be dispersed and load-balanced over different PICs and line cards. Service providers can enable BNG subscriber sessions on the PS interface with the support of multiple active links.

An RLT interface allows up to a maximum of 32 member LT interfaces. This redundancy protects the access and the core-facing link against anchor Packet Forwarding Engine failure across line cards.

[See [Pseudowire Subscriber Logical Interfaces Overview](#).]

- **CoS support for BNG on pseudowire service interface over active-active RLT interface (MX240, MX480, and MX960)**—In Junos OS Release 21.4R1, we've introduced CoS support for a BNG on subscriber-interface on pseudowire over an active-active redundant logical tunnel (RLT) interface for subscriber applications such as DHCP and PPPoE. This CoS property is achieved by providing the scheduling nodes for the logical tunnel links. For dynamic interfaces, interface sets, static underlying interfaces, and dynamic underlying interfaces over RLT, CoS allocates scheduling nodes for each link in the RLT, which has multiple logical tunnel links in active-active mode. In case of targeted interfaces and targeted interface sets, which have primary and backup links, CoS allocates scheduling nodes on the primary and backup links to optimize the use of scheduling nodes. Traffic for the subscriber targeted interfaces will be distributed to all the primary LT links when CoS is applied at the subscriber level.

When you enable targeting in a node, you must enable targeting for all the child nodes for CoS to function properly. Also, you must configure the network-services enhanced-ip at the [edit chassis] hierarchy level because this feature works only in enhanced IP mode.

[See [Anchor Redundancy Pseudowire Subscriber Logical Interfaces Overview](#), [targeted-options \(PS interface\)](#), [logical-interface-fpc-redundancy \(PS interface\)](#), [rebalance-subscriber-granularity](#), [show interfaces demux0 \(Demux Interfaces\)](#).]

## VPNs

- **Antispoofing protection for next-hop-based dynamic tunnels (MX240, MX480, MX960, MX2010, and MX2020 with MPC10E or MX2K-MPC11E line cards)—**

In Junos OS Release 21.4R1, we've added antispoofing capabilities IPv4 tunnels and IPv4 data traffic. Antispoofing for next-hop-based dynamic tunnels can detect and prevent a compromised virtual machine (inner source reverse path forwarding check) but does not apply to a compromised server that is label-spoofing. The antispoofing protection is effective when the VRF routing instance has label-switched interfaces (LSIs) using vrf-table-label or virtual tunnel (VT) interfaces. We do not support antispoofing protection for per-next-hop labels on VRF routing instances.

[See Anti-Spoofing Protection for Next-Hop-Based Dynamic Tunnels Overview.<https://www.juniper.net/documentation/us/en/software/junos/vpn-l3/topics/topic-map/l3-vpns-nh-tunnels.html#id-antispoofing-protection-for-nexthopbased-dynamic-tunnels-overview> .]

- **Support for AMS in IPsec MX-SPC3 (MX240, MX480, and MX960 with MX-SPC3) —**Starting in Junos OS Release 21.4R1, the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 service card to support an aggregated multiservices interface (AMS).

[See [Aggregated Multiservices Interface](#).]

- **Support for AMS warm standby (MX240, MX480, and MX960 with MX-SPC3)—**Starting in Junos OS Release 21.4R1, the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 service card to support warm standby on an aggregated multiservices interface (AMS). In AMS warm standby mode, you can use a single service interface as a backup for multiple service interfaces.

[See [Aggregated Multiservices Interface](#).]

- **Support for headend termination of pseudowire services in a VPLS-enabled virtual switch (MX Series)—**Starting in Junos OS Release 21.4R1, you can configure a pseudowire service transport logical interface in Layer 2 circuit. You can also configure a trunk service logical interface in a VPLS-enabled virtual switch to terminate a Layer 2 circuit instance in the virtual switch. You can terminate the same Layer 2 circuit in the VPLS instance-type routing instance with different service logical interfaces and Layer 3 VPN VRF instance-type routing instance using another service logical interface as well.

[See [Pseudowire Service Interfaces](#).]

## Additional Features

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

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
- **DHCP security** (EX9200, MX240, MX480, MX960, MX2010, MX2020). MPC10E line cards support the following DHCP security features:
  - DHCP snooping with Option 82.
  - DHCPv6 snooping with Option 16, Option 18, Option 37, and Option 79.
  - Lightweight DHCPv6 Relay Agent.

[See [DHCP Snooping](#).]

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running ike). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

This feature is supported only if the `junos-ike` package is installed in your device.

[See [Routing Protocols Support on IPsec VPN Tunnels](#).]

- **Enhancements to increase traffic selector flexibility** (MX240, MX480, and MX960 with MX-SPC3). You can do the following to add flexibility to your traffic selectors in different deployment scenarios:
  - Configure the routing metric for a traffic selector.
  - Define the source port range, destination port range, and protocol for a traffic selector.
  - Define multiple terms within a traffic selector, instead of creating multiple traffic selectors (or child security associations or SAs) for a VPN. Each term comprises the local and remote IP prefixes, the source and destination port ranges, and the protocol identifier. You can use these parameters in a single IPsec SA negotiation. In earlier Junos OS releases, you configure each traffic selector with one set of local and remote IP prefixes to be used in an IPsec SA negotiation with a peer.

This feature is supported only if the `junos-ike` package is installed in your device.

We recommend that you configure the same metric value if you define multiple traffic selectors under the same `[edit security ipsec vpn vpn_name]` hierarchy with the same value for `remote-ip ip-address/netmask`. If you configure different metric values, then the metric value of the st0 route installed will be the same as that for the traffic selector that is negotiated or installed first.

[See [traffic-selector](#) and [show security ipsec security-associations detail](#).]

- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

[See [EVPN Type 2 and Type 5 Route Coexistence with EVPN-VXLAN](#).]

- **Hybrid mode (Synchronous Ethernet and Precision Time Protocol) over LAG supports PTP over IPv4 and PTP over Ethernet** (MX204 and MX10003)

[See [PTP Overview](#) and [Hybrid Mode Overview](#).]

- **Hold timer support on aggregated Ethernet (ae-) interfaces** (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016) Specify the hold-time value to delay the advertisement of up and down transitions (flapping) on an interface.

[See [hold-time](#).]

- **Redistribution of IPv4 routes with IPv6 Next Hop into BGP through tunnels: (MX10008 and MX10016):**

IPv4 traffic is tunneled from CPE devices to IPv4-over-IPv6 gateways as described in RFC 5549.

[See [Understanding Redistribution of IPv4 Routes with IPv6 Next Hop into BGP](#).]

- **Support for Precision Time Protocol (PTP) over Ethernet in hybrid mode over link aggregation group (LAG)** (MX10008 with JNP10K-LC2101 MPC line card)

[See [Precision Time Protocol Overview](#) and [Hybrid Mode Overview](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 70



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

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [EVPN | 70](#)
- [General Routing | 70](#)
- [Interfaces and Chassis | 70](#)
- [Network Management and Monitoring | 71](#)
- [Routing Protocols | 71](#)
- [Subscriber Management and Services | 72](#)

## EVPN

- **Output for show Ethernet switching flood extensive**—The output for show ethernet-switching flood extensive now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unicast. Previously, the output for show ethernet-switching flood extensive would misidentify the next-hop type as composite.

## General Routing

- The range for source-pfe and destination-pfe at show class-of-service fabric statistics is now 0-15 (depending on platform type).
- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**—We do not support request, show, and clear PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The pkid process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

## Interfaces and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

- **Display the donor details of the IPv6 borrower interface**—The output for the `show interfaces` command now displays the donor details of the IPv6 borrower interface.

[See [show interfaces](#)].

## Network Management and Monitoring

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

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

## Routing Protocols

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

## Subscriber Management and Services

- **New output fields for subscriber management statistics (MX Series)**—If you enable the enhanced subscriber management, the non-DHCPv4 bootstrap protocol (BOOTP) requests might not get processed even if you configure the DHCP relay or server with the overrides `bootp-support` statement at the edit `forwarding-options dhcp-relay` hierarchy level. To monitor the DHCP transmit and receive packet counters, we've introduced the following output fields for `show system subscriber-management statistics dhcp` extensive operational command.

- BOOTP boot request packets received
- BOOTP boot reply packets received
- BOOTP boot request packets transmitted
- BOOTP boot reply packets transmitted

[See [show system subscriber-management statistics](#).]

## Known Limitations

### IN THIS SECTION

- [General Routing | 73](#)
- [Infrastructure | 74](#)
- [J-Web | 74](#)
- [MPLS | 74](#)
- [Network Management and Monitoring | 74](#)
- [Platform and Infrastructure | 75](#)

Learn about known limitations in Junos OS Release 21.4R1 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

- When the device is up and running for a long time, there is a possibility FS gets bad blocks and it is accumulated. When any change done to it, it reloads and tries to recover the bad blocks from the FS. [PR910445](#)
- When cmerror disables the Packet Forwarding Engine, it does not power off the EA and HCM chips. Temperature monitoring continues on the HMC and other devices, and the system can take proper actions, such as increasing the fan speed or shutting down the systems. [PR1324070](#)
- This ping latency behavior is expected for host generated ICMP traffic due to the design of Packet Forwarding Engine queue polling the packets from ASIC. [PR1380145](#)

ping

10 packets transmitted, 10 packets received, 0% packet loss

round-trip min/avg/max/stddev = 8.994/51.885/106.449/26.824 ms

- Currently, IPv4 options router are not supported and traffic is not hitting the egress firewall filter. For more information, see <https://www.juniper.net/documentation/us/en/software/junos/routing-policy/topics/concept/firewall-filter-match-conditions-for-ipv4-traffic.html> [PR1490967](#)
- LFM might flap during MX Series Virtual Chassis ISSU to and from this release. [PR1516744](#)
- On QFX5200 and QFX5100 switches with the IPIP tunnel feature, show dynamic-tunnels database statistics command output shows extra packet counts (that is, sampled packets when sFlow is enabled). [PR1555922](#)
- BUM traffic replication over VTEP is sending out more packets than expected and there seems to be a loop in the topology. [PR1570689](#)
- The PTP FPGA is kept in reset during BIOS boot. During Linux boot, the PTP FPGA is taken out of reset and pcie-tree is reenumerated. Therefore, you might see the Link-up/down during this sequence. [PR1572061](#)
- When a packet, which triggers ARP resolution, hits services interface style filter on the output will have session create and close log with incorrect ingress interface. This typically occurs with the first session hitting such a filter. [PR1597864](#)
- Enhanced policer counter output shows double value. [PR1615373](#)
- When the show command show services web-filter secintel-policy-db ip-prefix-information is being used, exact prefix mentioned in the feed file database needs to be provided. [PR1615465](#)
- Packet errors are detected in PSV block message and traffic loss is seen, when sending 250G traffic using filter with next term. [PR1617385](#)

- Percentage physical-interface policer is not working on aggregated Ethernet, after switching between baseline configuration to policer configuration. [PR1621998](#)
- Scaled number of PPPoE subscribers are hosted on PS anchored over RLT interface. When you try to remove LT member link from the RLT bundle, some of the subscribers might go down. As a workaround, bring down all the subscribers before removing RLT member links. [PR1623641](#)
- In ULC-based linecards, you can see duplicate leaf values for the following counters exported in / interfaces/interface/state/counters hierarchy - in-unicast-pkts in-broadcast-pkts in-multicast-pkts in-pause-pkts in-errors in-discards out-unicast-pkts out-multicast-pkts out-broadcast-pkts out-pause-pkts out-errors out-discards. These leaves are produced by picd and afd-trio. [PR1624864](#)

## Infrastructure

- The Junos OS Release 21.1 and earlier are running FreeBSD version 11 whereas from Junos OS Release 21.2 and later run FreeBSD version is 12. While upgrading the software image to Junos OS Release 21.2 or later, it is mandatory to use no-validate command. [PR1586481](#)

## J-Web

- The Firefox browser displays an unsaved changes error message in the J-Web basic settings page if the autofill login and password options are selected under the browser privacy and security settings. [PR1560549](#)

## MPLS

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

## Network Management and Monitoring

- Configuring the set system no-hidden-commands blocks NETCONF sessions. As a workaround, customer can disable the no-hidden-commands. [PR1590350](#)

## Platform and Infrastructure

- The following error message occurs while running `clear vpls mac-table`. [Mar 9 06:20:42.795 LOG: Err] `disp_force_callout(1994): EA[0:0].disp[0] forced callout timeout 0 msec`. [Mar 9 06:20:42.795 LOG: Err] `luss_send_callout_parcel(793): EA[0:0].disp[0] failed to send callout parcel (ptype 14, snum 977 tid 0)`. [Mar 9 06:20:43.510 LOG: Err] `dispatch_event_handler(684): EA[0:0].disp[0] PRIMARY_TIMEOUT (PPE 4 Zone 8)`. [PR1575316](#)
- When the `and deactivate routing-options rpm-tracking` CLIs are applied together and then committed. Some of the rpm tracked added routes are not deleted from the routing table. [PR1597190](#)
- Routing Engine-based BFD sessions might flap during switchover when there are large number of BFD, IS-IS, OSPF and LDP packets to be sent out. [PR1600684](#)

## Open Issues

### IN THIS SECTION

- [EVPN | 76](#)
- [Flow-based and Packet-based Processing | 76](#)
- [Forwarding and Sampling | 76](#)
- [General Routing | 77](#)
- [Interfaces and Chassis | 82](#)
- [Juniper Extension Toolkit \(JET\) | 82](#)
- [MPLS | 83](#)
- [Layer 2 Features | 83](#)
- [Network Management and Monitoring | 83](#)
- [Platform and Infrastructure | 84](#)
- [Routing Protocols | 84](#)
- [Services Applications | 85](#)
- [VPNs | 85](#)

Learn about open issues in Junos OS Release 21.4R1 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

- EVPN-MPLS multi-homing control MACs are missing after vlan-id removal and adding back on a trunk logical interfaces of one of the multi-homing PEs. [PR1596698](#)
- In a scenario with EVPN-VXLAN in the datacenter and EVPN-MPLS is in the WAN and the stitching is done with an LT interface, then the bridge mac-table learning entries are not as expected for EVPN-VXLAN routing instance. This could occur after restart interface-control is issued on gateways. [PR1600310](#)
- On all Junos OS platforms with proxy-macip-advertisement statement configured, at times during longevity tests, there are missing ARP, MAC, and ND entries in the kernel while the I2ald and rpd have the entry. [PR1609322](#)
- VM moves across DC where there is no translate VNI configuration in the interconnect work as designed. This problem occurs only with the translation VNI when MAC is moved from DC1 to DC2. [PR1610432](#)

## Flow-based and Packet-based Processing

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

## Forwarding and Sampling

- Firewall filter counter information do not match. [PR1623170](#)

## General Routing

- When VLAN is added as an action for changing the VLAN in both ingress and egress filters, the filter is not installed. [PR1362609](#)
- PTP-primary and PTP-secondary port configuration accepts the PTP packets with multicast MAC address according to the port settings. When `forwardable multicast` is configured, the PTP packets with forwardable MAC address is accepted and non-forwardable MAC address is dropped. When `link-local multicast` is configured, the PTP packets with non-forwardable MAC address is accepted and forwardable MAC address is dropped. [PR1442055](#)
- When you boot MPC11 linecard, the following harmless errors are seen. These errors have no functional impact. *timestamp* device kernel: i2c i2c-100: (11/1:0x41) i2c transaction error (0x00000002) *timestamp* device kernel: i2c i2c-64: (7/1:0x41) i2c transaction error (0x00000002) [PR1457655](#)
- On the MX960 router, the following error message might be observed: SCHED L4NP[0] Parity errors. [PR1464297](#)
- When running the command `show pfe filter hw filter-name filter name`, the command fails to retrieve the Packet Forwarding Engine programming details of the filter. [PR1495712](#)
- After backup Routing Engine halt, CB1 goes offline and comes back online; this leads to the backup Routing Engine booting up, and it shows the reboot reason as "0x1:power cycle/failure." This issue is only for the RE reboot reason, and there is no other functional impact of this. [PR1497592](#)
- In the platform using indirect next hop (INH), such as Unilist as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the `fastreroute` session might be enabled in Packet Forwarding Engines. When the version-id or session-id of the indirect next hop is above 256, the Packet Forwarding Engine might not respond to session update, which might cause the session-id to be stuck permanently with the weight of 65535 in the Packet Forwarding Engine. This might lead the Packet Forwarding Engine to have a different view of Unilist against load-balance selectors. Then, either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. [PR1501817](#)
- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. [PR1514364](#)
- Due to BRCM KBP issue route lookup might fail. Need to upgrade KBP to address this issue. [PR1533513](#)
- When an image with the third party SDK upgrade (6.5.x) is installed, the CPU utilization might go up by around 5 percent. [PR1534234](#)



- Flap might be observed on channelized ports during ZTP when one of the ports is disabled on the supporting device. [PR1534614](#)
- On a scaled MX2020 router with `vrf localisation` enabled, 4 million next hop scale, and 800k route scale, FPCs might go offline on GRES. Post GRES, router continues to report many fabric related CM\_ALARMS. FPC might continue to reboot and might not come online. Rebooting master and backup Routing Engine will help recovering and get the router back into a stable state. [PR1539305](#)
- FPC might not be recognized after power cycle (hard reboot). [PR1540107](#)
- The following error message is observed: "Feb 27 20:26:40 xolo fpc3 Cannot scan phys\_mem\_size.out. Please collect /var/log/\*.out (0;0xdd3f6ea0;-1) (posix\_interface\_get\_ram\_size\_info): Unknown error: -1." [PR1548677](#)
- 5M DAC connected between QFX10002-60C and MX2010 platforms does not link up. But with 1M and 3M DAC, interoperability works as expected. Also, it is to be noted that connection between QFX10002-60C and ACX or traffic generator works seamlessly with the same 5M DAC. [PR1555955](#)
- VE and CE mesh groups are default mesh groups created for a given routing instance. On adding VLAN or bridge domain, flood tokens and routes are created for both VE and CE mesh-group and flood-group. Ideally, VE mesh-group does not require a CE router where IGMP is enabled on CE interfaces. MX Series based CE boxes have unlimited capacity of tokens, so this would not be a major issue. [PR1560588](#)
- In MVPN case, if the nexthop index of a group is not same between primary and backup after a nsr switchover, you might see a packet loss of 250 to 400 ms. [PR1561287](#)
- Due to 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](#)
- To avoid the additional interface flap , interface hold time needs to be configured . [PR1562857](#)
- Stale TCNH entries are seen in a new primary Routing Engine after switchover with NSR even though all the prpd routes are deleted. These TCNH entries are present because NSR is not supported for BGP static programmable routes. This leads to an extra reference count in the backup Routing Engine, due to which the next hop is not freed. [PR1566666](#)
- Flag, source and logical address are not expected in MAC address found in BD BD-3 instance. [PR1569546](#)
- When an aggregated Ethernet link is brought down, a transient error message: [Error] Nexthop: EalNhHandler: failed to add Nh: xxxx, type: composite, as pil add failed might be seen. There is no functional impact due to this error. [PR1570710](#)

- The following messages might be seen in the logs from MPC11E line-card: Feb 9 11:35:27.357 router-re0-fpc8 aftd-trio[18040]: [Warn] AM : IPC handling - No handler found for type:27 subtype:9 There is no functional impact, these logs can be ignored. [PR1573972](#)
- In EVPN-VXLAN scenario with OSPF configured over the IRB, OSPF sessions might not get established due to connectivity issues. [PR1577183](#)
- When you configure /8 pool with block size as 1 and commit, the block creation utilizes more memory causing NAT pool memory shortage which is currently being notified to customer with syslog tagged RT\_NAT\_POOL\_MEMORY\_SHORTAGE. [PR1579627](#)
- In a fully loaded device, the firewall programming fails at times due to scaled prefix configuration with more than 64,800 entries. However, this issue is not observed in development setup. [PR1581767](#)
- Bridge domain names information is not displayed properly in show bridge statistics instance. [PR1584874](#)
- The output of the show services count command on vms interface is not as expected when you send the FTP traffic from the public side after configuring with NAPT44+EIM+APP+PCP. [PR1588046](#)
- An inline NPT on MX Series router does not translate source IPv6 packet with the current authentication header. The packet is simply passed through the upstream. Consequently, it is not expected that downstream traffic arrives with NPT pool, IPv6 address as IPv6 destination address, and with authentication header. Such traffic might be malicious and this must be handled via external configuration. As a workaround, configure firewall for downstream direction that blocks traffic destined to NPT pool address and with authentication header. [PR1592957](#)
- Pim VxLAN does not work on TD3 chipsets enabling VxLAN flexflow after Junos OS Release 21.3R1. Customers Pim VxLAN or data plane VxLAN can use the Junos OS Release 21.3R1. [PR1597276](#)
- On all MX Series routers, changing AMS 1:1 warm-standby configuration to load-balance or deterministic NAT might result in generating vmcore file causing traffic loss. [PR1597386](#)
- On MX10016 router, the SFB plane not online alarm gets generated after the primary Routing Engine switchovers. [PR1597630](#)
- On MX Series routers, compact forwarding engine board (afeb) process might crash with MIC-3D-8DS3-E3. If a MIC-3D-8DS3-E3 having any hardware fault is initialized into the device. The AFEB crash will restore automatically in sometime and faulty hardware need to be replaced. The AFEB crash might impact the traffic forwarding during the time of issue. [PR1598411](#)
- Read write lock is not acquired during the sysctl invocation. The assert triggered in the interface state function call leads to RE1 going to debug (db>) prompt. [PR1598814](#)
- It seems that ubuntu root-fs 18.04 shipped in the latest release does not have the "en\_US.UTF-8" locale enabled by default. [PR1601262](#)

- The convergence time degradation is seen in IS-ISv6, OSPFv2, and OSPFv3 when comparing convergence time with Junos OS Release 21.1R1.5. As it is a convergence time issue, many components are involved and hence need investigation of rpd, kernel, and Packet Forwarding Engine. [PR1602334](#)
- In vMX platform, after a system reboot, the protect-Routing Engine filter on lo0 interface is no longer applied. [PR1604401](#)
- In an MX Series Virtual Chassis setup with MS-MPC or SPC3 service cards using AMS/MAMS interfaces configuration, it is possible that the traffic on an MPC2 line card in the protocol backup chassis is not correctly load balanced due to timing conditions. As a workaround, reboot the affected line card while the service card is online. [PR1605284](#)
- IPv6 link local BFD session might not come up if there is no child link of an aggregated Ethernet mapped to pfe inst 0. This issue is applicable to MPC9 and below MX Series-based line cards. [PR1607077](#)
- On MX204, PIC 0 interfaces configured speed 1GE with QSFP-to-SFP adapter (QSA) keep flapping with "Ethernet PCS Block Not Locked/Locked Delta Event" messages. [PR1609988](#)
- When high pps traffic sent for a 'establish tunnels on-tarffic' ipsec vpn with S2S configuration, IKED process will be inundated with IKE trigger and IKE negotiation messages from peer. This causes delay in handling messages at IKED process and timeouts for IKE negotiations. Eventually results in tunnels do not get established. This issue might occur when the tunnels are negotiated for the first time or when one of the VMS in the AMS bundle goes down. [PR1610863](#)
- In some NAPT44 and NAT64 scenarios, duplicate SESSION\_CLOSE syslog will be seen. [PR1614358](#)
- ICMP error packet do not have relevant header when configured with DSLite and with appropriate ICMP ALG name and one UDP application name. [PR1616633](#)
- MPC gets rebooted while enabling FLT for inet6 filter with 10000 terms, instead of fallback to DMEM filter gracefully. Currently, fast lookup filter supports up to 8000 terms. [PR1617174](#)
- MPLS toplevel address contains invalid values as opposed to 0.0.0.0. [PR1617186](#)
- Fabric errors could be expected when SLC is restarted when ISSU is in progress, to avoid this problem "do not restart SLC when ISSU is in progress". [PR1619180](#)
- Error: "Nexthop: Egress NhChain: numOfTags is 2 and srteGlobalIndex is 0 on all 3 FPCs" is not seen until there is a composite next-hop with 2 labels in it. Typically, this scenario is not seen and there is no impact in behavior and traffic with these errors. [PR1621689](#)
- System\_id formate of AFT-MPC(MPC10E) is not aligned with non-AFT MPCs. [PR1622073](#)
- Fabric goes to check state when configuration changed on Bsys during ISSU on GNF. [PR1622511](#)

- A vmcore file will be generated when we have multiple netconf sessions to the router executing the following sequence of commands: `show interfaces lb-stats afX clear interfaces lb-stats afX`. [PR1627123](#)
- DHCPv6 server binding does not happen when LDRA is configured. To use dhcpv6 options, relay-server configuration can be used by the customer. LDRA is an alternative for that. Once we enable dhcp-relay configuration with snooping, dhcpv6 options or binding works fine . dhcp-relay configuration functionality is similar to LDRA. From customer point of view, LDRA can be achieved by dhcp-relay configuration. [PR1627600](#)
- On Junos platforms with MPC10E line cards, when aggregated Ethernet under the IRB interface is enabled between the snooping device and the DHCP server, the DHCP bindings can be seen in snooping device and DHCP server, but the DHCP client might not go to BOUND state, it might be stuck at discovering/requesting state. [PR1627611](#)
- DHCP binding will not happen, when MLD snooping is enabled. It might be a baseline MLD issue and not just specific to DHCP. [PR1627690](#)
- Carrier-transitions counters are not expected when doing interface down and up. [PR1601946](#)
- When rpd sends INH deletion or additions out of order (rarely occurs) message to backup rpd, the rpd crashes and generates a core file. [PR1607553](#)
- Transit IPv4-over-IPv6 encapsulated packets cannot pass through using IP over IP interface (ip-x/x/x). This behavior has been seen 'transit' packets only. [PR1618391](#)
- In the event that a line card loses power during the BIOS upgrade, there is a change that it'll not come up and will require the BIOS to be physical re-flashed. It is recommended as a best practice to ensure that chassis has backup power during a BIOS firmware upgrade. [PR1624345](#)
- Whenever vmhost image is installed on MX10008 chassis via USB, LC9600 will eventually go offline. Restart chassisd process (cli> restart chassis-control) upon completion of USB installation of VMHOST image on MX10008 REs to avoid LC9600 going offline. [PR1629558](#)
- For ACX5448, MX204 and MX2008 "VM Host-based" platforms, starting with Junos 21.4R1 or later, ssh and root login is required for copying line card image (chspmb.elf for MX2008) from Junos VM to Linux host during installation. The ssh and root login are required during installation. Use "deny-password" instead of "deny" as default root-login option under ssh config to allow internal trusted communication. Alternatively, once installed, it can be disabled in the configurations. Refer to <https://kb.juniper.net/TSB18224>. [PR1629943](#)
- DSLite not working on MX platform installed with MPC7E line card and SPC3 service PIC. [PR1632278](#)
- In Junos OS Release 21.4, observed that data traffic might not recover after Packet Forwarding Engine-reset execution when both configurations applicable to the same FPC are present: `set chassis`

fpc x error major action disable-pfe, set chassis fpc x error scope pfe category functional major action reset-pfe. [PR1632539](#)

- It is noted that the single hop BFD session over aggregated Ethernet is not fully functional after exercising Packet Forwarding Engine reset feature. The BFD session was up before Packet Forwarding Engine reset operation is initiated but after the reset the BFD rx session is not fully functional. [PR1632585](#)
- On MX Series platform with SPC3 service card installed, TFTP control sessions are getting refreshed with inactivity time out after data session is closed, causing the control session to stay in session table for some more time. Service impact is minor or negligible as the TFTP control session will eventually get deleted after timeout. [PR1633709](#)

## Interfaces and Chassis

- ICCP does not come up when mc-lag PE is rebooted since static ARP is deleted and never re-installed back. Therefore, it is not recommended to configure ICCP over IRB which is associated with mc-lag bridge 166 domain. Customer upgrading from old release to new release (PR 1075917 support) might come across issue like static ARP is not reinstalled for remote mc-lag IRB IP when existing static ARP entry is removed. [PR1409508](#)
- When family bridge is configured, logical interfaces are not created. If logical interfaces are not created, l2ald does not create IFBDs (interface to BD association) and if we do not have IFBDs in the system, STP is not enabled on that interface. [PR1622024](#)
- The remote-mep-state is not as expected. [PR1623960](#)

## Juniper Extension Toolkit (JET)

- Abrupt termination of the client socket may take time for the disconnect to be detected by JSD. The client would have to wait for the connection terminal to be detected in such cases, which could be around 1 hour or restart JSD before being able to connect back with the same client ID. [PR1549044](#)
- The stub creation functions will not be available. [PR1580789](#)

## MPLS

- BFD session flaps during unified ISSU only in MPC7E line card. The issue is not seen frequently. [PR1453705](#)
- The use-for-shortcut statement is meant to be used only in SR-TE tunnels which use Strict SPF Algo 1 (SSPF) prefix SIDs. If [set protocols isis traffic-engineering family inet-mpls shortcuts] and [set protocols isis traffic-engineering tunnel-source-protocol spring-te] is configured on a device, and if any SR-TE tunnel using Algo 0 prefix SIDs is configured with the use-for-shortcut statement, it could lead to routing loops or rpd process core files. [PR1578994](#)
- LDP session authentication key-chain configuration made based on the session remote-id on initiator stops from session establishment even though the responder's authentication key-chain is configured for its remote-id. [PR1592431](#)
- On the MX10016 routers, when there is scaled RSVP sessions (for example, 21,000) and the RSVP is enabled for all the interfaces, then the rpd process goes through all the interfaces which results into a high CPU utilization for some time. This also results in LSP flap. [PR1595853](#)

## Layer 2 Features

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

## Network Management and Monitoring

- On MX240 platform, the facter version is not installed and fails to set PATH variable. [PR1609185](#)
- mgd might crash and generate a core file when an invalid value is configured for identityref type leafs/leaf-lists while configuring Openconfig or any other third-party YANG, problem occurs with json and xml loads. [PR1615773](#)

## Platform and Infrastructure

- With GRES and NSR functionality with VXLAN feature, the convergence time might be slightly higher than expected for Layer 2 domain to Layer 3 VXLAN. [PR1520626](#)
- When the DHCP relay mode is configured as no-snoop, we are observing the offer gets dropped due to incorrect asic programming. This issue only affects while running DHCP relay on EVPN/VXLAN environment. [PR1530160](#)
- When a EX4400 Virtual Chassis is scaled with different features configurations and device is stressed with traffic, device might not respond for CLI commands for a short period of time and a vmcore might be reported at that time. Once VM core is saved, device will continue to operate normally. [PR1599498](#)
- The corrupted mbuf's m\_data is pointed to 0xdead, which will be set only during m\_free. And the m\_lw\_state is not set to deallocated. Slab\_info of the mbuf is in allocated state. but it's external buffer is in free state. In the socket's rcv buffer sb\_mb is null and sb\_ccc is zero, which indicates that the rcv buffer has been freed or there is no more data left in the buffer. [PR1602442](#)
- TWAMP-Light is supported on MX Series and PTX Series platforms. CLI configuration support will be disabled on all other platforms. Do not use the control-type light under platforms where this feature is not supported. Currently, IPv4 and IPv6 twamp-light is supported on the platforms using TRIO and PE chipsets. [PR1603128](#)
- On MX480 routers, traffic loss of 19 percent occurs with the vrrp mastership change from backup to master while bring up the route back after enabling the link. [PR1612504](#)

## Routing Protocols

- On MX960 router, the backup path fails to install in the LAN scenario and breaks the SR-MPLS for LAN when more than four end-x SIDs are configured on the interface. [PR1512174](#)
- In a Virtual Chassis or Virtual Chassis fabric scenario, inconsistent MCSNOOPD core file is seen when the igmp-snooping configuration is removed. [PR1569436](#)
- SHA-1 system login password format are not accepted post the upgrade. [PR1571179](#)
- On all Junos OS with nonstop routing (NSR) enabled, the rpd crash and restart might occur when Resource Public Key Infrastructure (RPKI) records are being replicated between the primary and backup Routing Engine and some of the records are withdrawn over the RPKI session. [PR1620463](#)
- Enabling FIPS mode fails with self-test failure and kernel crash. [PR1623128](#)

## Services Applications

- In L2TP environment on L2TP access concentrator (L2TP LAC), few L2TP tunnels might get stuck in down state and might not be able to re-establish if bbe-smgd process is restarted when these tunnels went down. [PR1629104](#)

## VPNs

- On MX Series devices, during unified ISSU, the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. [PR1416334](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1 | 85](#)

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.

### Resolved Issues: 21.4R1

### IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 86](#)
- [Class of Service \(CoS\) | 86](#)
- [EVPN | 87](#)
- [Forwarding and Sampling | 87](#)
- [General Routing | 87](#)
- [High Availability \(HA\) and Resiliency | 97](#)



- Infrastructure | 97
- Interfaces and Chassis | 97
- J-Web | 98
- Junos Fusion Enterprise | 98
- Layer 2 Ethernet Services | 98
- MPLS | 99
- Multicast | 99
- Network Address Translation (NAT) | 99
- Network Management and Monitoring | 100
- Platform and Infrastructure | 100
- Routing Policy and Firewall Filters | 101
- Routing Protocols | 101
- Services Applications | 102
- Subscriber Access Management | 102
- Unified Threat Management (UTM) | 103
- User Interface and Configuration | 103
- VPNs | 103

## Application Layer Gateways (ALGs)

- ALG traffic might be dropped [PR1598017](#)

## Class of Service (CoS)

- In a Junos Fusion deployment, dynamically removing and adding a logical interface under interface-set could lead to traffic control profile on the interface-set not working [PR1593058](#)
- Child mgd processes might get stuck when multiple sessions continuously ask for interface information [PR1599024](#)
- Traffic loss might be observed if per-unit-scheduler is configured on AE interface [PR1599857](#)
- 802.1p rewrite policies might not have any effect if the rewrite is tied to CCC interfaces [PR1603909](#)
- IEEE 802.1 rewrite rule might not work on MPC10 linecard [PR1604943](#)

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

## EVPN

- baseline EVPN-VXLAN Transition from IPV4 to IPV6 or vice verse doesn't work in certain sequence [PR1552498](#)
- The BUM traffic might be dropped after changing any configuration on the device without router-id configured [PR1576943](#)
- Traffic loss might be seen under EVPN scenario when MAC-IP moves from one CE interface to another [PR1591264](#)
- Transit Traffic gets dropped post disabling one of the PE-CE link on a remote Multi-Home PE in EVPN-MPLS A-A setup with Dynamic-List NextHop configured [PR1594326](#)
- EVPN might not work properly in multi-homing setup [PR1596723](#)
- The device announces router-mac, target, and EVPN VXLAN community to BGP IPv4 NLRI [PR1600653](#)

## Forwarding and Sampling

- Logical interface statistics for as(aggregated sonet) are displayed double value then expected. [PR1521223](#)
- The snmpwalk may not get polling the mib for dual-stack interface [PR1601761](#)

## General Routing

- On MX10003, despite of having all AC low/high PEM, "Mix of AC PEMs" alarm is raised [PR1315577](#)
- RE switchover does not work as expected while SSD failure occurs. [PR1437745](#)
- SSL-FP Logging for non SNI session [PR1442391](#)
- Inaccurate allocated memory for 'nh' and 'dfw\_rulemask' under kernel might be observed [PR1475478](#)
- The following error messages are observed: unable to set line-side lane config (err 30) [PR1492162](#)
- New fan failure alarm that would be reported after 3 consecutive failure interrupt status is high. [PR1500920](#)
- With multi-services scaled config and Jvision monitoring running after routing-restart, protocols/services remains down and rpd doesn't respond/recover [PR1520977](#)

- The BFD session status remains down at the non-anchor FPC even though BFD session is up after the anchor FPC reboots or panic. [PR1523537](#)
- CSPRNG is changed to the HMAC-DRBG and cannot be changed to either the FreeBSD Fortuna or the Juniper DYCE RNGs [PR1529574](#)
- cli show chassi picd fpc-slot pic-slot did not display qsfp modules firmware properly [PR1533645](#)
- The MACsec PICs may stay offline in the new primary after performing ISSU [PR1534225](#)
- Pfe statistics not shown GNF in sublc mode having PFE mapping from non-zero pfe [PR1547890](#)
- FPC crash may occur after flapping the multicast traffic [PR1548972](#)
- Some transmitting packets may get dropped due to the "disable-pfe" action is not invoked when the fabric self-ping failure is detected [PR1558899](#)
- The device may run out of service post GRES/ISSU [PR1558958](#)
- The MX150 device might reboot after performing request system snapshot recovery command. [PR1565138](#)
- Na-grpcd process can core during longevity tests [PR1565255](#)
- CLI-command "show pfe statistics traffic" shows wrong output [PR1566065](#)
- Junos OS and Junos OS Evolved: Local Privilege Escalation and Denial of Service [PR1568654](#)
- When using log templates (introduced in 21.1R1) with Unified Policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile (set security log profile name default-profile) that can be used to improve this behaviour when multiple log profiles are defined. [PR1570105](#)
- High CPU usage may occur on rpd for routes that use static subscriber [PR1572130](#)
- The fxpc process might crash and cause traffic loss in the IFBD scenario [PR1572305](#)
- DCPFE/FPC crash may be observed on the QFX10000 series platforms if ARP MAC move happens [PR1572876](#)
- Only root user is allowed to execute commands on host using vhclicent. [PR1574240](#)
- DS-Lite throughput degradation might be seen on MS-MPC [PR1574321](#)
- MIC specific alarms are not cleared after MIC reboot [PR1576370](#)
- MPC7E, MPC10E, MX-SPC3 and LC2103 line cards might become offline when the device is running on FIPS mode [PR1576577](#)

- Mirrored packets are corrupted when port-mirror and discard actions are both applied. [PR1576914](#)
- MPC7E/8E/9E/11E line card might be stuck in "Unresponsive" state in a Junos Node Slicing setup [PR1580168](#)
- The static MACs configured over AE might not get programmed in forwarding after the FPC restart [PR1581325](#)
- Certain fields in the GNMI extension header and show network-agent statistics cli will have incorrect values if the input subscription path contains a ":" character [PR1581659](#)
- Junos OS and Junos OS Evolved: A vulnerability in the Juniper Agile License Client may allow an attacker to perform Remote Code Execution (RCE) (CVE-2021-31354) [PR1582419](#)
- Traffic drop might be observed on MX platforms with SPC3 in the DS-LITE scenario [PR1582447](#)
- Load balancing is not working correctly on AMS interfaces for CGNAT traffic on MX USF mode with SPC3 [PR1582764](#)
- The bcmd process might crash on the MX150 platform [PR1583281](#)
- Firewall filter is not getting programmed after deleting a large filter and adding a new one in a single commit on QFX5000 line of switches. [PR1583440](#)
- The Layer 2 multicast VXLAN instance goes down since local vtep logical child interface is not associated to the EVPN instance. [PR1584109](#)
- The secure web proxy continues to send the DNS query for the unresolved DNS entry even after removing the entry. [PR1585542](#)
- Packet loss might be seen during global repair of FRR. [PR1586122](#)
- show security idp counters do not have tenant statement in it's syntax. [PR1586220](#)
- The RPD\_KRT\_KERNEL\_BAD\_ROUTE error message is seen in certain scenarios when the rpd process restarts or GRES happens when NSR is enabled. This error has no functional impact. [PR1586466](#)
- Remove SIB without turning offline first might impact traffic. [PR1586820](#)
- The MVPN traffic loss might be seen due to the flooded multicast next-hop is missed [PR1587054](#)
- Junos Telemetry Interface leaves such as "used-power" and "allocated-power" under /components do not reflect correct value. [PR1587184](#)
- PEM capacity shows incorrectly on MX10003 platform. [PR1587694](#)
- Incorrect error message is observed when request chassis cb slot 1 offline statement is executed before node goes offline. [PR1589433](#)

- The aftd process might crash in firewall filter scenario. [PR1589619](#)
- Fabric link training could be seen if the fabric selfping silently gets discarded. [PR1590054](#)
- The open configuration BGP route community command output is incorrect when you use large BGP communities. [PR1590083](#)
- PTP synchronization might get unstable. [PR1591667](#)
- The mobiled daemon might crash after switchover for an AMS interface or crashes on the service PIC with the AMS member interfaces. [PR1592345](#)
- AMS warm standby with deterministic NAT functionality might not work properly. [PR1592437](#)
- Routing Engine kernel might crash because the logical interface of aggregated interface fails in the Junos kernel. [PR1592456](#)
- The duplicate Junos Telemetry Interface leaf of oper-status tag for logical interface index 16386 have mismatch value. [PR1592468](#)
- The L2cpd-agent might go unresponsive after starting telemetry service. [PR1592473](#)
- Using the BITS interface from backup RE for clock recovery might not work. [PR1592657](#)
- After Routing Engine switchover, the following error messages are seen:

```
JexprSlowCntrRead - Unable to get the plct Inst for pfeIdx: 255, User-type:
OVFM_OFFCHIP_NEXTHOP_CNTR.
```

[PR1593079](#)

- The TCP connections to the telemetry server might be stuck in "CLOSE\_WAIT" status. [PR1593113](#)
- On a Junos Node sliced setup if an SLC on MPC11E is restarted on some instances the interfaces on other SLC might also go down. [PR1593500](#)
- IPv6 neighbor might remain unreachable in VRRP for IPv6 scenario. [PR1593539](#)
- Jweb Deny log nested-application displays unknown instead of the specific application. [PR1593560](#)
- The dcpfe process might crash in an EVPN-VxLAN scenario. [PR1593950](#)
- PICD restart or crash might result in junks statistics for carrier transition. [PR1594253](#)
- The next-hop used for lawful intercept might not get installed correctly on the Packet Forwarding Engine of MPC10E or MPC11E line card which does not host the tunnel interface used for flow-tap service. [PR1594380](#)

- The BFD session for MPLS LSP goes down after enabling ultimate-hop-popping. [PR1594621](#)
- The label field for the EVPN Type 1 route is set to 1. [PR1594981](#)
- Inconsistent component name for FPC CPU is observed. [PR1595109](#)
- Application error alarms and trace-writer core files are generated due to defunct rcv zombie. [PR1595409](#)
- Layer 2 VPN stops forwarding when interface encapsulation is changed to vlan-ccc from ethernet-ccc and back. [PR1595455](#)
- Some TCP sessions might not be established after performing the request system snapshot command. [PR1595470](#)
- The interface down might be delayed after you issue the set interface interface name disable command. [PR1595682](#)
- Firmware might fail to be downloaded to MIC on the MX Virtual Chassis setup. [PR1595693](#)
- Mismatch in the master and backup Routing Engines with inetcolour tables and BGP-SRTE tunnels occur after rpd-restart on the primary Routing Engine. [PR1596095](#)
- Packet Forwarding Engine wedge might occur if many IPv4 packets are received that need to be fragmented. [PR1596100](#)
- The DCI InterVNI and IntraVNI traffic might silently be dropped and discarded in a gateway node due to the tagged underlay interfaces. [PR1596462](#)
- Mscnnoopd might crash when deleting and then adding layer-2 forwarding configuration after performing unified ISSU. [PR1596483](#)
- The nsd process generates a core file when you verify the session-limit rate and issue the bypass-traffic-on-exceeding-flow-limits command. [PR1596578](#)
- Traffic loss might occur periodically in the MACsec-used setup if the Routing Engine works under a pressure situation. [PR1596755](#)
- SR-TE tunnel initiated from a non-juniper PCE might fail [PR1596821](#)
- bbesmgd core generated after RE goes down. [PR1596848](#)
- Traffic fails to recover after multiple quick dot1xd restarts when you enable the MACsec suspend-for option. [PR1596854](#)
- The interface might not learn mac-address if it is configured with vlan-id-list starting with VLAN id 1 and native-vlan-id. [PR1597013](#)
- Major alarms on all FPCs in chassis might be seen after some time from bootup. [PR1597066](#)

- The MAC/IP withdraw route might be suppressed by rpd in the EVPN-VxLAN scenario. [PR1597391](#)
- On MX10016 router, the SFB Plane not online alarm gets generated after the primary Routing Engine switchovers. [PR1597630](#)
- Major host 13 Ethernet interface link goes down with false alarm after RE1 is manually replaced. [PR1597763](#)
- MPC10E log messages will be observed with 'Temp Sensor Fail' alarm set/clear and 'cmtfpc\_cpu\_core\_temp\_get: Fail to get temp CPU7\_PMB' messages. [PR1597798](#)
- The cfmman process might crash on MPC10 linecard running on FPCs. [PR1597812](#)
- Deletion of MACsec configuration on a logical interface does not take effect. [PR1597848](#)
- Inconsistency in the platform name used in multiple places, version, snmp mibs, and so on. [PR1597999](#)
- [subscriber\_services][MX480] :: subinfo core file is generated with L2 node scaling. [PR1598187](#)
- Primary-only IP address keeps in old primary (new backup) and device becomes inaccessible after Routing Engine switchover. [PR1598173](#)
- arpd and ndp daemon crashes in scale setups. [PR1598217](#)
- Subscriber management daemons might continuously generate a core file and shutdown with Routing Engine sensor invalid configuration. [PR1598351](#)
- On MX10016 routers with JNP10K-RE1, unknown SMART attributes for StorFly VSFBM8CC200G SSD occurs. [PR1598566](#)
- Upper backplane type for the MX2020 router are incorrectly reported as Chassis. [PR1598594](#)
- The packet loop might occur after you receive the PCP request packets, which are destined to software concentrator address. [PR1598720](#)
- Component sensor does not export logs. [PR1598816](#)
- The l2ald process might crash due to memory leak when all active interfaces in a VLAN are unstable. [PR1599094](#)
- False fan failure alarm flaps (set and cleared) frequently. [PR1599183](#)
- NSR switchover performed with BGP SR-TE tunnels might generate an rpd core file. [PR1599446](#)
- On MX SPC3 services card, ICMP protocol is not detected and does not allow user to modify inactivity-timeout values. [PR1599603](#)
- gNMI Telemetry might stop working after Routing Engine switchover. [PR1600412](#)

- The multiservices card does not drop the TCP acknowledgment packet received as a reply to the self-generated TCP keepalive. [PR1600619](#)
- The config interface ip remove command is not working appropriately. [PR1600932](#)
- Duplicate address detection (DAD) flags appear for the IRB interfaces after removing the configuration and restoring which might lead to traffic block. [PR1601065](#)
- Traffic loss might be seen on MPC10E and MPC11E under EVPN scenario. [PR1601177](#)
- The BBE-SMGD process generates core files at bbe\_dequeue\_and\_deliver bbe\_process\_work\_queues bbe\_smd\_main\_post\_dispatch. [PR1601203](#)
- Unable to commit configuration due to the Check-out failed error message for the mobility process. [PR1601785](#)
- Traffic might be dropped at NAT gateway if you enable EIM. [PR1601890](#)
- Kernel crash might be seen when static routes are configured with GRE interfaces being used as next-hop. [PR1601996](#)
- The IPv6 traffic might be impacted on the QFX Series or PTX Series platforms when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)
- A few line cards might not come up online with increased-bandwidth mode. [PR1602080](#)
- Under certain scaling scenarios, with EVPN-VXLAN configurations, l2ald might abort and recover. [PR1602244](#)
- After upgrading, configured firewall filters might be applied on incorrect interfaces (CVE-2021-31382). [PR1602292](#)
- Traffic might be lost when rewrite rules are configured on an aggregated Ethernet egress interface of MX Series platforms with MPC10E linecards. [PR1602307](#)
- Jflow-syslog for CGNAT might use 0x0000 in IPv4 identification field for all fragments. [PR1602528](#)
- The show system errors fru detail command is not displaying "reset-pfe" as the cmerror configured action. [PR1602726](#)
- The Packet Forwarding Engine might get disabled by a detected major CMERROR event when you ungracefully remove the MIC from MPC2E-3D-NG/MPC3E-3D-NG. [PR1602939](#)
- Junos OS: When using J-Web with HTTP an attacker might retrieve encryption keys via Person-in-the-Middle attacks. (CVE-2021-31386). [PR1603199](#)
- Packet loss might be seen on filter-based GRE deployments. [PR1603453](#)



- 21.3TOT:TCP\_TLS\_SYSLOG:core-usf-qnc-a-fpc3.pic1-flowd\_spc3.elf.0.tgz is seeing while verifying TCP based logging functionality with GRES with AMS-Nexthop style [PR1603466](#)
- NSSU performed with MACsec configuration might generate fxpc core file. [PR1603602](#)
- The adapted sample rate might get reset to the configured sample rate without changing the sampling rate information in sFlow datagrams after configuring a new logical interface and enabling sFlow technology on this new logical interface at the same time. [PR1604283](#)
- NPC logs are observed when vrf localisation is enabled. [PR1604304](#)
- The following error message is observed: evo-aftmand-bt[18089]: [Error] IfStats:map entry not present for ifl:1039. [PR1604334](#)
- Interface hold-time up does not work on vMX and MX150 platforms. [PR1604554](#)
- The channel 0 physical interface does not come up after adding the correct speed configuration. [PR1604810](#)
- The interface on MCP3-NG HQoS/MPC7E flaps continuously after enabling LACP on aggregated Ethernet interface. [PR1605446](#)
- The MPLS transit router might push an extra Entropy label to the LSP. [PR1605865](#)
- Multicast streams might stop flooding in VXLAN setup. [PR1606256](#)
- Segment Routing License issue might occur by default chained-composite-next-hop configuration. [PR1606377](#)
- Observing continuous SNMP trap for "Over Temperature!" for all the MX10016 line cards (FPC: JNP10K-LC480). [PR1606555](#)
- With dslite prefix-based subscriber and PCP the APP mapping for multiple PCP requests with suggested external ports is not behaving as expected. [PR1606687](#)
- New subscribers might not connect due to the CR-features service object missing on FPC. [PR1607056](#)
- TCP traffic might be dropped on source port range 512 to 767 when the FlowSpec IPv6 filter is configured. [PR1607185](#)
- In subscriber management scenario, under a rare condition, the Routing Engine reboots and generates a vmcore. [PR1607282](#)
- When l2ald restart, the following error message might be present, "L2ALIPC : L2AL IPC client is not connected to l2ald on restart l2-learning" [PR1607580](#)

- On MX Series platforms, error messages might be seen on triggering restart routing when sensors are configured. [PR1608120](#)
- Traffic load balance issue might be seen while toggling link-protection mode of RLT interface on-the-fly. [PR1608300](#)
- Address error case in open message to comply to RFC 8664 in PCCD and PCE\_Server. [PR1608511](#)
- Memory leak might be observed on the l2cpd process when performing certain LLDP operations. [PR1608300](#)
- On PTX10K EVO platforms, defunct rcp processes increase which might cause master Routing Engine reboot. [PR1608776](#)
- High priority queue might not get the expected bandwidth on the EVO platforms. [PR1609823](#)
- The single-vlan tagged subscribers might fail to reconnect through dynamic-vlan over PS interface. [PR1609844](#)
- The authd process and RADIUS might have stale L2BSA subscriber entries. [PR1610476](#)
- After picd restart interface is down in channelized 100G link. [PR1611379](#)
- The service PICs are unable to come up when dnsf package is configured. [PR1612316](#)
- The Routing protocol engine CPU is getting stuck at 100 percent. [PR1612387](#)
- The B4 client traffic will be dropped on MX-SPC3 based AFTR in DS-Lite with EIM activated CGNAT scenario. [PR1612555](#)
- Some of the fabric links might go into faulty state after swapping FPC LC1201 with LC1202. [PR1612624](#)
- l2ald core file is generated during routing-instance configuration change. [PR1612738](#)
- Memory might be exhausted when both BGP rib-sharding and BGP Optimal Route Reflection (ORR) are enabled. [PR1613104](#)
- Traffic loss might occur due to the shaping rate being adjusted incorrectly in a subscriber environment on MX Series routers. [PR1613126](#)
- IGP routing updates might be delayed to program in Packet Forwarding Engine after interface flaps in a scaled BGP route environment. [PR1613160](#)
- For PS Service logical interface configured in MPC2-NG/MPC3-NG interface statistics do not show correct (shaped) value when shaping is applied. [PR1613395](#)
- IPsec tunnels are not deleted on disabling the AMS physical interface. [PR1613432](#)

- Enabling security-metadata-streaming DNS policy might cause a dataplane memory leak. [PR1613489](#)
- The rpd process might crash in BGP rib-sharding scenario. [PR1613723](#)
- Modifying the input-service-filter via COA might fail in subscriber management environment. [PR1614903](#)
- Line cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. [PR1614952](#)
- The l2ald process might crash in EVPN scenario. [PR1615269](#)
- Request to provide an API which gives list of potential policy given a session id. [PR1615355](#)
- show subscribers accounting-statistics, show services l2tp session interface asi0.xx statistics might not work on LNS with asi- interfaces. [PR1616454](#)
- The dual Routing Engine system might not be GRES ready after backup Routing Engine reboot in a subscriber management environment. [PR1616611](#)
- Inconsistent error counts in show interfaces brief and show interfaces extensive. [PR1616765](#)
- In MXVC spcd running on SPC3 crashes. [PR1617280](#)
- MPC8E in 1.6T bandwidth mode might not work correctly. [PR1617469](#)
- Automatic Routing Engine switchover might not happen after migration. [PR1617720](#)
- Traceroute packets might get dropped in SFW service-set when other service-sets with asymmetric traffic processing are also enabled on the same MS-MIC/MS-MPC. [PR1617830](#)
- The traffic loss of CGNAT might be seen after cleaning the large-scaled CGNAT sessions in MS-SPC3 based Inter-Chassis High Availability scenario. [PR1618360](#)
- [macsec] [fips] Lowest acceptable PN do not reflect correct value when replay-window-size is more than zero. [PR1618598](#)
- The clksyncd might crash and PTP/SyncE might not work. [PR1618929](#)
- The nsd might crash while validating NAT translation on MX Series platforms with SPC3. [PR1619216](#)
- /interfaces/interface/subinterfaces/subinterface/state/counters are not exported during initial synchronization for on-change. [PR1620160](#)
- EVPN type 5 routes might not be installed. [PR1620808](#)
- All ports from the same Packet Forwarding Engine goes down at the same time causes mqchip\_disable\_ostream timeout then triggers host loopback path wedge and disable-pfe. [PR1621286](#)

- Invocation of `netconf get` command will fail if there are no L2 interfaces in the system. [PR1622496](#)
- Port speed might show as 100G even though chassis configuration is set for 40G manually. [PR1623237](#)
- The aggregated Ethernet member link might not be correctly populated on the Packet Forwarding Engine after FPC restart on MX Series platforms. [PR1624772](#)
- Implement `show task scheduler-slip-history` to display number of scheduler slips and last 64 slip details. [PR1626148](#)
- S-PTX10K-144C License SKUs do not load, 400G SKUs do load. [PR1627459](#)
- Commit related to dynamic profile configuration changes might fail upon executing "request vmhost reboot routing-engine both" on MX platforms [PR1607494](#)
- Adding and removing VLANs might cause traffic loss. [PR1632444](#)

## High Availability (HA) and Resiliency

- When MTU is configured on an interface a rare ifstate timing issue might occur at a later point resulting in `ksyncd` process crash on backup Routing Engine. [PR1606779](#)

## Infrastructure

- In `tcpdump` command processing allows an attacker to bypass configured access protections and execute arbitrary shell commands (CVE-2021-31357). [PR1596122](#)
- Upgrade might fail when upgrading from legacy release. [PR1602005](#)
- The `fxpc` process might crash and generate core file. [PR1611480](#)

## Interfaces and Chassis

- Traffic might be interrupted while adding `xe-/ge-` interfaces as member of aggregated Ethernet interface bundle. [PR1569399](#)
- ARP resolution failure might occur during VRRP failover. [PR1578126](#)
- Junos Telemetry Interface optics sensor's alarm data type changed from "bool\_val" to "str\_val". [PR1580113](#)
- The `dcd` process might crash after performing Routing Engine switchover/reboot/management interface configuration change. [PR1587552](#)

- The dcd process crash might be observed after removing aggregated Ethernet logical interface from the targeted distribution database. [PR1591032](#)
- SIB might get stuck at an "offlining" state after performing offline and online operations. [PR1591076](#)
- Duplicate source and destination pair check is done only across same tunnel encapsulation type for FTI. [PR1599266](#)
- The dcd process might crash and FPC might be stuck in ready state on MX Series platforms. [PR1601566](#)
- The aggregated Ethernet interface might flap upon configuration changes. [PR1602656](#)
- LACP system priority might take a value of 0 and cause an LACP interoperability issue . [PR1602724](#)
- Few links on channelized interface is down after oir\_enable and oir\_disable in 4X25G. [PR1606644](#)
- Memory leak on dcd process occurs when committing configuration changes on any interfaces in a setup with AMS interface configured. [PR1608281](#)
- [interface] [platformtag] mx960 : :: PDT - MX960 : seeing dcd[40867]: %DAEMON-5: lo0 family maximum labels is non-adjustable in syslog messages. [PR1611098](#)

## J-Web

- J-Web allows a locally authenticated attacker to escalate their privileges to root. (CVE-2021-31372) [PR1594516](#)

## Junos Fusion Enterprise

- Reverting mastership from RE1 to RE0 might lead to l2ald daemon crash and cause an outage. [PR1601817](#)

## Layer 2 Ethernet Services

- The traffic received on a port in LACP detached state might be incorrectly forwarded. [PR1582459](#)
- The DHCP client might be offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)
- Delegated prefix IPv6 address is missing in accounting stop messages. [PR1588813](#)
- The DHCP ALQ queue might get stuck causing subscriber flap. [PR1590421](#)
- Uneven traffic distribution might be observed between member links of LAG. [PR1599029](#)

- The rpd scheduler might continuously slip after GRES when there are 7000 DHCP clients in a subscriber management environment. [PR1625617](#)

## MPLS

- The rpd process might crash in corouted bidirectional RSVP LSP scenario. [PR1544890](#)
- [mpls][generic] D-CSPF node segment label: unresolved when Node Index 0 configured. [PR1564169](#)
- The rpd core file is seen in the backup Routing Engine with in mirror\_process\_recvd\_data\_queue with mldp NSR configuration. [PR1594405](#)
- The LDP replication session might not get synchronized when dual-transport is enabled. [PR1598174](#)
- Sometimes MPLS LSP might go down due to a timing issue when a protected link goes down. [PR1598207](#)
- Static LDP P2MP might fail after NSR switchover. [PR1598344](#)
- The rpd might crash with LSP external controller configuration. [PR1601763](#)
- VPLS connection might get down if dual-transport is configured. [PR1601854](#)
- RSVP detour LSP might fail to come up when an LSR in the detour path goes down. [PR1603613](#)
- LDP P2MP traffic might be interrupted post GRES. [PR1609559](#)
- The rpd process might crash on standby\_re LDP module when vpls mac-flush is enabled on peer by default or configuration. [PR1610638](#)
- Configuring protocols mpls lsp-external-controller also throws commit error if in-place-lsp-bandwidth-update is configured under any LSP. [PR1612269](#)
- The rpd process might crash if express segments using SR-TE underlay are configured. [PR1613372](#)

## Multicast

- Intermittent p2mp traffic drop might be seen in MVPN scenario. [PR1608311](#)

## Network Address Translation (NAT)

- Services NAT mappings and sessions are incorrect while checking the SIP sessions from public to private and RTP from private to public. [PR1577922](#)

## Network Management and Monitoring

- The syslog archival transfer might fail if the archive site URL is configured with an IPv6 address. [PR1603342](#)
- SNMP reflects outdated ARP entries. [PR1606600](#)

## Platform and Infrastructure

- The L2TP tunnel might not work with filter-based encapsulation. [PR1568324](#)
- Aggregated Ethernet interface queue statistics will be exported to Junos Telemetry Interface server. [PR1571985](#)
- FPC crashes on MX Series and EX9200 platforms. [PR1579182](#)
- The system generates an audit core file while changing TACACS and login user passwords. [PR1589953](#)
- Upon receipt of specific sequences of genuine packets destined to the device, the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). [PR1595649](#)
- VLAN tagged traffic might be dropped with service provider style configuration. [PR1598251](#)
- The service filter might get programmed incorrectly in Packet Forwarding Engine because of the rare timing issue in enhanced subscriber management environment. [PR1598830](#)
- There might be FPC core file and packet drop in VxLAN-EVPN scenario. [PR1600030](#)
- The mgd process might crash with an authentication setup. [PR1600615](#)
- The kernel core file might be seen if BGP connections are restarting after deleting BGP authentication. [PR1601492](#)
- The ZTP service might not work and the image installation fails. [PR1603227](#)
- RTT output might not get displayed when show services rpm twamp client history-results command is issued. [PR1605243](#)
- The FPC might crash if flow-table-size is configured on MX Series platforms. [PR1606731](#)
- Multicast traffic is dropped when forwarded over VPLS via IRB. [PR1607311](#)
- FPC crash might be seen because of mac-move between two interfaces under same bridge domain. [PR1607767](#)
- Degraded traffic processing performance might be observed in case of processing very high PPS rate traffic. [PR1619111](#)

- CoS custom classifier might not work on logical interface. [PR1619630](#)
- Configuration commit might fail while configuring authentication-key-chains statement under groups. [PR1626400](#)

## Routing Policy and Firewall Filters

- BGP import policy is not applied to all the routes when CCNH inet is enabled. [PR1596436](#)
- The configuration check might fail if more than 8 FCs are configured and CBF is enabled. [PR1600544](#)
- The firewalld might crash if you configure fragment-offset statement outside the range (fragment-offset 1-900000000000). [PR1605805](#)

## Routing Protocols

- BGP session might be down due to BGP-LS TLV received out of order. [PR1546416](#)
- Conformance issues with draft-ietf-idr-bgp-ext-opt-param. [PR1554639](#)
- Incorrect authentication-algorithm is set in BGP neighbor. [PR1571705](#)
- Short multicast packets drop using PIM when multicast traffic is received at a non-RPT/SPT interface. [PR1579452](#)
- Traffic drop might occur on link flap when IS-IS is configured. [PR1585471](#)
- The rpd crash might be seen if BGP peer flaps. [PR1592123](#)
- NTF-AGENT core file is seen at `_Tthr_rwlock_unlock CRYPTO_THREAD_unlock OPENSSL_init_crypto`. [PR1597714](#)
- After first parallel ISSU aborts, subsequent ISSU attempts on failed node aborts with 'Aborting Daemon Prepare'. [PR1598786](#)
- IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. [PR1599084](#)
- Some routes might get incorrectly programmed in the forwarding table in the kernel with next-hop installed as DEAD. [PR1601163](#)
- The rpd process might be stuck at 100 percent in OSPFv3 scenario. [PR1601187](#)
- Packet drop might be seen when changing INET MTU for MPLS enabled interface in IS-IS SPRING scenario. [PR1605376](#)



- MPC10E at [topgun] rpd core file `rt_table_flash_job_cancel`, `rt_instance_set_lsi_ifl_data_shard`, and `rt_flash_all_internal` might be seen after deactivating and then re-activating the interfaces. [PR1605620](#)
- IS-IS LSP might not be originated if egress protection is configured. [PR1605969](#)
- The BGP replication might be stuck in "InProgress" state. [PR1606420](#)
- Multicast traffic might be duplicated on subscriber interface on MX Series platforms. [PR1607493](#)
- With rib-sharding enabled any commit will flap all BGP sessions with 4 byte peer-as (AS number 65536 or greater). [PR1607777](#)
- commit might fail when `microloop-avoidance post-convergence-path` is configured with out SR and SRv6. [PR1608992](#)
- The rpd might crash after a commit if there are more than one address in the same address ranges configured under [bgp allow]. [PR1611070](#)
- The rpd crash might be seen on all Junos OS and Junos OS Evolved platforms. [PR1613384](#)
- Verification of BGP peer count fails, after deleting BGP neighbors. [PR1618103](#)
- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific bgp export policies. [PR1626367](#)

## Services Applications

- `show services l2tp tunnel extensive`, `show services l2tp session extensive` and `show subscribers accounting-statistics` commands do not work on LTS. [PR1596972](#)
- Kmd core file has been generated at `kmd_gen_fill_sa_pair_sadb_flags @kmd_update_sa_in_kernel @kmd_sa_cfg_children_sa_free`. [PR1600750](#)
- `show services l2tp tunnel extensive`, `show services l2tp session extensive` commands provide incorrect outputs on LTS. [PR1601886](#)

## Subscriber Access Management

- Subscribers might be stuck in terminated state when the RADIUS server is unreachable. [PR1600655](#)
- The "Service session entry creation failed" errors are seen during ephemeral commit. [PR1603030](#)
- Install discard routes is not supported on APM managed BNGs running Junos OS Release 21.3R1. [PR1604967](#)
- Prefix duplication errors might occur for DHCPv6 over PPPoE subscribers. [PR1609403](#)

- DHCP session fails with CLI session-limit-per-username statement. [PR1612196](#)
- BNG does not correctly issue abatement alarm to APM when condition is met. [PR1626632](#)
- When connectivity between BNG and APM is lost, the BNG does not regenerate pool drained alarms to APM. [PR1627974](#)

## Unified Threat Management (UTM)

- There is no counter for juniper-local default action. [PR1570500](#)

## User Interface and Configuration

- Updates to the system login configuration might not be reflected after a commit. [PR1589858](#)
- File copy command is not accepting HTTPS URLs. [PR1596881](#)
- The dfwc and dcd processes might crash when a commit-check is performed after a previously terminated (with ctrl+c) commit-check [PR1600435](#)
- The commitd core file may be observed after committing some configuration change. [PR1601159](#)
- Configuration transfer-on-commit not working if commit is done via netconf. [PR1602331](#)
- Invalid JSON and xml output format for command like show system resource-monitor ifd-cos-queue-mapping fpc x | display [json|xml]. [PR1605897](#)

## VPNs

- The iked process might crash when IKEv2 negotiation fails on MX Series devices. [PR1577484](#)
- Cannot add BGP standard community to NGMVPN Type-6 and Type-7 routes in VRF export policy. [PR1589057](#)
- The rpd process might crash if the interface goes down in the BGP-MVPN scenario. [PR1597387](#)
- Wrong st0 IFL deletion at spoke when multiple VPNs negotiate same destination address as TS. [PR1601047](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 20.4R1 documentation for MX Series routers.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.4R1 | 105](#)
- [Procedure to Upgrade to FreeBSD 11.x-Based Junos OS | 105](#)
- [Procedure to Upgrade to FreeBSD 6.x-Based Junos OS | 108](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of- Life Releases | 110](#)
- [Upgrading a Router with Redundant Routing Engines | 110](#)
- [Downgrading from Release 21.4R1 | 111](#)

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 21.4R1

**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-
x86-32-20.4R1.9-signed.tgz
```

- For 64-bit Routing Engine version:

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

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

- For 32-bit Routing Engine version:

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

- For 64-bit Routing Engine version:

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

Replace source with one of the following values:

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

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

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

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

Rebooting occurs only if the upgrade is successful.

#### NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the `request vmhost software add` command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).
- Starting in Junos OS Release 21.4R1, 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 21.4R1 `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-20.4R1.9-
signed.tgz
```

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

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

Replace source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

**NOTE:** After you install a Junos OS Release 21.4R1 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 and Extended End-Of- Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

## 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 21.4R1

To downgrade from Release 21.4R1 to another supported release, follow the procedure for upgrading, but replace the 21.4R1 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 | 112](#)
- [What's Changed | 114](#)
- [Known Limitations | 114](#)
- [Open Issues | 114](#)
- [Resolved Issues | 115](#)
- [Documentation Updates | 117](#)
- [Migration, Upgrade, and Downgrade Instructions | 117](#)

These release notes accompany Junos OS Release 21.4R1 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [What's New in 21.4R1 | 112](#)

Learn about new features introduced in the Junos OS main and maintenance releases for NFX Series devices.

## What's New in 21.4R1

### IN THIS SECTION

- [Network Management and Monitoring | 112](#)
- [Routing Policy and Firewall Filters | 112](#)

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

### Network Management and Monitoring

- **Support for libvirt MIB (NFX150, NFX250 NextGen, and NFX350)**—Starting in Junos OS Release 21.4R1, you can monitor the performance of virtual machines by using the libvirt MIB. You can use either SNMPv2c or SNMPv3 to access the MIB data.

[See [Configuring SNMP on NFX150, NFX250 NextGen, and NFX350 Devices.](#)]

### Routing Policy and Firewall Filters

- **Support for secure vector routing (SVR) with 128T (NFX Series, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)**—

Starting in Junos OS Release 21.4R1, you can deploy software-based 128T distributed routing and network services with SRX Series or NFX Series. 128T services provide session-aware routing for IPv4 traffic and run on any general-purpose compute platform, while the SRX Series or NFX Series device provides a secure SD-WAN gateway and reliable service delivery.

For targeted sessions, the SRX Series or NFX Series device can be the first hop from the client or the last hop to the server. Vector routing packets that enter the device are tagged with source-tenant and destination-service and select the SVR path (to the 128T peer or another SRX Series or NFX Series device). Non-vector-routing packets such as preexisting IPsec tunnels follow their usual path through the device.

To support vector routing, we've introduced new CLI commands at the `[edit services vector-routing]` hierarchy level. Here you can identify the routers you will use with SVR:

```
router-name <router-name> {
  node-name <node-name> {
    interfaces <if-name>
  }
  service-route <service-route-name> {
    destination-service <destination-service-name>
    peer <peer-name>
  }
}
```

You can then define the source and destination sessions:

```
services {
  vector-routing {
    authority-name <authority-name>
    source-tenant <name> {
      interface <if-name>
      ip-prefix <...>
    }
  }
  destination-service <name> {
    ip-prefix <...>
    transport <tcp | udp | icmp | gre>
    port-range <start-port> to <end-port>
  }
  access-policy <source-tenant-name> permission permit / deny
  cipher-suite <cipher-suite-name>
}
}
```

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for NFX Series devices.

## Known Limitations

### IN THIS SECTION

- [Interfaces](#) | 114

Learn about known limitations in Junos OS Release 21.4R1 for NFX Series devices.

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

## Interfaces

- When you issue a show interface command on NFX150 devices to check the interface details, the system does not check whether the interface name provided is valid or invalid. The system does not generate an error message if the interface name is invalid. [PR1306191](#)

## Open Issues

### IN THIS SECTION

- [High Availability](#) | 115
- [Platform and Infrastructure](#) | 115
- [Virtual Network Functions \(VNFs\)](#) | 115

Learn about open issues in Junos OS Release 21.4R1 for NFX Series devices.

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

## High Availability

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

## Platform and Infrastructure

- On NFX250 devices, vector packet processing (VPP) is not loaded in a dual CPE, and at times in a single CPE. [PR1461238](#)

## Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interface (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. [PR1512331](#)
- Coredump might happen in the first boot of an NFX Series device that is in compute mode and has VNFs configured with more than 2G memory. [PR1589655](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | 116

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

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

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [Intrusion Detection and Prevention \(IDP\) | 116](#)
- [Interfaces | 116](#)
- [Platform and Infrastructure | 116](#)
- [Virtual Network Functions \(VNFs\) | 116](#)

## Intrusion Detection and Prevention (IDP)

- IDP predefined-attack-groups "Enterprise - Recommended" policy load fails on NFX250 NextGen devices due to insufficient heap memory on the data plane. [PR1588881](#)

## Interfaces

- Unable to configure destination-port on firewall filter on NFX250 NextGen devices. [PR1592019](#)
- On NFX Series devices, deletion of VNF interfaces that are mapped SR-IOV interface fails. [PR1598993](#)
- L3 dataplane interfaces are not appearing when flex mode is enabled on NFX350-S3 devices. [PR1599643](#)

## Platform and Infrastructure

- When the available free physical memory drops below 1.5 GB, configuration commits by Junos Device Management Daemon (JDMD) might not take effect and mustd core files are seen. This issue does not have any impact on the running traffic. [PR1599641](#)

## Virtual Network Functions (VNFs)

- On NFX Series devices, while configuring vmhost vlans using vlan-id-list, the system allows duplicate VLAN IDs in the VLAN ID list. [PR1438907](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for NFX Series devices.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 117](#)
- [Basic Procedure for Upgrading to Release 21.4 | 118](#)

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

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

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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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 21.4

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 21.4R1:

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 PTX Series

## IN THIS SECTION

- [What's New | 119](#)
- [What's Changed | 122](#)
- [Known Limitations | 124](#)
- [Open Issues | 125](#)
- [Resolved Issues | 127](#)
- [Documentation Updates | 130](#)
- [Migration, Upgrade, and Downgrade Instructions | 130](#)

These release notes accompany Junos OS Release 21.4R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

## IN THIS SECTION

- [What's New in 21.4R1 | 120](#)

Learn about new features introduced in the Junos OS main and maintenance releases for the PTX Series routers.

## What's New in 21.4R1

### IN THIS SECTION

- [Juniper Extension Toolkit \(JET\) | 120](#)
- [Operation, Administration, and Maintenance \(OAM\) | 120](#)
- [Routing Protocols | 121](#)
- [Source Packet Routing in Networking \(SPRING\) or Segment Routing | 122](#)
- [Additional Features | 122](#)

Learn about new features or enhancements to existing features in this release for the PTX Series.

### Juniper Extension Toolkit (JET)

- **Support for programming FTIs using JET APIs (PTX1000, PTX10002, PTX10008, PTX10016, QFX5100, and QFX10008)**—Starting in Junos OS Release 21.4R1, you can use the Interfaces Service API to configure flexible tunnel interfaces (FTIs) in Junos OS. You can change the attributes of the tunnel configurations for the unit under an existing FTI but cannot change the existing tunnel encapsulation type using the APIs. For the following families, you can configure only the listed attributes when you use JET APIs:

- `inet` and `inet6`: address and destination-udp-port
- `mpls` and `iso`: destination-udp-port

[See [Overview of JET APIs](#) and [Configure Flexible Tunnel Interfaces](#).]

### Operation, Administration, and Maintenance (OAM)

- **Enhancements to BFD-triggered FRR for unicast next hops and forwarding-table session-id-change-limiter-indirect to address issue of traffic being silently discarded (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)**—In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and forwarding-table session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

To align the traffic by creating session-id-change-limiter indirect next hop, set the `set routing-options forwarding-table session-id-change-limiter-indirect` configuration statement at the `[edit routing-options forwarding-table]` hierarchy level.

[See [Bidirectional Forwarding Detection \(BFD\) for MPLS](#).]

## Routing Protocols

- **Higher DDoS bandwidth for Layer 2 and Layer 3 protocols (PTX1000, PTX10002, PTX10008, QFX10002, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 21.4R1, we support higher distributed denial-of-service (DDoS) bandwidth for the following Layer 2 and Layer 3 protocols:

- Layer 3 protocols— RSVP, LDP, OSPF, BGP, BFD, PIM, IGMP, and ICMP
- Layer 2 protocol — IS-IS

[See [protocols \(DDoS\) \(ACX Series, PTX Series, and QFX Series\)](#).]

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by the Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

[See [How to Enable Link Delay Measurement and Advertising in OSPF](#).]

- **Enhanced support to handle S flag, D flag and A flags in IS-IS (MX Series and PTX Series)**—Starting in Junos OS Release 21.4R1, you can set the S flag to allow the label binding type, length and values (TLV) to leak through the IS-IS level (Level 1 or Level 2). You can set the A flag to program the penultimate-hop popping (PHP). You can set the D flag to prevent the leaking of the label binding TLV from Level 2 back to Level 1. Use the `no-binding` configuration statement at the `[edit protocols isis source-packet-routing no-binding-sid-leaking]` hierarchy level to disable label binding TLV leaks.

[See [Handling of the IS-IS Binding SID 'S' Flag and RFC 7794 Prefix Attribute Flags](#).]

- **Support for FAD and FAPM on traffic engineering database and BGP-LS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.4R1, we support FlexAlgo Definition (FAD) and FlexAlgo Prefix Metric (FAPM) on the traffic engineering database and BGP Link State (BGP-LS). You can store FAD and FAPM entries in the traffic engineering database and BGP-LS. You can also store multiple prefix segment identifiers (SIDs) for a prefix in BGP-LS. You can import the FAD and FAPM entries from the traffic engineering database to BGP-LS and export the FAD entries from BGP-LS to the traffic engineering database.

[See [What is Flexible Algorithm Definition \(FAD\)](#).]

## Source Packet Routing in Networking (SPRING) or Segment Routing

- **Compute traffic-engineered path delays using delay metrics (ACX5448, MX480, MX960, MX2010, MX2020, and PTX10008)**—Starting in Junos OS Release 21.4R1, you can use delay-based metrics for a Path Computation Element (PCE) to compute traffic engineered paths. You can use delay-based metrics to steer packets on the least latency paths, or the least delay path. To do this, you need to measure the delay on every link and advertise that using a suitable routing protocol (IGP or BGP-LS), so that the ingress has the per link delay properties in its TED.

[See [Computing Delay Optimized Intradomain and Interdomain Segment Routing Paths.](#)]

## Additional Features

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

- **Supported transceivers, optical interfaces, and DAC cables (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).**—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
- **Hold timer support on aggregated Ethernet (ae-) interfaces (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10004, MX10008, MX10016, PTX1000, PTX5000, PTX10002, PTX10008, PTX10016)** Specify the hold-time value to delay the advertisement of up and down transitions (flapping) on an interface.

[See [hold-time.](#)]

- **Increase in the number of supported aggregated Ethernet (ae-) interfaces to 256 from 128**(PTX1000, PTX5000, PTX10002, PTX10008, and PTX10016)

[See [Aggregated Ethernet Interfaces.](#)]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 123

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

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [General Routing | 123](#)
- [EVPN | 123](#)
- [Interface and Chassis | 123](#)
- [Network Management and Monitoring | 123](#)

## General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**— We do not support `request`, `show`, and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

## EVPN

- **Output for `show Ethernet switching flood extensive` command** The output for `show ethernet-switching flood extensive` now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as `unilist`. Previously, the output for `show ethernet-switching flood extensive` would misidentify the next-hop type as `composite`.

## Interface and Chassis

- When configuring multiple flexible tunnel interface (FTI) tunnels, the source and destination address pair needs to be unique only among the FTI tunnels of the same tunnel encapsulation type. Prior to this PR, the source and destination address pair had to be unique among all the FTI tunnels regardless of the tunnel encapsulation type.

## Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type `identityref` in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type `identityref` in the corresponding YANG data model, the

device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.

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

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

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 124

Learn about known limitations in Junos OS Release 21.4R1 for PTX Series routers.

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

## General Routing

- Condition: Offlining/restarting an FPC 'x' that is sending traffic to FPC 'y'. The error messages listed below are seen on the destination FPC. A corresponding alarm is set on the destination FPC Specific

to PTX10000 is the transient alarm, which gets set when this condition occurs. The alarm clears later because the source FPC is being offlined. Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210613), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: F0:core intr: 0x00000010: Grant spray drop due to unspray-able condition error Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Error (0x210614), module: PE Chip, type: Apr 09 10:31:24 [TRACE] [asta] Apr 9 10:19:59 asta fpc4 Cmerror Op Set: PE Chip: PE1[1]: F0:core intr: 0x00000008: Request spray drop due to unspray-able condition error. [PR1268678](#)

- JFlow cannot handle traffic with multiple Explicit NULL labels. When sampled traffic has two Explicit NULL labels, the packets are dropped and the trapstats increment. [PR1601552](#)

## Open Issues

### IN THIS SECTION

- [General Routing | 125](#)
- [User Interface and Configuration | 126](#)

Learn about open issues in Junos OS Release 21.4R1 for PTX Series routers.

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

## General Routing

- On the PTX Platform with FPC-PTX-P1-A or FPC2-PTX-P1A, you might encounter a single event upset (SEU) event that might cause a linked-list corruption of the TQCHIP. The following syslog message gets reported: Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt\_min\_free\_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Junos OS chassis management error handling does detect such condition, and raises an alarm and performs the disable-pfe action for the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, a restart



of the FPC is needed. Contact your Juniper support representative if the issue persists even after the FPC restarts. [PR1254415](#)

- On the PTX Series platform using indirect next hop (such as Unilist) as route next hop type for multiple paths scenario (such as BGP PIC or ECMP), the fast reroute session might be enabled in Packet Forwarding Engines. When the version-id or session-id of the indirect next hop is above 256, the Packet Forwarding Engine might not respond to session update, which might cause the session-id to be stuck permanently with the weight of 65535 in the Packet Forwarding Engine. This might lead the Packet Forwarding Engine to have a different view of Unilist against load-balance selectors. Then, either the BGP PIC or the ECMP-FRR might not work properly and traffic might be dropped or silently discarded. [PR1501817](#)
- Flapping might be observed on channelized ports of PTX Series routers during ZTP, when one of the port is disabled on the supporting device. [PR1534614](#)
- A vulnerability in the handling of exceptional conditions in Juniper Networks Junos OS Evolved allows an attacker to send specially crafted packets to the device, causing the Advanced Forwarding Toolkit manager (evo-aftmand-bt or evo-aftmand-zx) process to crash and restart, impacting all traffic going through the FPC, resulting in a Denial of Service (DoS). Please refer to <https://kb.juniper.net/JSA11188> for more information. [PR1572969](#)
- On PTX10000 platforms running Junos OS, file permissions might be changed for `/var/db/scripts` files after rebooting the device. This issue might have an impact on the scripts running on the box. [PR1583839](#)
- On all PTX platforms, when a Provider Edge (PE) router is configured with multipath, traffic loss might be seen even though the link is up. After the fix, `no-ifl-based-frr-for-inh-primary` can be applied under routing-option to evade such issue. [PR1618507](#)

## User Interface and Configuration

- When a user tries to deactivate the MPLS related configuration, the commit fails on backup Routing Engine. Work-around details are provided in the corresponding section below. [PR1519367](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1 | 127](#)

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

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

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [General Routing | 127](#)
- [Interfaces and Chassis | 129](#)
- [Layer 2 Ethernet Services | 129](#)
- [MPLS | 129](#)
- [Network Management and Monitoring | 129](#)
- [Routing Policy and Firewall Filters | 129](#)
- [User Interface and Configuration | 129](#)

## General Routing

- Routing Engine switchover does not work as expected while solid-state drive (SSD) failure occurs. [PR1437745](#)
- The device might run out of service post GRES or unified ISSU. [PR1558958](#)
- Upgrading PTX1000 platforms with unified SSDs (2x32G SSD) might result in boot loop in certain scenario. [PR1571275](#)
- Mirrored packets get corrupted when a filter is applied with the port-mirror and discard action. [PR1576914](#)

- File permissions are changed for `/var/db/scripts` files after reboot on PTX platforms. [PR1583839](#)
- High FPC CPU utilization might be seen on PTX10002-60C platform. [PR1585728](#)
- The `RPD_KRT_KERNEL_BAD_ROUTE` error message is seen in certain scenarios when the `rpd` process restarts or GRES happens when NSR is enabled. This error has no functional impact. [PR1586466](#)
- PTX1000 RCB FIPS 140-2 Level 1 - certification support. [PR1590640](#)
- The `I2cpd` agent might become unresponsive after starting the telemetry service. [PR1592473](#)
- Layer 2 VPN stops forwarding when interface encapsulation is changed to `vlan-ccc` from `ethernet-ccc` and back. [PR1595455](#)
- [MPC10E] messages log will be filled with **Temp Sensor Fail** alarm set/clear and **cmtfpc\_cpu\_core\_temp\_get: Fail to get temp CPU7\_PMB** messages. [PR1597798](#)
- On PTX10001-36MR platforms, inconsistency in the platform name used in multiple places, version, `snmp mibs`, etc. [PR1597999](#)
- On PTX1000 platforms, sFlow data (for example: inner VLAN and outer VLAN value, forwarding-class, and DSCP value) is not exported while checking from server flow records at the collector for ingress sampling. [PR1598263](#)
- False fan failure alarm flaps (set and cleared) frequently. [PR1599183](#)
- CRC errors increase continuously after interface flap. [PR1600768](#)
- Traffic might get silently dropped and discarded due to the RS Fatal error on FPC-PTX-P1-A, FPC2-PTX-P1A, FPC-SFF-PTX-P1-A, and FPC-SFF-PTX-T. [PR1600935](#)
- The `I2circuit` packets with PVST and RPVST destination multicast MAC might get dropped. [PR1601360](#)
- `OutputInt=0` in JFLOW data reported to collector. [PR1601531](#)
- The IPv6 traffic might get impacted on the PTX platforms when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)
- Junos OS, PTX10002-60C System: After upgrading, configured firewall filters might be applied on incorrect interfaces (CVE-2021-31382). [PR1602292](#)
- Packet loss might be seen on filter-based GRE deployments. [PR1603453](#)
- Link flaps might be observed momentarily on PTX5000 platforms. [PR1606008](#)
- Memory leaks might be observed on the `I2cpd` process when you perform certain LLDP operations. [PR1608699](#)

- Line-cards might be unstable due to the continuous growing memory usage of evo-cda-bt app. [PR1614952](#)
- VCCV for LDP signaled pseudowire goes down periodically on PTX10008 and PTX10004 with Junos OS. [PR1615419](#)
- While migration from Junos OS to Junos OS Evolved, customer have to delete chassis redundancy failover or set chassis redundancy failover **disable**. [PR1617720](#)

## Interfaces and Chassis

- Junos telemetry interface optics sensor's alarm data type changed from **bool\_val** to **str\_val**. [PR1580113](#)

## Layer 2 Ethernet Services

- Uneven traffic distribution might be observed between member links of LAG. [PR1599029](#)

## MPLS

- The LDP replication session might not get synchronized when the dual-transport is enabled. [PR1598174](#)
- VPLS connection might get down if the dual-transport statement is configured. [PR1601854](#)

## Network Management and Monitoring

- On PTX10008 platforms, syslog does not log information on IPv4 after upgrade. [PR1611504](#)

## Routing Policy and Firewall Filters

- BGP route preference using PBR is not applied to all the routes when CCNH inet6 is enabled. [PR1596436](#)

## User Interface and Configuration

- The commitd core file might be observed after committing some configuration change. [PR1601159](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for PTX Series routers.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Basic Procedure for Upgrading to Release 21.4 | 130](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 133](#)
- [Upgrading a Router with Redundant Routing Engines | 133](#)

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

## Basic Procedure for Upgrading to Release 21.4

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

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

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

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

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

To download and install Junos OS Release 21.4R1:

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

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

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

```
user@host> request system software add validate reboot source/junos-install-ptx-  
x86-64-21.4R1.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-  
x86-64-21.4R1.9-limited.tgz
```

Replace the source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

**NOTE:** You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the request vmhost software add command. For more information, see the VM Host Installation topic in the [Installation and Upgrade Guide](#).

**NOTE:** After you install a Junos OS Release 21.4 jinstall package, you cannot return to the previously installed software by issuing the `request system software rollback` command. Instead, you must issue the `request system software add validate` command and specify the jinstall package that corresponds to the previously installed software.

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

## Upgrade and Downgrade Support Policy for Junos OS Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

## Upgrading a Router with Redundant Routing Engines

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



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

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

## Junos OS Release Notes for QFX Series

### IN THIS SECTION

- [What's New | 135](#)
- [What's Changed | 143](#)
- [Known Limitations | 145](#)
- [Open Issues | 146](#)
- [Resolved Issues | 149](#)
- [Documentation Updates | 155](#)
- [Migration, Upgrade, and Downgrade Instructions | 155](#)

These release notes accompany Junos OS Release 21.4R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [EVPN | 135](#)
- [High Availability | 137](#)
- [Juniper Extension Toolkit \(JET\) | 137](#)
- [Junos Telemetry Interface \(JTI\) | 137](#)
- [Licensing | 138](#)
- [MPLS | 138](#)
- [Network Management and Monitoring | 138](#)
- [Operation, Administration, and Maintenance \(OAM\) | 139](#)
- [Routing Policy and Firewall Filters | 139](#)
- [Routing Protocols | 140](#)
- [Services Applications | 142](#)
- [Additional Features | 142](#)

Learn about new features introduced in the Junos OS main and maintenance releases for QFX Series switches.

### EVPN

- **EVPN-VXLAN fabric with an IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure an 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, configure the underlay VXLAN tunnel endpoint (VTEP) source interface in the MAC-VRF instance as an IPv6 address. However, you must use the IPv4 loopback address as the router ID for BGP handshaking to work.

This feature was introduced in Junos OS Release 21.2R2.

[See [EVPN-VXLAN with an IPv6 Underlay](#) and [Understanding EVPN with VXLAN Data Plane Encapsulation](#).]

- **DHCP relay in an EVPN-VXLAN fabric with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, EVPN-VXLAN fabrics with an IPv6 underlay support DHCP relay. You can configure the DHCP relay agent in centrally routed and edge-routed bridging overlays. Support for DHCP relay includes support for DHCPv4 and DHCPv6. This feature was introduced in Junos OS Release 21.2R2.

[See [DHCP Relay Agent over EVPN-VXLAN](#).]

- **CoS support for EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.4R1, you can configure CoS features, which enable you to prioritize traffic, on an EVPN-VXLAN fabric with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

[See [CoS Support on EVPN VXLANs](#).]

- **Support for firewall filters on EVPN-VXLAN with IPv6 underlay (QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-24YM, and QFX5120-48YM)**—Starting in Junos OS Release 21.4R1, QFX5120 switches support firewall filters for ingress and egress traffic on EVPN-VXLAN with an IPv6 underlay. This feature was introduced in Junos OS Release 21.2R2.

[See [Understanding EVPN with VXLAN Data Plane Encapsulation](#).]

- **Support for EVPN-VXLAN group-based policies (QFX5120-48Y, QFX5120-48YM, QFX5120-48T, and QFX5120-32C)**—Starting in Junos OS Release 21.4R1, QFX5120 switches provide standards-based multilevel segmentation (also called group-based policy, or GBP) on the basis of Layer 3 virtual networks and group-based tags rather than IP-based filters. GBP supports an application-centric policy model that separates network access policies from the underlying network topology through the use of policy tags, thus allowing different levels of access control for endpoints and applications even within the same VLAN.

The QFX5120 switches also provide GBP support for locally switched traffic on VXLAN access ports.

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

- **Symmetric integrated routing and bridging (IRB) with EVPN Type 2 routes (QFX5210)**—Starting in Junos OS Release 21.4R1, you can enable symmetric IRB EVPN Type 2 routing on QFX5210 switches in an EVPN-VXLAN ERB overlay fabric. With the symmetric routing model, leaf devices can route and bridge traffic on both ingress and egress sides of a VXLAN tunnel. To do this, the leaf devices use a special transit VXLAN network identifier (VNI) and Layer 3 interfaces on the associated VLAN to exchange traffic across the VXLAN tunnels.

We support this feature with:

- EVPN instances configured using MAC-VRF routing instances.
- VLAN-aware bundle or VLAN-based Ethernet service types.

- EVPN Type 5 routing using Layer 3 virtual routing and forwarding (VRF) instances with IRB interfaces for intersubnet reachability.

This feature was introduced in Junos OS Release 21.3R1-S1.

[See [Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network.](#)]

## High Availability

- **Unified ISSU support on QFX5120-48Y**—Starting in Junos OS Release 21.4R1, QFX5120-48Y switches support unified in-service software upgrade (ISSU). The unified ISSU feature enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic.

Use the `request system software in-service-upgrade package-name.tgz` command to use unified ISSU. Use the `request system software validate in-service-upgrade package-name.tgz` command to verify that your device and target release are compatible.

**NOTE:** QFX5120-48Y switches provide unified ISSU support only if the Cancun versions of the chipset SDK are the same for the current version and the version you are upgrading to. See, "[High Availability](#)" on page 146.

[See [Getting Started with Unified In-Service Software Upgrade](#) and [Understanding In-Service Software Upgrade \(ISSU\)](#).]

## Juniper Extension Toolkit (JET)

- **Support for programming FTIs using JET APIs (PTX1000, PTX10002, PTX10008, PTX10016, QFX5100, and QFX10008)**—Starting in Junos OS Release 21.4R1, you can use the Interfaces Service API to configure flexible tunnel interfaces (FTIs) in Junos OS. You can change the attributes of the tunnel configurations for the unit under an existing FTI but cannot change the existing tunnel encapsulation type using the APIs. For the following families, you can configure only the listed attributes when you use JET APIs:
  - `inet` and `inet6`: address and destination-udp-port
  - `mpls` and `iso`: destination-udp-port

[See [Overview of JET APIs](#) and [Configure Flexible Tunnel Interfaces](#).]

## Junos Telemetry Interface (JTI)

- **Packet Forwarding Engine performance sensors (EX4650, QFX5110, QFX5120-48Y, QFX5200, and QFX5210)**—Starting in Junos OS Release 21.4R1, JTI streams NPU utilization statistics by means of

remote procedure calls (gRPC), gRPC network management interface (gNMI), or UDP (native) transport from a device to an outside collector.

[See [sensor \(Junos Telemetry Interface\)](#), [Guidelines for gRPC and gNMI Sensors \(Junos Telemetry Interface\)](#), and [Telemetry Sensor Explorer](#).]

## Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:
  - `set system license autoupdate url <link>`
  - `set system license renew before-expiration <days>`
  - `set system license renew interval <hours>`

The license autoupdate and license renew commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

[See [License Autoupdate and License Renew](#).]

## MPLS

- **Support for optimizing auto-bandwidth adjustments for MPLS LSPs (QFX10008)**—Starting in Junos OS Release 21.4R1, you can configure faster auto-bandwidth adjustment for MPLS LSPs under overflow or underflow conditions. This feature decreases the minimum allowed value of `adjust-threshold-overflow-limit` and `adjust-interval` to 150 seconds when `adjust-threshold-overflow-limit` and `adjust-threshold-underflow-limit` cross the configured threshold values. In releases before Junos OS Release 21.4R1, the `adjust-interval` value is 300 seconds under overflow or underflow conditions.

You can configure a faster in-place LSP bandwidth update that avoids signaling of a new LSP instance as part of make-before-break. To configure, include the `in-place-lsp-bandwidth-update` configuration statement at the `[edit protocols mpls label-switched-path lsp-name]` hierarchy level.

You can also configure RSVP interfaces to support subscription percentage per priority. To configure, include the `subscription priority priority percent` value configuration statement at the `[edit protocols rsvp interface interface-name]` hierarchy level.

[See [Configuring Optimized Auto-bandwidth Adjustments for MPLS LSPs](#).]

## Network Management and Monitoring

- **Remote port mirroring to IPv6 address (EX4650, EX4650-48Y-VC, QFX5120-32C, QFX5120-48T, QFX5120-48T-VC, QFX5120-48Y, QFX5120-48Y-VC, and QFX5120-48YM)**—Starting in Junos OS

Evolved Release 21.4R1, you can use remote port mirroring to copy packets entering or exiting a port or entering a VLAN and send the copies to the IPv6 address of a device running an analyzer application on a remote network (sometimes referred to as *extended port mirroring*). When you use remote port mirroring to an IPv6 address, the mirrored packets are GRE-encapsulated.

Add the address you would like to have the copied packets sent to in the CLI hierarchy. For example, set forwarding-options analyzer ff output ip-address 2000::1.

[See [Understanding Port Mirroring and Analyzers](#).]

- **Support for port mirroring and analyzers with Layer 3 VXLAN gateway (QFX5210)**—Starting in Junos OS Release 21.4R1, the QFX5210 supports port mirroring when used as a Layer 3 VXLAN gateway. However, the QFX5210 does not support true egress mirroring. Packet contents are different when you configure egress mirroring on the network port. Layer 2 fields in the mirrored packets are undefined, and you should not consider those fields for validation.

[See [Port Mirroring and Analyzers](#) and [Using a RIOT Loopback Port to Route Traffic in an EVPN-VXLAN Network](#).]

## Operation, Administration, and Maintenance (OAM)

- **Enhancements to BFD-triggered FRR for unicast next hops and forwarding-table session-id-change-limiter-indirect to address issue of traffic being silently discarded (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)**—In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and forwarding-table session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

To align the traffic by creating session-id-change-limiter indirect next hop, set the set routing-options forwarding-table session-id-change-limiter-indirect configuration statement at the [edit routing-options forwarding-table] hierarchy level.

[See [Bidirectional Forwarding Detection \(BFD\) for MPLS](#).]

## Routing Policy and Firewall Filters

- **Support for IPv4 and IPv6 firewall filters on Layer 3 gateways in EVPN-VXLAN fabrics (QFX5210)**—Starting in Junos OS Release 21.4R1, QFX5210 switches acting as Layer 3 gateways in EVPN-VXLAN fabrics support IPv4 and IPv6 firewall filters in the ingress direction of the IRB interface. We recommend that you do not apply filters on the RIOT loopback interface. The switch supports the following match conditions:
  - source-address
  - destination-address

- source-port
- destination-port
- ttl
- ip-protocol
- hop-limit

The supported actions are:

- accept
- discard
- log
- syslog
- policer

The QFX5210 does not support filter-based forwarding (FBF).

[See [Firewall Filter Match Conditions and Actions \(QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX5700, EX4600, EX4650\)](#).]

- **Support for source-port and destination-port range optimize conditions to reduce the TCAM space—** Starting in Junos OS Release 21.4R1, we support the source-port-range-optimize and the destination-port-range-optimize conditions at the [edit firewall family ethernet-switching filter <filter-name> term <term-name> from] hierarchy level. This configuration considerably reduces the ternary content addressable memory (TCAM) space usage. QFX5100 switches support up to 24 non-contiguous matching conditions for the source-port-range-optimize and destination-port-range-optimize options.

[See [Firewall Filter Match Conditions and Actions \(QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX5700, EX4600, EX4650\)](#).]

## Routing Protocols

- **Higher DDoS bandwidth for Layer 2 and Layer 3 protocols (PTX1000, PTX10002, PTX10008, QFX10002, QFX10002-60C, and QFX10008)**—Starting in Junos OS Release 21.4R1, we support higher distributed denial-of-service (DDoS) bandwidth for the following Layer 2 and Layer 3 protocols:
  - Layer 3 protocols— RSVP, LDP, OSPF, BGP, BFD, PIM, IGMP, and ICMP
  - Layer 2 protocol — IS-IS

[See [protocols \(DDoS\) \(ACX Series, PTX Series, and QFX Series\)](#).]

- **Remote LFA support for LDP in IS-IS (QFX10000 line of switches)** —Starting in Junos OS Release 21.4R1, you can configure a remote loop-free alternate (LFA) path to extend the backup provided by the LFA route in an IS-IS or OSPF network. This feature is especially useful for Layer 1 metro rings where the remote LFA is not directly connected to the point of local repair (PLR). You can reuse the existing LDP implementation for the MPLS tunnel setup for the protection of IS-IS and OSPF networks and subsequent LDP destinations. By doing this, you eliminate the need for RSVP-TE backup tunnels for backup coverage.

[See [Understanding Remote LFA over LDP Tunnels in IS-IS Networks](#) and [Remote LFA over LDP Tunnels in OSPF Networks Overview](#).]

- **OSPF link delay measurement and advertising (ACX Series, MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.4R1, you can measure and advertise various performance metrics in IP networks with scalability through probe messages that are sent by the Two-Way Active Measurement Protocol (TWAMP) Light. OSPF receives probe messages and the measured values from TWAMP Light. OSPF advertises these messages as TLVs in packets. You can use these metrics to make path-selection decisions based on the network performance.

[See [How to Enable Link Delay Measurement and Advertising in OSPF](#).]

- **Support for multiple update threads to service a peer group (MX Series, PTX Series, and QFX Series)** —Starting in Junos OS Release 21.4R1, you can configure multiple update threads to service a peer group to improve the performance of BGP. You can use the group-split-size configuration statement at the [edit system processes routing bgp update-threading] hierarchy level and configure a threshold value (0 through 2000).

[See [update-threading](#).]

- **Support for ICMP extension (QFX5100)**—Starting in Junos OS Release 21.4R1, we've implemented RFC 5837, *Extending ICMP for Interface and Next-Hop Identification*, for both numbered and unnumbered aggregated Ethernet interfaces. We can now append additional fields to the following ICMP (IPv4 and IPv6) messages:

- ICMPv4 Time Exceeded
- ICMPv4 Destination Unreachable
- ICMPv6 Time Exceeded
- ICMPv6 Destination Unreachable

Use the set system allow-icmp4-extension command to enable ICMP extension.

[See [Configure ICMP Features](#).]



## Services Applications

- **Inband Flow Analyzer (IFA) 2.0 (QFX5120-48Y and QFX5120-32C)**—In Junos OS Release 21.4R1, we've introduced support for IFA 2.0 on QFX Series switches. IFA 2.0 monitors and analyzes packets entering and exiting the network. You can use IFA 2.0 to monitor the network for faults and performance issues. IFA 2.0 supports both Layer 3 and VXLAN flows.

With IFA 2.0, you can collect various flow-specific information from the data plane, without the involvement of the control plane or the host CPU. IFA collects data on a per-hop basis across the network. You can export this data to external collectors to perform localized or end-to-end analytics.

IFA 2.0 contains three different processing nodes:

- IFA initiator node
- IFA transit node
- IFA terminating node

[See [Inband Flow Analyzer \(IFA\) 2.0 Probe for Real-Time Performance Monitoring](#), [inband-flow-telemetry](#), [show services inband-flow-telemetry](#), and [clear inband-flow-telemetry stats](#).]

## Additional Features

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

- **Supported transceivers, optical interfaces, and DAC cables** (ACX Series, EX Series, PTX Series, MX Series, and QFX Series).—Select your product in the [Hardware Compatibility Tool](#) to view supported transceivers, optical interfaces, and DAC cables for your platform or interface module. We update the HCT and provide the first supported release information when the optic becomes available.
- **EVPN-VXLAN support** (QFX5120-48YM):
  - EVPN-VXLAN with MAC-VRF routing instances
  - Filter-based forwarding in EVPN-VXLAN
  - IPv6 data traffic support through an EVPN-VXLAN overlay network
  - IPv6 support for firewall filtering and policing on EVPN-VXLAN traffic
  - Port mirroring and analyzers on EVPN-VXLAN
  - Storm control on EVPN-VXLAN

[See [EVPN User Guide](#).]

- **EVPN Type 2 and Type 5 route coexistence** (EX9200, EX9251, EX9253, MX204, MX240, MX480, MX960, MX2010, MX10003, MX10008, and QFX10002-60C)

[See [EVPN Type 2 and Type 5 Route Coexistence with EVPN-VXLAN](#).]

- **MACsec bounded delay protection** (EX4400 and SRX380)

[See [bounded-delay](#).]

- **MACsec timer-based SAK refresh** (QFX5120-48YM)

[See [sak-rekey-interval](#).]

- **Storm control in an EVPN-VXLAN fabric with Layer 3 gateway** (QFX5210)

**NOTE:** We recommend that you do not configure storm control on the aggregated Ethernet interface used as the loopback port to support RIOT functionality.

[See [Understanding Storm Control](#).]

- **Support for Precision Time Protocol (PTP) G.8275.2 enhanced profile with PTP over IPv4 and IPv6 unicast traffic** (QFX5120-48T)

[See [G.8275.2 Enhanced Profile](#).]

- **Support for sFlow with EVPN-VXLAN Layer 3 gateway** (QFX5210)

[See [sFlow Monitoring Technology](#) and [Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 144

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

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [EVPN | 144](#)
- [Network Management and Monitoring | 144](#)

## EVPN

- **Community information no longer included in VRF routing table**—The QFX series switches will no longer include the inherited advertised route target communities, EVPN extended communities, or vxlan encapsulation communities for EVPN Type 2 and EVPN Type 5 routes when an IP host is added in the VRF routing table.
- **Output for the show Ethernet switching flood extensive command**—The output for the show ethernet-switching flood extensive command now displays the correct next-hop type for Virtual Ethernet and WAN mesh group in an EVPN-VXLAN network as unilist. Previously, the output for the show ethernet-switching flood extensive command would misidentify the next-hop type as composite.

## Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 145
- [Infrastructure](#) | 146
- [High Availability](#) | 146

Learn about known limitations in Junos OS Release 21.4R1 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 the QFX5000 line of switches with storm control, there is a significant difference between the configured rate and the actual rate. [PR1526906](#)
- On the QFX5200 and QFX5100 line of switches, double-count packets gets forwarded over IP-IP tunnel that are egress-sampled. [PR1555922](#)
- Unexpected multicast traffic streams after enabling EVPN. [PR1570689](#)
- On the QFX5000 line of switches, the IRACL filters do not match the VXLAN tunnel terminated packets. [PR1594319](#)
- The 1pps performance test fails on the copper ports. [PR1618533](#)
- Junos OS does not support the unified ISSU on QFX5120-48Y line of switches if there is a change in the Cancun versions of the chipset SDKs between the releases. A change in the Cancun firmware

leads to the chip reset impacting ISSU. The Cancun versions in the chipset SDKs must be the same between two Junos OS releases for ISSU to work. [PR1634695](#)

## Infrastructure

- Software image upgrade from Junos OS Release 21.1 (or earlier) to Junos OS Release 21.2 (or later) requires `no-validate` command as a mandatory action. [PR1586481](#)

## High Availability

- Starting in Junos OS Release 21.4R1, QFX5120-48Y switches support unified in-service software upgrade (ISSU). However, QFX5120-48Y switches provide unified ISSU support only if the Cancun versions in the chipset SDK are the same in the current version and the version you are upgrading to. [PR1634695](#)

## Open Issues

### IN THIS SECTION

- [EVPN | 147](#)
- [General Routing | 147](#)
- [Interfaces and Chassis | 148](#)
- [Layer 2 Features | 149](#)
- [Platform and Infrastructure | 149](#)
- [Routing Protocols | 149](#)

Learn about open issues in Junos OS Release 21.4R1 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

- With the shared-tunnels enabled, the AR tunnels do not get formed on the DC GWs for the MAC-VRF instances. [PR1584790](#)
- Need to modify I-ESI workflow on DC-GW. [PR1600600](#)
- Few ARP/ND/MAC entries for VLANs gets missed with the MAC-VRF configuration. [PR1609322](#)
- MAC-IP that moves across Layer 2 DCI does not get updated in the MAC-IP table of the GW nodes for VLANs that have translate VNI configuration. [PR1610432](#)

## General Routing

- On the QFX10000 line of switches, the `show pfe filter hw filter-name` command does not retrieve the Packet Forwarding Engine program. [PR1495712](#)
- On the QFX5100 line of switches that does not run the QFX-5E codes (non TVP architecture), when you install image with Broadcom SDK upgrade (6.5.X), the CPU utilization might go up by around 5 percent. [PR1534234](#)
- On the QFX5000 line of switches, route leaking does not work for IPv4 routes if the mask is less than 16 and for IPV6 routes if the mask is less than 64. [PR1538853](#)
- FPC might not be recognized after power cycle (hard reboot). [PR1540107](#)
- On the QFX10002-60c line of switches, NP-100G-DAC-3M/5M does not start on QFX10002-60C switches. [PR1555955](#)
- On the QFX10002-60c line of switches, after DUT or remote 100G DAC interfaces flaps, the carrier transition counters increases unexpectedly. [PR1562857](#)
- The OSPF session over IRB might not come up in the EVPN-VXLAN scenario. [PR1577183](#)
- Partial traffic loss occurs after disabling the protected link on R2 due to which convergence delay for link-protection for PE1\_P link occurs. [PR1579931](#)
- On the QFX5100 Virtual Chassis, the DHCP ACK messages do not get generated while verifying Smart Relay with interfaces in the routing instance. [PR1581025](#)
- When you commit soft loopback port and analyzer configurations, mirror ingress to local port does not work. [PR1581542](#)

- On the QFX10002-60C line of switches, complete packet gets lost while testing the VACL ingress terms scale configuration. [PR1581767](#)
- After reboot, the file permissions gets changed for the `/var/db/scripts` files. [PR1583839](#)
- On the QFX5000 line of switches, the dcpfe process might crash. [PR1588704](#)
- The IS-IS adjacency might fail to be formed if you configure the MTU size of an IRB interface with a value great than 1496 bytes. [PR1595823](#)
- On the QFX10008 line of switches, the Routing Engine1 goes to the database prompt when loading the profile configurations over LRM configurations. [PR1598814](#)
- On the QFX5200 line of switches, the dcpfe process generates core files while testing ISSU from Junos OS Release 21.1R1.11 to Junos OS Release 21.2R1.7. [PR1600807](#)
- On the QFX10002 line of switches, the IGP convergence time gets degraded. [PR1602334](#)
- On the QFX5120 line of switches, traffic loss occurs when the primary link gets disabled with the aggregated Ethernet interface Link Protection configuration. [PR1604350](#)
- On the QFX10002-72q line of switches, the sFlow samples do not get generated for the transit MPLS traffic carrying IPv6. [PR1607497](#)
- On the QFX10002-60C line of switches, the output-mac-control-frames and output-mac-pause-frames counters do not increase. [PR1610745](#)
- On the QFX5100 Virtual Chassis, traffic loss occurs while testing the 118 AE groups. [PR1611162](#)
- On the QFX10002, QFX10008, and QFX10016 line on switches, on scaling more than 80,000 ARP/NDP, the `prds_jpf_nh_token_change: Token change failed for rnh` error messages gets generated. [PR1616224](#)
- On the QFX5120 line on switches, the `tv_p_is_qsfp_has_single_led ioctl call failed ret:-1` error message gets generated while loading the build. [PR1621630](#)
- When the IFA2.0 init feature enabled on switch and flows are sampled, incorrect pps and bps statistics gets displayed at the logical child interface level on the ingress and egress ports. [PR1620139](#)

## Interfaces and Chassis

- On the QFX5120 line of switches, multiple `mclag-cfgchkd` process generates core files after loading the recent Junos OS Release 20.4R2-S1 build. [PR1599025](#)

## Layer 2 Features

- Adding one more sub-interface logical interface to an existing interface causes 20 to 50 milliseconds traffic drop on the existing logical interface. [PR1367488](#)

## Platform and Infrastructure

- The offer message from the server reaches the relay agent. However, the offer message does not get forwarded to IRBs on which clients are connected. [PR1530160](#)

## Routing Protocols

- When you remove igmp-snooping from the device, the device might encounter inconsistency in the mcsnoopd process. [PR1569436](#)
- The mcsnoopd process might generate core files at `rt_mcnh_nh_add_del`, `rt_mcnh_nh_add_with_table_id`, `mc_build_nh_for_bd_evpn_extended`, `mc_bd_create_or_update_all_fld_grp_routes`. [PR1605393](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1 | 150](#)

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.



## Resolved Issues: 21.4R1

### IN THIS SECTION

- [Class of Service \(CoS\) | 150](#)
- [EVPN | 150](#)
- [General Routing | 150](#)
- [Infrastructure | 154](#)
- [MPLS | 154](#)
- [Layer 2 Ethernet Services | 154](#)
- [Routing Protocols | 154](#)

### Class of Service (CoS)

- The TCP-ECN traffic might not be forwarded with high priority. [PR1585854](#)

### EVPN

- Traffic loss might occur under the EVPN scenario when MAC-IP moves from one CE interface to another. [PR1591264](#)
- The device announces router-MAC, target, and EVPN VXLAN community to the BGP IPv4 NLRI. [PR1600653](#)
- Traffic sent by the QFX5000 leaf to remote leaf with link goes into the Down state. [PR1605375](#)
- The MAC-table aging timeout fails in some scenarios. [PR1612866](#)

### General Routing

- Routing Engine switchover does not work as expected when SSD fails. [PR1437745](#)
- Unexpected next-hop might occur after the route gets deleted. [PR1477603](#)
- The interface might go into the Blocking state impacting the traffic when the link-protection switches from primary to backup. [PR1555294](#)
- On the QFX5100 line of switches, the Virtual Chassis Port (VCP) might not come up after upgrading to Junos OS Release 18.4R2-S4 or later. [PR1555741](#)

- On the QFX5110 line of switches, the untagged traffic routed over native-vlan might be dropped. [PR1560038](#)
- The na-grpcd process might generate core files during the longevity tests. [PR1565255](#)
- The MAC address points to an incorrect interface after traffic stops and not ages out. [PR1565624](#)
- On the QFX10000 line of switches, the dcpfe and fpc process might crash if the ARP MAC moves. [PR1572876](#)
- On the QFX10K2-60C line of switches, the disk missing alarm does not get generated. [PR1573139](#)
- On QFX Series switches, when a VRF instance configuration exists and you upgrade to Junos OS Release 20.3 or later and commit the upgrade might generate the warning: requires 'l3vpn' license" warning message. [PR1575608](#)
- On the QFX10000 line of switches, the port might not be brought down immediately during some abnormal type of line card reboot. [PR1577315](#)
- On QFX5000 line of switches, the show route detail command might not display the Next-hop type IPoIP Chained comp nexthop in the output. [PR1584322](#)
- ARP resolution for data traffic received over Type5 might fail. [PR1612905](#)
- The l2cpd process generates a core file with the FIP snooping configuration on any interface. [PR1617632](#)
- Junos OS does not support the Dot1x based firewall policers. [PR1619405](#)
- On the QFX5100 line of switches, some 40G ports might not be channelized successfully. [PR1582105](#)
- On the QFX5000 line of switches, the firewall filter does not get programmed after you delete a large filter and add a new one in a single commit. [PR1583440](#)
- File permissions changes for the **/var/db/scripts** files after a reboot. [PR1583839](#)
- On the QFX10002-60C line of switches, high FPC CPU utilization might occur. [PR1585728](#)
- On the QFX5210-64C line of switches, the PSU firmware upgrades through Junos OS. [PR1589572](#)
- On the QFX5120 line of switches, the MPLS traffic might not be forwarded after the aggregate interface flaps. [PR1589840](#)
- The Virtual Chassis mastership changes and the connection drops after renumbering the backup member ID. [PR1590358](#)
- On the QFX5120-48T line of switches after removing 1G speed on interfaces, the interface does not come back as 10G. [PR1591038](#)

- Routing Engine kernel might crash due to logical interface of the aggregated interface, adding failure in the Junos OS kernel. [PR1592456](#)
- The IPv4 fragmented packets might be broken if you configure PTP transparent clock. [PR1592463](#)
- The BFD session might flap during the Routing Engine switchover. [PR1593244](#)
- The dcpfe process might crash in the EVPN-VXLAN scenario. [PR1593950](#)
- Packet might drop in the ECMP next-hop flap scenario. [PR1594030](#)
- ARP entry might be missed intermittently after FPC reboots. [PR1594255](#)
- The label field for the EVPN Type-1 route gets set to 1. [PR1594981](#)
- The re-installation of the Type-5 tunnels might fail in the EVPN-VXLAN scenario. [PR1595197](#)
- The DCI InterVNI and IntraVNI traffic might be silently discarded in the gateway node due to the tagged underlay interfaces. [PR1596462](#)
- The mscnoopd process might crash when you delete or add the Layer 2 forwarding configuration after ISSU. [PR1596483](#)
- The fpc0 bcm pkt reinsert failed log gets generates in the log messages in an aggressive way. [PR1596643](#)
- Traffic might be dropped after the backup FPC reboots in a Virtual Chassis scenario. [PR1596773](#)
- The interface might not be brought up when you configure QinQ. [PR1597261](#)
- Deletion of MACsec configuration on an logical interface does not work. [PR1597848](#)
- The socket connection drops as the keepalive timer expires with port 33015. [PR1598019](#)
- On the QFX5000 line of switches, sFlow impacts on ICMP traffic. [PR1598239](#)
- On the OFX5100, QFX5110, QFX5120, QFX5200, and QFX5210 line of switches, the DDoS violations might be reported for the IP multicast miss traffic (IPMCAST-MISS) incorrectly. [PR1598678](#)
- File permissions changes for the **/var/db/scripts** files after reboot. [PR1599365](#)
- On the QFX10002-60C line of switches, the Layer 3 traffic silently gets discarded with the IRB interface. [PR1599692](#)
- Not able to disable the management port em1. [PR1600905](#)
- On QFX5120-48y-8c line of switches, the dcpfe process generates core file while issuing the show pfe vxlan nh-usage command in the ERB EMC scenario with around 6000 ARP entries. [PR1601949](#)

- InterDC traffic loss might occur in the MAC-VRF EVI with the `dlu.ucode.discard` trap status. [PR1601961](#)
- The IPv6 traffic might be impacted when an IPv6 route resolves over a dynamic tunnel. [PR1602007](#)
- Under certain scaling scenarios with EVPN-VXLAN configurations, the `l2ald` process might be aborted and then recovered. [PR1602244](#)
- The egress interface of the GRE tunnel does not dynamically get updated when the destination to tunnel changes. [PR1602391](#)
- FPC goes into the `Down` state and the `dcpcfe` process might generate core file in some cases. [PR1602583](#)
- Traffic loss might occur in the MC-LAG scenario. [PR1602811](#)
- On the QFX5000 line of switches, traffic might be dropped in the Virtual Chassis scenario when you configure the firewall filter. [PR1602914](#)
- On the QFX5120 line of switches, traffic gets mirrored even after deactivating the analyzer configuration. [PR1603192](#)
- Unicast DHCP packets might get flooded when you configure the DHCP relay in the non-default routing-instance. [PR1603444](#)
- Packet loss might occur on the filter-based GRE deployments. [PR1603453](#)
- Duplicate packets might appear when you bring up all the interfaces on the spine switch. [PR1604393](#)
- The carrier transition counter might not get incremented upon link flap after the reboot. [PR1605037](#)
- MAC might move between the ICL and MC-LAG interface if you add or remove VLANs on the ICL interface. [PR1605234](#)
- Multicast streams might stop flooding in the VXLAN setup. [PR1606256](#)
- The Virtual Chassis ports might remain in the `Down` state after you remove and add the ports. [PR1606705](#)
- The LLDP packets received on VXLAN-enabled port might be flooded unexpectedly. [PR1607249](#)
- The `fxpc` process might crash and generate a core file. [PR1607372](#)
- Ping to `lo0`/IRB over Type-5 fails. [PR1610093](#)
- On the QFX10000 line of switches, continuous Layer 3 traffic might drop with the MC-LAG configuration. [PR1610173](#)
- The QFX Virtual Chassis might lose license on Junos OS Release 21.2R1. [PR1610272](#)

- On the QFX10002-60C line of switches, continuous FPC might crash and the dcpfe process might generate core file. [PR1612871](#)
- On the QFX5000 line of switches, the VLAN firewall filter does not get deleted in the Packet Forwarding Engine after configuration changes. [PR1614767](#)
- The l2ald process might crash in the EVPN scenario. [PR1615269](#)
- The BFD session might get become nonresponsive in the Init state after l2-learning restart due to incomplete ARP resolutions. [PR1618280](#)
- Disabled VCP (Virtual chassis port) might go into the Up state after the optic is reseated. [PR1619997](#)
- Traffic might be lost after configuring VXLAN over the IRB interface. [PR1625285](#)
- Need to implement the `show task scheduler-slip-history` command to display the number of the scheduler slips and the last 64 slip details. [PR1626148](#)

## Infrastructure

- The Host 0 Active Disk Usage Exceeded alarm might be generated due to large files, which were already marked as deleted. [PR1601251](#)

## MPLS

- On the QFX5000 line of switches, traffic loss occurs after the STP topology changes. [PR1616878](#)

## Layer 2 Ethernet Services

- Traffic received on a port in the LACP Detached state might be incorrectly forwarded. [PR1582459](#)
- The DHCP client might become offline for about 120 seconds after sending the DHCPINFORM message. [PR1587982](#)

## Routing Protocols

- The remaining BFD sessions of the aggregated Ethernet interface flaps continuously if one of the BFD sessions gets deleted. [PR1516556](#)
- The IPv4 static route might still forward traffic unexpectedly even when the static route configuration has already been deleted. [PR1599084](#)
- On the QFX10002 line of switches, the verification of BGP peer count fails after deleting the BGP neighbors. [PR1618103](#)

- Time delay to export prefixes to BGP neighbors might occur post applying peer-specific BGP export policies. [PR1626367](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for QFX Series switches.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrading Software on QFX Series Switches | 155](#)
- [Installing the Software on QFX10002-60C Switches | 157](#)
- [Installing the Software on QFX10002 Switches | 158](#)
- [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 | 159](#)
- [Installing the Software on QFX10008 and QFX10016 Switches | 161](#)
- [Performing a Unified ISSU | 165](#)
- [Preparing the Switch for Software Installation | 165](#)
- [Upgrading the Software Using Unified ISSU | 166](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases | 168](#)

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

## Upgrading Software on QFX Series Switches

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For

information about the contents of the jinstall package and details of the installation process, see the [Installation and Upgrade Guide](#) and [Junos OS Basics](#) in the QFX Series documentation.

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

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

The Junos Platforms Download Software page appears.

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

An Alert box appears.

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

A login screen appears.

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

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

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

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-20.3-R1.n-secure-signed.tgz reboot
```

Replace *source* with one of the following values:

- **/pathname**—For a software package that is installed from a local directory on the switch.

- For software packages that are downloaded and installed from a remote location:

- **`ftp://hostname/pathname`**
- **`http://hostname/pathname`**
- **`scp://hostname/pathname`** (available only for Canada and U.S. version)

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

Rebooting occurs only if the upgrade is successful.

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

## Installing the Software on QFX10002-60C Switches

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

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

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

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

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

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



For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.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 165](#)
- ["Upgrading the Software Using Unified ISSU" on page 166](#)

## 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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

## Junos OS Release Notes for SRX Series

### IN THIS SECTION

- [What's New | 169](#)
- [What's Changed | 176](#)
- [Known Limitations | 179](#)
- [Open Issues | 179](#)
- [Resolved Issues | 182](#)
- [Documentation Updates | 188](#)
- [Migration, Upgrade, and Downgrade Instructions | 188](#)

These release notes accompany Junos OS Release 21.4R1 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- [Application Identification \(AppID\) | 169](#)
- [Authentication and Access Control | 170](#)
- [Chassis | 170](#)
- [Chassis Cluster-specific | 170](#)
- [Flow-Based and Packet-Based Processing | 171](#)
- [Hardware | 171](#)
- [J-Web | 171](#)
- [Network Address Translation \(NAT\) | 173](#)
- [Platform and Infrastructure | 173](#)
- [Routing Policy and Firewall Filters | 174](#)
- [Software Installation and Upgrade | 175](#)
- [Unified Threat Management \(UTM\) | 175](#)
- [Additional Features | 175](#)

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

### Application Identification (AppID)

- **Dual stacking of IPv4 and IPv6 (SRX Series and vSRX)**—Starting in Junos OS Release 21.4R1, we support dual stacking of IPv4 and IPv6 addresses for overlay and underlay networks in an AppQoS configuration.

[See [Support for IPv6 Traffic in AppQoS](#).]

## Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the address-assignment option at the [edit access profile profile-name authentication-order ldap ldap-options] hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

[See [ldap-options](#).]

## Chassis

- **Support for FPC major alarm (SRX5400, SRX5600, and SRX5800 with SPC3)**—In Junos OS Release 21.4R1, we've enhanced the following commands to show more details about the FPC major alarm:
  - show chassis error active
  - show chassis error active detail
  - show chassis error active fpc-slot *slot-number*
  - show chassis error active detail fpc-slot *slot-number*

You can use these commands to identify and troubleshoot the hardware issues.

[See [show chassis errors active](#).]

- **Increase in AC redundancy mode to 2+2 for high-capacity high-line PEMs (SRX5400)**—Starting in Junos OS Release 21.4R1, the SRX5400 device supports 2+2 AC redundancy mode on high-capacity high-line power entry modules (PEMs). The support for 2+2 redundancy mode increases the PEM's capacity from 2050 W to 4100 W.

[See [SRX5400 Services Gateway AC Power Supply Specifications](#).]

## Chassis Cluster-specific

- **Support for external 10GbE ports on SCB2, SCB3, SCB4 (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.4R1, you can connect the HA control links in a chassis cluster using external 10GbE ports on SCB2, SCB3, or SCB4. The Ethernet ports are supported on these types of Switch Control Boards (SCB) as HA control ports. The control link traffic can bypass the SPCs to increase the resiliency of the chassis cluster.

[See [Understanding SCB Control Links](#) and [Chassis Cluster Dual Control Links](#).]

## Flow-Based and Packet-Based Processing

- **Express Path+ for Layer 2 secure-wire traffic (SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.4R1, we've added support for Express Path+ to secure-wire interfaces. This support allows the SRX device to automatically accelerate the flow traversing secure-wire interfaces with their network processor, increasing throughput and decreasing latency.

[See [Express Path](#).]

- **Support for fat flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support fat flow technology to improve the firewall and NAT throughput value up to 10 times of the current value.

[See [Understanding Symmetric Fat IPsec Tunnel](#).]

## Hardware

- **High-capacity second-generation AC PSM for SRX5800**—Starting in Junos OS Release 21.4R1, SRX5800 supports the new high-capacity second-generation AC power supply module (PSM). This single or dual feed PSM provides a maximum output power of 5100 W. In single-feed mode, the PSM provides power at a reduced capacity (2550 W). In dual feed mode, the PSM provides power at full capacity (5100W). The PSM supports 1+1 redundancy.

**High-voltage second-generation Universal PSM for SRX5800**—Starting in Junos OS 21.4R1, the SRX5800 supports the new high-voltage second-generation universal power supply module (PSM). This single feed PSM provides a maximum output power of 5100W, and supports either AC or DC input. The PSM supports 1+1 redundancy.

The increased power supply capacity enables SRX5800 devices to support service cards like SPC3. `show chassis power` command displays PSM status, including state, input type, feed, capacity, output, and remaining power. `show chassis environment pem` command displays the power entry module (PEM) status for state, temperature, AC/DC input, and AC/DC output for the SRX5800 device.

[See [show chassis power](#) and [show chassis environment](#).]

## J-Web

- **Support for Adaptive Threat Profiling in security and IPS policies (SRX Series)**—Starting in Junos OS Release 21.4R1, we support Adaptive Threat Profiling for security and intrusion prevention system (IPS) policy rules.

When creating security policy rules:

- Under Source and Destination, you can configure source and destination identity feeds.
- Under Advanced Settings, you can configure source and destination IP addresses to the feed.

When creating IPS policy rules, you can configure attacker and target IP addresses to the feed.

[See [Add a Rule](#) and [Add Rules to an IPS Policy](#).]

- **Enhanced IPS Policies page (SRX Series)**—In Junos OS Release 21.4R1, we've refreshed the IPS Policies page for better experience. You can:
  - Drag and drop a selected policy to change the order.
  - Search for policies using the Search icon.
  - Add IPS signatures using the new simplified Predefined or Custom tabs.
  - Navigate directly to the Security Policies page to associate the selected IPS policies.
  - When creating IPS policy rules, you can add attacker and target IP addresses.

[See [About the IPS Policies Page](#).]

- **New Security Package Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, you can configure and manage IPS signatures, application signatures, and URL categories at our one-stop shop, the Security Package Management page. You can access this page at **Device Administration > Security Package Management**.

We've removed the following options and pages to avoid duplication:

- Dynamic Applications page:
  - Removed the **Download** button and the **Uninstall/Install** link.
  - Removed the **Download** section from the Global Settings page.
- Security Services menus:
  - Removed the Web Filtering Category Update page from Security Services > UTM.
  - Removed the Signature Update page from Security Services > IPS.

[See [About the Security Package Management Page](#).]

- **Enhanced filtering support on the Monitor Logs pages (SRX Series)**—Starting in Junos OS Release 21.4R1, you can choose many filter values to filter the logs and events on the following pages under Monitor > Logs:
  - Session
  - Threats
  - Web Filtering
  - ATP

- All Events

[See [Monitor Session](#) and [Monitor Threats](#).]

## Network Address Translation (NAT)

- **Enhancements to source NAT pool IP address range and NAT pool name character length (SRX Series and MX-SPC3)**—Starting in Junos OS Release 21.4R1, we've increased the source NAT pool IP address range from 8 IP addresses to 64 IP addresses.

We've also increased the configurable length of the source NAT pool name, destination NAT pool name, source NAT rule name, destination NAT rule name, static NAT rule name, and rule set name from 31 characters to 63 characters.

[See [show security nat source rule](#), [show security nat destination rule](#), and [show security nat static rule](#).]

## Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:
  - View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name group-name` command. See [request security pki ca-profile-group-status](#).
  - Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` command. See [auto-re-enrollment](#).
  - View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <cert_id> detail` command. See [show security pki local-certificate \(View\)](#).
  - View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See [show security pki ca-certificate \(View\)](#).
  - View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See [request security pki ca-certificate verify \(Security\)](#) and [request security pki local-certificate verify \(Security\)](#).
  - View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See [show security pki statistics](#) and [clear security pki statistics](#).



## Routing Policy and Firewall Filters

- **Support for secure vector routing (SVR) with 128T (NFX Series, SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600, and vSRX 3.0)—**

Starting in Junos OS Release 21.4R1, you can deploy software-based 128T distributed routing and network services with SRX Series or NFX Series. 128T services provide session-aware routing for IPv4 traffic and run on any general-purpose compute platform, while the SRX Series or NFX Series device provides a secure SD-WAN gateway and reliable service delivery.

For targeted sessions, the SRX Series or NFX Series device can be the first hop from the client or the last hop to the server. Vector routing packets that enter the device are tagged with source-tenant and destination-service and select the SVR path (to the 128T peer or another SRX Series or NFX Series device). Non-vector-routing packets such as preexisting IPsec tunnels follow their usual path through the device.

To support vector routing, we've introduced new CLI commands at the `[edit services vector-routing]` hierarchy level. Here you can identify the routers you will use with SVR:

```
router-name <router-name> {
  node-name <node-name> {
    interfaces <if-name>
  }
  service-route <service-route-name> {
    destination-service <destination-service-name>
    peer <peer-name>
  }
}
```

You can then define the source and destination sessions:

```
services {
  vector-routing {
    authority-name <authority-name>
    source-tenant <name> {
      interface <if-name>
      ip-prefix <...>
    }
  }
  destination-service <name> {
    ip-prefix <...>
    transport <tcp | udp | icmp | gre>
  }
}
```

```

    port-range <start-port> to <end-port>
  }
  access-policy <source-tenant-name> permission permit / deny
  cipher-suite <cipher-suite-name>
}
}

```

## Software Installation and Upgrade

- **BIOS firmware (SRX5400, SRX5600, and SRX5800 with SPC3)**—Starting in Junos OS Release 21.4R1, you can download and install a new version of BIOS by installing the jfirmware package that contains the new BIOS capsule. You do not need to install a new version of Junos OS.

[See [Upgrading BIOS and Firmware \(SRX only\)](#).]

## Unified Threat Management (UTM)

- **Content filtering based on file content (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, unified threat management (UTM) performs content filtering to determine the file type based on the file content and not on file extensions. This feature complements application identification (App ID) by enabling you to configure the firewall to identify and to control access to the Web (HTTP and HTTPS) traffic and to protect your network from attacks.

This content filtering improvement replaces the existing content filtering based on filename extensions and profile-based filtering on application profiles.

Use the **show security utm content-filtering statistics** command to view the content-filtering system statistics and errors.

With this feature implementation, we do not support content filtering based on MIME type, content type, and protocol commands.

The legacy content-filtering configurations are deprecated and are hidden. You will receive system logs and error messages if you try to configure the legacy content filtering options. You can use the legacy functionality if you don't want to migrate to this improved functionality.

[See [Content Filtering](#), [content-filtering \(Security UTM Policy\)](#), [utm](#), and [utm default-configuration](#).]

## Additional Features

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

- **Configure concurrent connections** (SRX Series devices and vSRX running ike). Configure the number of concurrent connections that the group profile supports using the `connections-limit` configuration statement at the `[edit security ike gateway gateway-name dynamic]` hierarchy level. We support this

configuration for both IKEv1 and IKEv2. This configuration is applicable only to AutoVPN, ADVPN, dynamic endpoint, and remote access (preshared-key and PKI-based tunnels).

There are no restrictions on the number of connections accepted if you haven't configured the `connections-limit` option.

[See [dynamic \(Security\)](#)].

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running ike2). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

This feature is supported only if the `junos-ike` package is installed in your device.

[See [Routing Protocols Support on IPsec VPN Tunnels](#).]

- **MACsec bounded delay protection** (EX4400 and SRX380)

[See [bounded-delay](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 176

Learn about what changed in this release for SRX Series Gateways.

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [General Routing](#) | 177
- [J-Web](#) | 177
- [Network Management and Monitoring](#) | 177
- [Unified Threat Management \(UTM\)](#) | 178

## General Routing

- **No support for PKI operational mode commands on the Junos Limited version (MX Series routers, PTX Series routers, and SRX Series devices)**— We do not support `request`, `show`, and `clear` PKI-related operational commands on the limited encryption Junos image ("Junos Limited"). If you try to execute PKI operational commands on a limited encryption Junos image, then an appropriate error message is displayed. The `pkid` process does not run on Junos Limited version image. Hence, the limited version does not support any PKI-related operation.

## J-Web

- **Changes to the Dashboard and Monitor pages (SRX Series)**—To improve the J-Web UI loading speed:
  - On the Dashboard page, we've removed the on-box reports related widgets.
  - On the Monitor > Maps and Charts > Traffic Map page, we've changed the default duration from "Last 1 hour" to Last "5 minutes".
- **Changes in Identity Management page (SRX Series)**—Starting in Junos OS Release 21.4R1, we've renamed Identity Management as Juniper Identity Management Services (JIMS) in the following location:
  - In Security Services > Firewall Authentication, the Identity Management menu is renamed to JIMS.
  - In Identity Management page, all instances of Identity Management are renamed to Juniper Identity Management Services.

## Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type `identityref` in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type `identityref` in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following

changes apply when you deactivate or delete ephemeral database instances in the static configuration database:

- When you deactivate the entire `[edit system configuration-database ephemeral]` hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
- When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.
- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

## Unified Threat Management (UTM)

- **Default action hit output field for UTM Web filtering statistics (SRX Series)**—We've introduced a new `Default action hit` output field for the `show security utm web-filtering statistics` operational command. The `Default action hit` output field displays the number of sessions for which the `juniper-local`, `juniper-enhanced`, or `websense-redirect` profiles took the default action.

[See [show security utm web-filtering statistics](#).]

## VPNs

- **Deprecated Dynamic VPN CLI configuration statements and operational commands (SRX Series Devices)**—Starting in Junos OS Release 21.4R1, we've deprecated the dynamic VPN remote access solution. This means that you cannot use Pulse Secure Client on these devices.

As part of this change, we've deprecated the `[edit security dynamic-vpn]` hierarchy level and its configuration options. We've also deprecated the `show` and `clear` commands under the `[dynamic-vpn]` hierarchy level.

As an alternative, you can use the Juniper Secure Connect remote access VPN client that we introduced in Junos OS Release 20.3R1. Juniper Secure Connect is a user-friendly VPN client that supports more features and platforms than dynamic VPN does. SRX comes with two built-in concurrent users on all SRX Series devices. If you need additional concurrent users, then contact your Juniper Networks representative for remote-access licensing. To understand more about Juniper Secure Connect licenses, see [Licenses for Juniper Secure Connect and Managing Licenses](#).

[See [Juniper Secure Connect User Guide](#), [Juniper Secure Connect Administrator Guide](#), [Licenses for Juniper Secure Connect](#), and [Managing Licenses](#) .]

## Known Limitations

### IN THIS SECTION

- [J-Web | 179](#)
- [VPNs | 179](#)

Learn about known limitations in Junos OS Release 21.4R1 for SRX Series Gateways.

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

## J-Web

- The Firefox browser displays an unsaved changes error message in the J-Web basic settings page if the autofill logins and passwords option is selected under the browser privacy and security settings. [PR1560549](#)

## VPNs

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

## Open Issues

Learn about open issues in Junos OS Release 21.4R1 for SRX Series Gateways.

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

- Use 512 antireplay window size for IPv6 in fat-tunnel. The ESP sequence check might otherwise report out-of-order packets if the fat-tunnel parallel encryption is within 384 packets (12 cores \* 32 packets in one batch). Hence there are no out-of-order packets with 512 antireplay window size. [PR1470637](#)
- For accelerated flows such as Express Path, the packet or byte counters in the session close log and show session output take into account only the values that accumulated while traversing the NP. [PR1546430](#)

## General Routing

- HTTP sessions takes approximately 10 minutes to re-establish after a link flap between hub and spoke. [PR1577021](#)
- With SSL proxy configured along with Web proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- HA AP mode on-box logging in logical systems and tenant systems, the intermittently security log contents of binary log file in logical systems and tenant systems are not as expected. [PR1587360](#)
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This might affect the app identification for the web-proxy session traffic. [PR1588139](#)
- The switch reason is being shown as nh change instead of sla violated in the best path log message. [PR1602571](#)
- Advanced anti malware hash feature is deprecated. [PR1604426](#)
- The issue is when we enable TCP path finder in the VPN gateway, VPN connection is established properly. After VPN connection is established, able to ping from JSC installed CLIENT to SERVER behind gateway, but unable to ping from SERVER behind gateway to Juniper Secure Connect installed CLIENT. [PR1611003](#)
- The t1 interface admin status will be shown as test instead of down during FPC failover. [PR1615494](#)
- On SRX345 device, Junos OS release 21.3R1 with custom application configured with matching pattern in traffic, APPQOE\_APP\_BEST\_PATH\_SELECTED is showing the custom application name instead of predefined Layer7 application name. [PR1617087](#)
- FIPS mode enabling fails with self test failure and kernel process stops. [PR1623128](#)

- For LTE interfaces (dl0, cl-\*) on security devices, configured in a High Availability cluster mode if redundancy failover is performed then user might lose connection to the internet. If redundancy failover is not performed then no issue is seen. [PR1625125](#)
- On SRX1500 devices, ISSU is getting aborted with ISSU is not supported for Clock Synchronization (SyncE). [PR1632810](#)

## Intrusion Detection and Prevention (IDP)

- While executing CLI show security idp attack attack-list policy combine-policy, CLI might get stuck and only partial output gets displayed. [PR1616782](#)

## Layer 2 Ethernet Services

- LACPD generates core files sometimes when member links are swapped between two reth bundle using rollback operation given that prior to rollback each of the bundle already has maximum number of child links. [PR1632371](#)

## Routing Policy and Firewall Filters

- If tunnel inspection policies are defined, VXLAN sessions are not getting established. [PR1604625](#)

## VPNs

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. [PR1416334](#)
- An IPsec policy must not have both ESP and AH proposals. The configuration will commit, but the IPsec traffic will not work. Do not configure an IPsec policy with proposals using both ESP and AH. protocols. [PR1552701](#)
- Fragment packets through policy based IPsec tunnel could be dropped in some rare case when PMI is enabled. [PR1624877](#)



## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | **182**

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

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

### Resolved Issues: 21.4R1

#### IN THIS SECTION

- [Application Layer Gateways \(ALGs\)](#) | **182**
- [Authentication and Access Control](#) | **183**
- [Flow-Based and Packet-Based Processing](#) | **183**
- [General Routing](#) | **183**
- [Infrastructure](#) | **186**
- [Interfaces and Chassis](#) | **186**
- [Intrusion Detection and Prevention \(IDP\)](#) | **186**
- [J-Web](#) | **186**
- [Network Address Translation \(NAT\)](#) | **187**
- [Platform and Infrastructure](#) | **187**
- [Routing Policy and Firewall Filters](#) | **187**
- [Routing Protocols](#) | **187**
- [Unified Threat Management \(UTM\)](#) | **187**
- [VPNs](#) | **187**

### Application Layer Gateways (ALGs)

- ALG traffic might be dropped. [PR1598017](#)

## Authentication and Access Control

- UAC authentication might not work post system reboot. [PR1585158](#)

## Flow-Based and Packet-Based Processing

- Performance degradation might be observed when power-mode-ipsec is enabled. [PR1599044](#)
- The services offload packets processed counter not incremented in security flow statistics. [PR1616875](#)
- Security traffic log display service-name as none for some application. [PR1619321](#)
- Cleartext fragments are not processed by flow. [PR1620803](#)
- On SRX4600 and SRX5000 line of devices, when an interface is configured in TAP mode, the vlan-id-range is now supported in non-default routing instances. [PR1624041](#)

## General Routing

- SSL-FP logging for non SNI session. [PR1442391](#)
- In non-FIPS mode, the RNG in FreeBSD 12 based Junos OS versions has been changed from the default FreeBSD Fortuna RNG to the FIPS/SP800-90A&B HMAC-DRBG CSPRNG. [PR1529574](#)
- Some transmitting packets might get dropped due to the disable-pfe action is not invoked when the fabric self-ping failure is detected. [PR1558899](#)
- The CLI command show pfe statistics traffic shows wrong output. [PR1566065](#)
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile set security log profile default-profile can be used to improve this behavior when multiple log profiles are defined. [PR1570105](#)
- Changes in SNMP traps configuration and data exported for TWAMP. [PR1573169](#)
- On SRX Series devices with Chassis Cluster, the tcp\_timer\_keep:Local(0x81100001:60753) Foreign(0x8f100001:33010) is seen in messages log every 80 seconds. [PR1580667](#)
- Traffic is dropped to or through VRRP virtual IP on SRX380 device. [PR1581554](#)
- The srpxfe process might stop on SRX1500 devices. [PR1582989](#)
- Secure Web proxy continue sending DNS query for unresolved DNS entry even after the entry was removed. [PR1585542](#)

- On SRX Series devices, significant performance improvements for JDPI's micro-application identification were included in this release. [PR1585683](#)
- The show security idp counters command is not having tenant command in the syntax. [PR1586220](#)
- IP packets might be dropped on SRX Series devices. [PR1588627](#)
- The jsqsyncd process files generation might cause device to stop after upgrade. [PR1589108](#)
- The REST API does not work for SRX380 devices. [PR1590810](#)
- The issue (empty feed-name) starts with the hit returned from cache which points to the node with the parameter of feed-ID (2) inconsistent with the feeds-update (when it's 1). As a result the incorrect feed-ID points to the empty entry in the array of the feed-names. [PR1591236](#)
- J-Web deny log nested-application as UNKNOWN instead of specific application. [PR1593560](#)
- When combining log profiles and unified policies RT\_FLOW\_SESSION\_DENY logs were not being generated corrected. [PR1594587](#)
- System logs are generated when maximum session or total memory limit is hit for packet capture. [PR1594669](#)
- The flowd process might stop when AppID marks the application as complete and the inspection limits are hit. [PR1595310](#)
- Node1 fpc0 (SPM) goes down after ISSU and RGO failover. [PR1595462](#)
- Sometimes, when Jflow v9 flow record can contain wrong application id from cache, which can lead wrong identification of traffic application. [PR1595787](#)
- On SRX Series devices with SPC3, when SPC3 fails in specific circumstances, there might be delay observed in failover to other node. [PR1596118](#)
- The flowd process might generate core files if application services security policy is configured. [PR1597111](#)
- The srxpfe process might stop and generate a core file post "targeted-broadcast forward-only" interface-config commit. [PR1597863](#)
- The flowd process might generate core files if the AppQOS module receiving two packets of a session. [PR1597875](#)
- The flowd process might stop in AppQoS scenarios [PR1599191](#)
- The httpd-gk process generates core files when IPsec VPN is configured. [PR1599398](#)
- CRC or align errors and fragment frames might be seen with traffic against 400G ports. [PR1601151](#)

- Traffic might be dropped at NAT gateway if EIM is enabled. [PR1601890](#)
- Kernel crash might be seen when static routes are configured with GRE interfaces being used as next-hop. [PR1601996](#)
- The flowd process might stop if the DNS-inspection feature is enabled by configuring SMS policy. [PR1604773](#)
- Memory leak at the useridd process might be observed when integrated user firewall is configured. [PR1605933](#)
- When the tap mode is enabled, the packet on ge-0/0/0 is dropped on RX side. [PR1606293](#)
- The flowd process might stop if the DNS-inspection feature is enabled within SMS. [PR1607251](#)
- DNS proxy functionality might not work on VRRP interfaces. [PR1607867](#)
- Enabling dnsf traceoptions on SRX300 line of devices might result in flowd process to stop. [PR1608669](#)
- Enabling security-metadata-streaming-policy command might cause Packet Forwarding Engine stop. [PR1610260](#)
- DNS-based SecIntel statistics were not populating correctly on SRX Series devices. [PR1611071](#)
- On SRX Series devices running DNS security, the notification option 'log-detections' was not honoured. Prior to this release, a log was generated for every DNS request, regardless of its intent. [PR1611177](#)
- Interface might not come up when 10G port is connected to 1G SFP. [PR1613475](#)
- Enabling security-metadata-streaming DNS policy might cause a data plane memory leak. [PR1613489](#)
- On SRX Series devices running DNS Security in secure-wire mode, DGA verdicts would not be returned to the device. [PR1616075](#)
- The srpxfe process might stop when the DNS security feature is enabled. [PR1616171](#)
- Traffic might get dropped due to memory issue on some SRX Series devices. [PR1620888](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)
- When viewing DNS Tunnel detections in the ATP Cloud portal, the Source-IP and Destination-IP metadata is reversed. [PR1629995](#)

## Infrastructure

- Upgrade might fail when upgrading from previous releases. [PR1602005](#)

## Interfaces and Chassis

- IPv4 or IPv6 address from the config on the interface might not be applied when the interface is moved from tenants to interface stanza in the configuration. [PR1605250](#)

## Intrusion Detection and Prevention (IDP)

- IDP signature DB update fails. [PR1594283](#)
- Custom attack IDP policies might fail to compile. [PR1598867](#)
- IDP policy compilation is not happening when a commit check is issued prior to a commit. [PR1599954](#)
- The srpxfe process might stop while the IDP security package contains a new detector. [PR1601380](#)
- This release includes optimizations made to IDP that help improve its performance and behavior under load. [PR1601926](#)
- High Routing Engine CPU usage occurs when routing instance is configured under security idp security-package hierarchy level. [PR1614013](#)
- IDP signature install taking longer time. [PR1615985](#)
- Application identification DB update failing to download when used through IDP offline method. [PR1623857](#)

## J-Web

- J-Web a custom application name contains "any" is listed under pre-defined applications. [PR1597221](#)
- J-Web might not display customer defined application services if one new policy is created. [PR1599434](#)
- J-Web application might stop and generate the httpd process core files. [PR1602228](#)
- Radius users might not be able to view or modify configuration through J-Web. [PR1603993](#)
- On all SRX Series devices, some widgets in J-Web might not load properly for logical systems users. [PR1604929](#)
- The error displays "your session has expired. click ok to re-login" when using root user. [PR1611448](#)

- The AM or PM time format is displayed in customize for last field at Monitor > Logs > All Events. [PR1628649](#)

## Network Address Translation (NAT)

- Incorrect IPv6 UDP checksum inserted after translation of packet from IPv4 to IPv6. [PR1596952](#)

## Platform and Infrastructure

- Junos OS: Upon receipt of specific sequences of genuine packets destined to the device the kernel will crash and restart (vmcore) (CVE-2021-0283, CVE-2021-0284). [PR1595649](#)
- The process mgd might stop with authentication setup. [PR1600615](#)
- SRX accounting and auditd process might not work on secondary node. [PR1620564](#)

## Routing Policy and Firewall Filters

- High CPU usage might be seen on some SRX Series devices. [PR1579425](#)

## Routing Protocols

- Short multicast packets drop using PIM when multicast traffic received at a non-RPT/SPT interface. [PR1579452](#)
- The fwauthd process generates core file when upgrading to Junos OS 21.2R1 release. [PR1588393](#)
- While testing pppoe\_dhcpv6, observing commit error while configuring routing-options rib inet6.0 static. [PR1599273](#)

## Unified Threat Management (UTM)

- There is no counter for juniper-local default action. [PR1570500](#)

## VPNs

- The iked process might restart and generate core during session state activation or deactivation [PR1573102](#)
- The iked process might stop when IKEv2 negotiation fails on MX or SRX Series devices. [PR1577484](#)
- Memory leaks on the iked process on SRX5000 line of devices with SRX5K-SPC3 installed. [PR1586324](#)

- Certificate identifier length for PKI CMPv2 CA cert is not displayed as expected in certain cases. [PR1589084](#)
- The IPsec tunnel might not come up if configured with configuration payload in a certain scenario. [PR1593408](#)
- The kmd process might crash when VPN peer initiates using source-port other than 500. [PR1596103](#)
- Tail drops might occur on SRX Series devices if shaping-rate is configured on st-interface. [PR1604039](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for SRX Series Gateways.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases](#) | 188

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

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

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release

to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.4.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

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

## Junos OS Release Notes for vMX

### IN THIS SECTION

- [What's New | 190](#)
- [What's Changed | 191](#)
- [Known Limitations | 192](#)
- [Open Issues | 192](#)
- [Resolved Issues | 193](#)
- [Documentation Updates | 193](#)
- [Upgrade Instructions | 193](#)

These release notes accompany Junos OS Release 21.4R1 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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



## What's New

### IN THIS SECTION

- [Licensing | 190](#)
- [Operation, Administration, and Maintenance \(OAM\) | 190](#)

Learn about new features introduced in this release for vMX Virtual Router.

### Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:
  - `set system license autoupdate url <link>`
  - `set system license renew before-expiration <days>`
  - `set system license renew interval <hours>`

The `license autoupdate` and `license renew` commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

[See [License Autoupdate and License Renew](#).]

### Operation, Administration, and Maintenance (OAM)

- **Enhancements to BFD-triggered FRR for unicast next hops and forwarding-table session-id-change-limiter-indirect to address issue of traffic being silently discarded (MX150, MX204, MX240, MX304, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX3000, PTX5000, PTX10001, PTX10002, PTX10016, QFX10002-60C, QFX10002, QFX10008, QFX10016, and vMX)**—In Junos OS Release 21.4R1, we've enhanced the BFD-triggered fast reroute (FRR) for unicast next hops and forwarding-table session-id-change-limiter-indirect to address the issue of traffic being silently discarded because of a session mismatch between the control plane and data plane.

To align the traffic by creating session-id-change-limiter indirect next hop, set the `set routing-options forwarding-table session-id-change-limiter-indirect` configuration statement at the [edit routing-options forwarding-table] hierarchy level.

[See [Bidirectional Forwarding Detection \(BFD\) for MPLS.](#)]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 191

Learn about what changed in this release for vMX Virtual Router.

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [Network Management and Monitoring](#) | 191

## Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.

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

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

## Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R1 for vMX Virtual Router.

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

## Open Issues

### IN THIS SECTION

- [Platform and Infrastructure](#) | 192

Learn about open issues in Junos OS Release 21.4R1 for vMX Virtual Router.

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

## Platform and Infrastructure

- In VMX platform, after a system reboot, the Protect-RE filter on lo0 interface is no longer applied. This issue has been fixed in 17.1R1 and later releases. A commit full can clear the issue. [PR1604401](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1 | 193](#)

Learn about the issues fixed in this release for vMX Virtual Router.

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

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [Interfaces and Chassis | 193](#)

## Interfaces and Chassis

- Interface hold-time up does not work on vMX and MX150 devices. [PR1604554](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for vMX Virtual Router.

## Upgrade Instructions

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

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

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

# Junos OS Release Notes for vRR

## IN THIS SECTION

- What's New | 194
- What's Changed | 194
- Known Limitations | 194
- Open Issues | 195
- Resolved Issues | 195
- Documentation Updates | 196

These release notes accompany Junos OS Release 21.4R1 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

There are no new features or enhancements to existing features in Junos OS Release 21.4R1 for Virtual Route Reflector.

## What's Changed

There are no changes in behavior and syntax in Junos OS Release 21.4R1 for Virtual Route Reflector.

## Known Limitations

There are no known limitations in hardware and software in Junos OS 21.4R1 for Virtual Route Reflector.

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

To learn more about common BGP or routing known limitations in Junos OS 21.4R1, see "[Known Limitations](#)" on [page 72](#) for MX Series routers.

## Open Issues

### IN THIS SECTION

- [Platform and Infrastructure](#) | [195](#)

Learn about open issues in Junos OS Release 21.4R1 for Virtual Route Reflector.

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 knowns issues in Junos OS 21.4R1, see "[Open Issues](#)" on [page 75](#) for MX Series routers.

## Platform and Infrastructure

- vRR VM might come up as Olive after a CLI software upgrade using junos-install-mx\* package if the XML used to spawn the VM didn't have SMBIOS entry "<entry name='product'>VRR</entry>".  
[PR1635950](#)

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1](#) | [196](#)

Learn about the issues fixed in this release for Virtual Route Reflector.

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

## Resolved Issues: 21.4R1

### IN THIS SECTION

- [General Routing | 196](#)

## General Routing

- Memory might be exhausted when both the BGP rib-sharding and the BGP ORR (Optimal Route Reflection) enabled. [PR1613104](#)
- The process rpd might crash in BGP rib sharding scenario. [PR1613723](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for Virtual Route Reflector.

# Junos OS Release Notes for vSRX

### IN THIS SECTION

- [What's New | 197](#)
- [What's Changed | 201](#)
- [Known Limitations | 202](#)
- [Open Issues | 202](#)
- [Resolved Issues | 205](#)

- Documentation Updates | 207
- Migration, Upgrade, and Downgrade Instructions | 207

These release notes accompany Junos OS Release 21.4R1 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

## What's New

### IN THIS SECTION

- Application Identification (AppID) | 197
- Authentication and Access Control | 198
- Flow-Based and Packet-Based Processing | 198
- Interfaces | 198
- Licensing | 198
- Platform and Infrastructure | 199
- Unified Threat Management (UTM) | 199
- Additional Features | 200

Learn about new features introduced in this release for vSRX Virtual Firewall.

### Application Identification (AppID)

- **Dual stacking of IPv4 and IPv6 (SRX Series and vSRX)**—Starting in Junos OS Release 21.4R1, we support dual stacking of IPv4 and IPv6 addresses for overlay and underlay networks in an AppQoS configuration.

[See [Support for IPv6 Traffic in AppQoS](#).]



## Authentication and Access Control

- **LDAP authentication for Juniper Secure Connect (SRX Series devices and vSRX with Juniper Secure Connect)**—In Junos OS Release 21.4R1, we've introduced support for native LDAP authentication with secure connection to simplify deployments of Juniper Secure Connect. With the LDAP authentication support, you can determine which groups should be granted access after successful authentication. Use the address-assignment option at the [edit access profile profile-name authentication-order ldap ldap-options] hierarchy level to assign IP addresses specifically for those groups of users to simplify IP address management.

[See [ldap-options](#).]

## Flow-Based and Packet-Based Processing

- **Support for MPLS Layer 3 VPN in flow mode (vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support MPLS Layer 3 VPN in flow mode. We also support IP unicast packet processing. Thus, IP unicast packets de-encapsulated from MPLS enter the flow processing when you enable set security forwarding-options family mpls mode flow-based.

[See [Flow Management in SRX Series Devices Using VRF Routing Instance](#).]

- **Support for fat flow (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, we support fat flow technology to improve the firewall and NAT throughput value up to 10 times of the current value.

[See [Understanding Symmetric Fat IPsec Tunnel](#).]

## Interfaces

- **Microsoft Azure Advanced Networking with SR-IOV support (vSRX 3.0)**—Starting in Junos OS Release 21.4R1, vSRX 3.0 supports the Azure Accelerated Networking (AAN) feature. AAN utilizes the Mellanox single-root I/O virtualization (SR-IOV) virtual function for high-speed networking. Microsoft Azure uses Mellanox ConnectX-3, ConnectX-4, and ConnectX-5 NICs to support AAN. However, vSRX 3.0 supports only ConnectX-4 and ConnectX-5 AAN.

See [Understand vSRX with Microsoft Azure Cloud](#) and [Enable Accelerated Networking for Replicated VMs](#).

## Licensing

- **License renewal or automatic update (EX2300, EX3400, EX4300, EX4400-24MP, PTX10001-36MR, PTX10003, PTX10008, PTX10016, QFX5130-32CD, QFX5220, vMX, and vSRX)**—Starting in Junos OS Release 21.4R1, you can renew or automatically update all software feature licenses using the following commands:
  - set system license autoupdate url <link>

- `set system license renew before-expiration <days>`
- `set system license renew interval <hours>`

The `license autoupdate` and `license renew` commands streamline license tracking. Use these commands to reduce the manual tracking effort for license renewal.

[See [License Autoupdate and License Renew](#).]

## Platform and Infrastructure

- **PKI usability enhancements (MX240, MX480, MX960, SRX Series, and vSRX)**—Starting in Junos OS Release 21.4R1, we've enhanced PKI commands to provide additional details about the local and certificate authority (CA)-issued certificates. With these enhancements, you can:
  - View the CA certificate status of a CA profile group using the `request security pki ca-profile-group-status ca-group-name group-name` command. See [request security pki ca-profile-group-status](#).
  - Configure certificate automatic reenrollment trigger time in days, hours, or percentage using the `set security pki auto-re-enrollment cmpv2 certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` or `set security pki auto-re-enrollment scep certificate-id certificate-id-name re-enroll-time (days value| hours value| percentage value)` command. See [auto-re-enrollment](#).
  - View the CA chain, SHA256 fingerprint, and certificate serial number (hexadecimal and decimal format) for a local certificate using the `show security pki local certificate <cert_id> detail` command. See [show security pki local-certificate \(View\)](#).
  - View the CA profile associated with a CA certificate and SHA256 fingerprint using the `show security pki ca-certificate <brief|detail>` command. See [show security pki ca-certificate \(View\)](#).
  - View additional verification information about local and CA certificate using the `request security pki local-certificate verify` and the `request security pki ca-certificate verify` command, respectively. See [request security pki ca-certificate verify \(Security\)](#) and [request security pki local-certificate verify \(Security\)](#).
  - View more PKI-related statistics using the `show security pki statistics` command. Clear the PKI statistics using the `clear security pki statistics` command. See [show security pki statistics](#) and [clear security pki statistics](#).

## Unified Threat Management (UTM)

- **Content filtering based on file content (SRX Series and vSRX 3.0)**—Starting in Junos OS Release 21.4R1, unified threat management (UTM) performs content filtering to determine the file type based on the file content and not on file extensions. This feature complements application identification (App ID) by enabling you to configure the firewall to identify and to control access to the Web (HTTP and HTTPS) traffic and to protect your network from attacks.

This content filtering improvement replaces the existing content filtering based on filename extensions and profile-based filtering on application profiles.

Use the **show security utm content-filtering statistics** command to view the content-filtering system statistics and errors.

With this feature implementation, we do not support content filtering based on MIME type, content type, and protocol commands.

The legacy content-filtering configurations are deprecated and are hidden. You will receive system logs and error messages if you try to configure the legacy content filtering options. You can use the legacy functionality if you don't want to migrate to this improved functionality.

[See [Content Filtering](#), [content-filtering \(Security UTM Policy\)](#), [utm](#), and [utm default-configuration](#).]

## Additional Features

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

- **Configure concurrent connections** (SRX Series devices and vSRX running ike). Configure the number of concurrent connections that the group profile supports using the `connections-limit` configuration statement at the `[edit security ike gateway gateway-name dynamic]` hierarchy level. We support this configuration for both IKEv1 and IKEv2. This configuration is applicable only to AutoVPN, ADVPN, dynamic endpoint, and remote access (preshared-key and PKI-based tunnels).

There are no restrictions on the number of connections accepted if you haven't configured the `connections-limit` option.

[See [dynamic \(Security\)](#).]

- **Dynamic routing protocols** (MX240, MX480, and MX960 with MX-SPC3, SRX5000 line of devices with SPC3 card and vSRX running ike). We support the exchange of dynamic routing information through IPsec VPN tunnels. You can now enable the dynamic routing protocol, such as OSPF, BGP, BFD, PIM, and RIP on a st0 interface of an IPsec VPN tunnel.

This feature is supported only if the `junos-ike` package is installed in your device.

[See [Routing Protocols Support on IPsec VPN Tunnels](#).]

## What's Changed

### IN THIS SECTION

- [What's Changed in Release 21.4R1](#) | 201

Learn about what changed in this release for vSRX Virtual Firewall.

## What's Changed in Release 21.4R1

### IN THIS SECTION

- [Network Management and Monitoring](#) | 201

## Network Management and Monitoring

- **The configuration accepts only defined identity values for nodes of type identityref in YANG data models (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—If you configure a statement that has type identityref in the corresponding YANG data model, the device accepts only defined identity values (as defined by an identity statement) as valid input. In earlier releases, the device also accepts values that are not defined identity values.
- **Changes when deactivating or deleting instances of the ephemeral configuration database (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—The following changes apply when you deactivate or delete ephemeral database instances in the static configuration database:
  - When you deactivate the entire [edit system configuration-database ephemeral] hierarchy level, the device deletes the files and corresponding configuration data for all user-defined ephemeral instances. In earlier releases, the files and configuration data are preserved; however, the configuration data is not merged with the static configuration database.
  - When you delete an ephemeral instance in the static configuration database, the instance's configuration files are also deleted. In earlier releases, the configuration files are preserved.

- You can delete the files and corresponding configuration data for the default ephemeral database instance by configuring the `delete-ephemeral-default` statement in conjunction with the `ignore-ephemeral-default` statement at the `[edit system configuration-database ephemeral]` hierarchy level.

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

## Known Limitations

### IN THIS SECTION

- [General Routing](#) | 202

Learn about known limitations in Junos OS Release 21.4R1 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.

## General Routing

- There is maximum limit on number of vlans that can be configured per VF for i40e driver. The number is 8. The maximum VLAN supported per VF is 63 VLANs in SR-IOV trust mode. [PR1610282](#)
- When multiple vlan-tagging sub-interfaces are configured and switching vSRX3.0 between vlan-tagging and flexible-vlan-tagging support mode, traffic will stop and must reboot vSRX3.0 to recover, if trust mode is disabled for the virtual functions. [PR1610287](#)

## Open Issues

### IN THIS SECTION

- [Flow-Based and Packet-Based Processing](#) | 203

- General Routing | 203
- Intrusion Detection and Prevention (IDP) | 204
- Routing Policy and Firewall Filters | 204
- VPNs | 204

Learn about open issues in Junos OS Release 21.4R1 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.

## Flow-Based and Packet-Based Processing

- The traffic in the power mode still passthrough when the ingress logic interface is manually disabled. [PR1604144](#)
- You must keep 1 to 2 minutes gap between two configuration commits if there are lots of security policies which need time to be processed. [PR1625531](#)

## General Routing

- Tag "RT\_FLOW\_SESSION\_XXX" is missing in stream mode. [PR1565153](#)
- During auto reenrollment of cmpv2 certificates, if the CA server is unresponsive and cmpv2 request retries has reached the maximum limit, then pkid core might occur. [PR1580442](#)
- With SSL proxy configured along with web-proxy, the client session might not closed on the device even though proxy session ends gracefully. [PR1580526](#)
- Getting UNKNOWN instead of HTTP-PROXY for application and UNKNOWN instead of GOOGLE-GEN in RT-FLOW close messages These messages can be seen in the RT-flow close log and these are due to JDPI not engaged for the session. This may affect the application identification for the web-proxy session traffic. [PR1588139](#)
- The performance will be improved by set security forwarding-options no-allow-dataplane-sleep command. [PR1602564](#)

- The switch reason is being shown as nh change instead of sla violated in the best path log message. [PR1602571](#)
- One needs to configure set security forwarding-options no-allow-dataplane-sleep for high traffic rate use cases. [PR1602606](#)
- The advanced anti-malware Hash feature is deprecated. [PR1604426](#)

## Intrusion Detection and Prevention (IDP)

- While executing CLI show security idp attack attack-list policy combine-policy, CLI might get stuck and only partial output gets displayed. CLI recovers in its own. [PR1616782](#)

## Routing Policy and Firewall Filters

- When SSL proxy global configuration is set with enable-proxy-on-default-fw-policy-match, the traffic is hitting pre-id policy instead of default policy for Yahoo traffic. [PR1542790](#)
- For Junos OS 21.4R1 release, policy rematch capability for src-tenant, dest-service dimensions won't be supported due to high risk . [PR1625172](#)

## VPNs

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

## Resolved Issues

### IN THIS SECTION

- [Resolved Issues: 21.4R1 | 205](#)

Learn about the issues fixed 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: 21.4R1

#### IN THIS SECTION

- [Application Layer Gateways \(ALGs\) | 205](#)
- [Authentication and Access Control | 205](#)
- [General Routing | 206](#)
- [Intrusion Detection and Prevention \(IDP\) | 206](#)
- [Network Address Translation \(NAT\) | 206](#)
- [Routing Policy and Firewall Filters | 207](#)
- [Routing Protocols | 207](#)
- [VPNs | 207](#)

### Application Layer Gateways (ALGs)

- ALG traffic might be dropped. [PR1598017](#)

### Authentication and Access Control

- UAC authentication might not work post system reboot. [PR1585158](#)



## General Routing

- IKE configure mode payload is not pushing secondary DNS and secondary WINS attributes to Xauth module with IKEv1. Hence, the client is not getting assigned with secondary DNS and secondary WINS with IKEv1. [PR1558831](#)
- When using log templates with unified policies, logs were not generated in a predictable manner. A new construct has been added that allows you to define a default log profile (set security log profile default-profile) that can be used to improve this behavior when multiple log profiles are defined. [PR1570105](#)
- The srxpfe or flowd process might stop when using Juniper ATP cloud. [PR1573157](#)
- vSRX unreachable over SSH after integration with KMS on AWS. [PR1584415](#)
- When combining log profiles and unified policies RT\_FLOW\_SESSION\_DENY logs were not being generated corrected. [PR1594587](#)
- Network based application recognition value for IPv4 application ID are not as expected. [PR1595787](#)
- The FPC might not come up if the vCPU number is configured more than 5 vCPU on vSRX3.0. [PR1601823](#)
- vSRX3.0 with Mellanox SR-IOV interfaces on VMware, the interface order is random. [PR1604060](#)
- vSRX might stop forwarding traffic 60 days after Junos OS upgrade due to the trial license expiring. [PR1609551](#)
- For apps getting classified on first packet, the volume update syslog is not getting generated. [PR1613516](#)
- The interface speed is limited to 1G on vSRX 2.0 even the speed is set as more than 1G. [PR1617397](#)
- Assert core might be seen when the application goes to **no path selected** state. [PR1617506](#)
- Running DNS on all SRX Series devices, a memory leak on Packet Forwarding Engine might occur. [PR1624655](#)

## Intrusion Detection and Prevention (IDP)

- The flowd or srxpfe process might stop when IDP is used on Junos OS Release 21.2R1. [PR1610706](#)

## Network Address Translation (NAT)

- SNMP object "jnxJsNatSrcNumPortAvail" does not show the proper value. [PR1611479](#)

## Routing Policy and Firewall Filters

- After policy configuration commit with source tenant and destination services id field set as 0 due to this Incoming traffic processed by first policy. [PR1617026](#)
- Policy re-match extensive is not working for SVR traffic. [PR1618717](#)

## Routing Protocols

- The rpd process generates core files because of memory corruption. [PR1599751](#)

## VPNs

- Unable to set DynamoDB in HSM module. [PR1599069](#)

## Documentation Updates

There are no corrections or changes in Junos OS Release 21.4R1 documentation for vSRX Virtual Firewall.

## Migration, Upgrade, and Downgrade Instructions

### IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 214](#)

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 21.4R1 for vSRX using J-Web (see [J-Web](#)) or the Junos Space Network Management Platform (see [Junos Space](#)).

Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

Check this using the following command:

```
show system storage | match " /var$" /dev/vtbd1s1f
2.7G      82M      2.4G      3% /var
```

Using the request system storage cleanup command might help reach that percentage.

- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the request system software add /var/host-mnt/var/tmp/<upgrade\_image>
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.
- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

**NOTE:** For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX instance on the targeted OS version.

## Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 21.4R1 for vSRX .tgz** file from the [Juniper Networks website](#). Note the size of the software image.

2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```

root@vsvrx> 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@vsvrx> 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
21.4K	Sep 25 14:15	/var/log/messages.0.gz
27B	Sep 25 14:15	/var/log/wtmp.0.gz
27B	Sep 25 14:14	/var/log/wtmp.1.gz
3027B	Sep 25 14:13	/var/tmp/BSD.var.dist
0B	Sep 25 14:14	/var/tmp/LOCK_FILE
666B	Sep 25 14:14	/var/tmp/appidd_trace_debug

```

0B Sep 25 14:14 /var/tmp/eedebug_bin_file
34B Sep 25 14:14 /var/tmp/gksdchk.log
46B Sep 25 14:14 /var/tmp/kmdchk.log
57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
42B Sep 25 14:13 /var/tmp/pfe_debug_commands
0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
30B Sep 25 14:14 /var/tmp/policy_status
0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
Delete these files ? [yes,no] (no) yes
<
output omitted>

```

**NOTE:** If this command does not free up enough disk space, see [\[SRX\] Common and safe files to remove in order to increase available system storage](#) for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.4R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```

root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsr-x86-64-21.4-2021-10-12.0_RELEASE_21.4_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
x86-64-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsr-x86-64-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE signed by
PackageDevelopmentEc_2021 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:   This package will load JUNOS 21.4 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-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE.tgz

```

```

Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_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-21.4-2021-10-12.0_RELEASE_21.4_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-21.4-2021-10-12.0_RELEASE_21.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-21.4-2021-10-12.0_RELEASE_21.4_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-21.4-2021-10-12.0_RELEASE_21.4_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-21.4-2021-10-12.0_RELEASE_21.4_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 21.4R1 for vSRX.

**NOTE:** Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade, the original image is removed by default as part of the upgrade process.

## 6. Log in and use the show version command to verify the upgrade.

```

--- JUNOS 21.4-2021-10-12.0_RELEASE_21.4_THROTTLE Kernel 64-bit
JNPR-11.0-20211012.170745_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: 21.4-2021-10-12.0_RELEASE_21.4_THROTTLE
JUNOS OS Kernel 64-bit [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20211012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20211012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20211012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20211012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20211017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20211017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20211012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20211012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs compat32 [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20211017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx platform support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20211017.110007_ssd-builder_release_174_throttle]
JUNOS daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20211017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20211017.110007_ssd-builder_release_174_throttle]
JUNOS jail runtime [20211012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20211017.110007_ssd-builder_release_174_throttle]

```

## Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see [Validating the vSRX .ova File for VMware](#).



Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

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

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.4.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of 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.

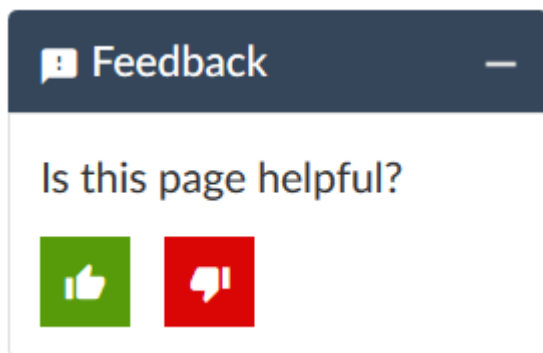
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#).

<https://pathfinder.juniper.net/compliance/>

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net). Include the document or topic name, URL or page number, and software version (if applicable)

## Requesting Technical Support

### IN THIS SECTION

- [Self-Help Online Tools and Resources | 217](#)
- [Creating a Service Request with JTAC | 217](#)

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net/>

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

## Creating a Service Request with JTAC

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

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

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

# Revision History

16 December 2021—Revision 1, Junos OS Release 21.4R1— ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

---

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 © 2021 Juniper Networks, Inc. All rights reserved.