

Release Notes: Junos[®] OS Release 15.1X49-D30 for the SRX Series

Release 15.1X49-D30
18 July 2017
Revision 9

Contents

Introduction	4
New and Changed Features	5
Release 15.1X49-D30 Hardware Features	5
SRX550 High Memory Services Gateway	5
SRX1500 Services Gateway	5
Release 15.1X49-D30 Software Features	5
AppSecure	5
Flow-Based and Packet-Based Processing	6
IP Monitoring	6
J-Web	7
Network Address Translation (NAT)	8
Platform and Infrastructure	8
Screen	8
Virtual Private Networks (VPNs)	9
Changes in Behavior and Syntax	10
Application Identification and Tracking	10
Chassis Cluster	10
CLI	11
Interfaces and Routing	11
Layer 2 Features	11
Screen	12
System Management	12
User Interface and Configuration	12
VPN	12
Known Behavior	13
Application Identification and Tracking	13
Attack Detection and Prevention (ADP)	13
Chassis Cluster	13
CLI	13
Flow-Based and Packet-Based Processing	14

Hardware	14
Interfaces and Routing	14
IP Monitoring	15
J-Web	15
Layer 2 Features	15
Network Address Translation (NAT)	15
Platform and Infrastructure	15
Security Policies	16
Software Installation and Upgrade	16
System Logging	16
VPN	16
Known Issues	17
Chassis Cluster	17
CLI	17
Dynamic Host Configuration Protocol (DHCP)	18
Flow-Based and Packet-Based Processing	18
J-Web	19
Network Address Translation (NAT)	19
Platform and Infrastructure	19
Routing Policy and Firewall Filters	19
Security Policies	19
Unified Threat Management (UTM)	20
Resolved Issues	20
Resolved Issues	20
Application Layer Gateways (ALGs)	20
Chassis Cluster	20
Flow-Based and Packet-Based Processing	21
Interfaces and Routing	22
Intrusion Detection and Prevention (IDP)	22
J-Web	22
Layer 2 Ethernet Services	22
Network Address Translation (NAT)	22
Platform and Infrastructure	22
Routing Policy and Firewall Filters	23
Routing Protocols	24
Switching	24
User Interface and Configuration	24
VPNs	24
Documentation Updates	24
Layer 2 Bridging and Transparent Mode for Security Devices	25
Migration, Upgrade, and Downgrade Instructions	25
Upgrade for Layer 2 Configuration	25
Upgrading an AppSecure Device	25
Network and Security Manager Support	26
Upgrade and Downgrade Scripts for Address Book Configuration	26
About Upgrade and Downgrade Scripts	26
Running Upgrade and Downgrade Scripts	27
Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases	28

Product Compatibility	29
Hardware Compatibility	29
Transceiver Compatibility for SRX Series Devices	29
Finding More Information	29
Documentation Feedback	30
Requesting Technical Support	30
Self-Help Online Tools and Resources	30
Opening a Case with JTAC	31
Revision History	32

Introduction

Junos OS runs on the following Juniper Networks[®] hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 15.1X49-D30 for the SRX Series. They describe new and changed features, known behavior, 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/techpubs/software/junos/>.



NOTE: Junos OS Release 15.1X49-D30 supports vSRX, SRX550 High Memory (SRX550M), and SRX1500 devices. Junos OS Release 15.1X49-D30 also supports SRX5400, SRX5600, and SRX5800 devices with host subsystems composed of either an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCBE (SCB2), or an SRX5K-RE-1800X4 (RE2) with an SRX5K-SCB3 (SCB3). Use the Junos OS Release 15.1X49-D30 Release Notes and the 15.1X49-D30 documentation for the supported platforms.

Junos OS Release 15.1X49-D30 does not support SRX5400, SRX5600, or SRX5800 devices with the following cards:

- SRX5K-40GE-SFP I/O Card (IOC1)
- SRX5K-4XGE-XFP I/O Card (IOC1)
- SRX5K-FPC-IOC Flex I/O card (Flex IOC1)
- SRX5K-RE-13-20 Routing Engine (RE1)
- SRX5K-SCB Switch Control Board (SCB1)
- SRX5K-SPC-2-10-40 Services Processing Card (SPC1)

Junos OS Release 15.1X49-D30 does not support SRX1400, SRX3400, or SRX3600 devices.

With the exception of SRX550M devices, Junos OS Release 15.1X49-D30 does not support SRX Series devices SRX100 through SRX650.

If you have any questions concerning this notification, please contact the Juniper Networks Technical Assistance Center (JTAC).

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 15.1X49-D30 for the SRX Series devices.

Release 15.1X49-D30 Hardware Features

SRX550 High Memory Services Gateway

- The SRX550M device is a large branch office gateway that combines security, routing, switching, and WAN interfaces for distributed enterprises. With advanced threat mitigation capabilities, the services gateway provides cost-effective and secure connectivity across distributed enterprise locations. The services gateway simplifies network complexity, protects and prioritizes network resources, and improves user and application experience.

The SRX550M device comes with 4 GB of DRAM memory and 8 GB of flash memory.

[See [SRX550 High Memory Services Gateway Description](#).]

- Starting in Junos OS Release 15.1X49-D30, the SRX550M expands the SRX Series family of next-generation security platforms. The SRX550M device supports 4 GB of DRAM and 8 GB of compact flash memory. All software features that were earlier supported on the SRX550 devices are supported on the SRX550M devices.

SRX1500 Services Gateway

- The SRX1500 Services Gateway is a midrange dynamic services gateway that consolidates security functionality, networking services, and uncompromised performance for small to medium enterprises. With advanced security and threat mitigation capabilities, the SRX1500 Services Gateway provides campus edge Integrated Security Appliance (ISA) support.

The SRX1500 Services Gateway is 1 rack unit tall with twelve 1 G Ethernet ports, four 1 G SFP ports, and four 10G SFP+ ports. The services gateway provides two slots for WAN Physical Interface Modules (PIMs), one slot for a solid-state drive (SSD) device, and two slots for power supplies.

[See [SRX1500 Services Gateway Overview](#).]

Release 15.1X49-D30 Software Features

AppSecure

- **SSL protocols support for SRX Series devices**—Starting with Junos OS Release 15.1X49-D30, the following SSL protocols are now supported on SRX Series devices along with TLS version 1.0:
 - TLS version 1.1—This enhanced version of TLS provides protection against cipher-block chaining (CBC) attacks.
 - TLS version 1.2—This enhanced version of TLS provides improved flexibility for negotiation of cryptographic algorithms.

Because of these change, the syntax of the **set services ssl termination profile profile-name protocol-version** command is changed as follows:

```
set services ssl termination profile profile-name protocol-version (all | tls1 | tls1.1 | tls1.2)
set services ssl initiation profile profile-name protocol-version (all | tls1 | tls1.1 | tls1.2)
```

[See [SSL Proxy Overview](#).]

- **CRL validation support for SSL proxy on SRX Series devices**—Starting with Junos OS Release 15.1X49-D30, SRX Series devices support certificate revocation list (CRL) validation support for server certificates in SSL proxy mode. A CRL contains the list of digital certificates that have been canceled before their expiration date. When a participating device uses a digital certificate, it checks the certificate signature and validity. It also acquires the most recently issued CRL and checks that the certificate serial number is not on that CRL.

CRL validation on SRX Series device involves checking for revoked certificates from servers. You can enable or disable the CRL validation to meet your specific security requirements. By default, CRL verification is enabled on any SSL proxy profile.

[See [SSL Proxy Overview](#).]

Flow-Based and Packet-Based Processing

- **Central point architecture enhancements for SRX5000 Line**—Starting in Junos OS Release 15.1X49-D30, the central point architecture is enhanced to handle higher concurrent sessions and connections per second (cps) for the SRX5000 line. The new central point architecture prevents data packets from going through the central point by offloading traffic management to SPUs. The system session capacity is extended, as the session limit on the central point is removed. The SPUs manage the IP action match and now there is no IP action match on the central point.

As mobile subscribers grow, mobile data usage and demand to support higher concurrent sessions and cps increase. The central point architecture can now support 2.5 million cps and 258 million concurrent sessions on the SRX5000 line with 11 SPCs.

[See [Understanding Enhancements to Central Point Architecture for the SRX5000 Line](#).]

IP Monitoring

- **Increasing IP monitoring capacity for SRX5000 Line Devices for IOC2 and IOC3**—Starting with Junos OS Release 15.1X49-D30, IOC2 and IOC3 on SRX5000 line devices support IP monitoring on both the primary and secondary nodes.

The following IOC2 MICs support IP monitoring:

- MIC with 20x1GE SFP Interfaces (SRX-MIC-20GE-SFP)— 20 ports
- MIC with 10x10GE SFP+ Interfaces (SRX-MIC-10XG-SFPP)—10 ports
- MIC with 1x100GE CFP Interface (SRX-MIC-1X100G-CFP)—1 port
- MIC with 2x40GE QSFP+ Interfaces (SRX-MIC-2X40G-QSFP)—2 ports

The following IOC3 support IP monitoring:

- SRX5K-MPC3-100G10G (2x100GE and 4x10GE ports)
- SRX5K-MPC3-40G10G (6x40GE and 24x10GE ports)

IP monitoring checks the end-to-end connectivity of configured IP addresses and allows a redundancy group to automatically fail over when the monitored IP address is not reachable through the reth interface. Both the primary and secondary nodes in the chassis cluster monitor specific IP addresses to determine whether an upstream device in the network is reachable.

[See [IP Monitoring Overview](#)]

J-Web

- **Support for J-Web for the SRX1500**—Starting with Junos OS Release 15.1X49-D30, J-Web is supported on the SRX1500.
- **J-Web GUI improvements for the SRX1500**—The following usability improvements are incorporated:
 - Home page:
 - a. Title bar displays the Juniper logo, hostname, username, and Help icon.
 - b. Taskbar now has six tabs (Dashboard, Configure, Monitor, Maintain, Troubleshoot, and Commit).
 - Dashboard tab—A **Show Rear View** button is added on the right side of Chassis View for easy switching between front and rear views.
 - Configure and Monitor tab—Overall layouts have been enhanced.
- The Configure>Security>UTM>Anti-Virus has the Sophos Engine Type option only.
- The Configure>Security>UTM>Web Filtering page no longer includes the Surf Control Integrated option.
- All occurrences of *Bridge Domain* and *Bridge Options* are now replaced with *VLAN*.
- The following changes are made to the Configuring Network Interfaces Page:
 - *Bridge* is replaced with *Ethernet Switching*.
 - *Port mode* is replaced with *Interface mode*.

Network Address Translation (NAT)

- **Central point architecture enhancements for NAT for SRX5000 Line**—Starting in Junos OS Release 15.1X49-D30, the central point architecture can handle higher system session capacity and session ramp-up rate for the SRX5000 line, which were previously limited by the central point memory capacity and CPU capacity. Hence, the workload on the central point is reduced to increase the session capacity and to support more sessions to achieve higher connections per second (cps).

[See [Understanding Central Point Architecture Enhancements for NAT](#) and [Understanding Reverse NAT Enhancements for Central Point Architecture](#).]

Platform and Infrastructure

- **SRX1500 Services Gateway**—Starting in Junos OS Release 15.1X49-D30, the SRX1500 Services Gateway expands the SRX Series family of next-generation security platforms. The SRX1500 Services Gateway is a midrange, dynamic services gateway that consolidates security functionality, networking services, and uncompromised performance for small to medium enterprises. The SRX1500 replaces the SRX650 and SRX1400 devices. The SRX1500 supports the following software features:
 - Routing policies with multicast
 - QoS and network services
 - Stateful firewall
 - IPsec VPN, AutoVPN, AES-GCM
 - AppSecure suite
 - IDP
 - UTM (Sophos AV, Web filtering, antispam)
 - Chassis cluster
 - J-Web
 - Advanced anti-malware
- **Secure Boot (SRX1500)**—Junos OS Release 15.1X49-D30 introduces a significant system security enhancement: Secure Boot. The Secure Boot implementation is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, the bootloader, and the kernel are cryptographically protected. No action is required to implement Secure Boot.

Screen

- **Central point architecture enhancement for screens for SRX5000 Line**—Starting in Junos OS Release 15.1X49-D30, the central point session and central point packet processing are handled by the SPU instead of the central point for the SRX5000 line. This change impacts the statistic and signature screen functionalities. The SPU now handles all screen-related actions, including statistic counter, logs, and SNMP trap.

[See [Understanding Central Point Architecture Enhancements for Screens](#).]

- **Improved logging and trapping for SRX Series devices**—Starting with Junos OS Release 15.1X49-D30, the system log information for IP-based session limits is enhanced to include more information. Each session-limit screen log now contains five tuples of information. The hard core screen SNMP trap interval can now be configured in the range from 1 second to 3600 seconds. The default interval is 2 seconds.

[See [Understanding Source-Based Session Limits](#)]

Virtual Private Networks (VPNs)

- **Copying outer IP header DSCP and ECN to inner IP header for SRX5400, SRX5600, and SRX5800 devices and vSRX instances**—Starting with Junos OS Release 15.1X49-D30, copying the Differentiated Services Code Point (DSCP) from the outer IP header to the inner IP header type of service (ToS) field is supported.

This feature is supported on IPv4 and IPv6 and in chassis cluster mode.

The benefit in enabling this feature is that after IPsec decryption, clear text packets can follow inner CoS (DSCP+ECN) rules. When you enable this feature on a VPN object, the corresponding IPsec security association (SA) is cleared and reestablished.

By default, this feature is disabled.

- To enable the feature:

```
set security ipsec vpn vpn-name copy-outer-dscp
```

- To disable the feature:

```
delete security ipsec vpn vpn-name copy-outer-dscp
```

- To verify whether the feature is enabled or not:

```
show security ipsec security-associations detail
```

[See [Copying Outer IP Header DSCP and ECN to Inner IP Header](#)]

- Related Documentation**
- [Changes in Behavior and Syntax on page 10](#)
 - [Known Behavior on page 13](#)
 - [Known Issues on page 17](#)
 - [Resolved Issues on page 20](#)
 - [Documentation Updates on page 24](#)
 - [Migration, Upgrade, and Downgrade Instructions on page 25](#)

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X49.

Application Identification and Tracking

- On SRX Series devices, the following CLI statements are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

edit services ssl termination profile *profile-name* protocol-version ssl3

edit services ssl initiation profile *profile-name* protocol-version ssl3
- On SRX1500 devices, AppSecure is part of Juniper Networks Secure Edge software (a default shipping software package on the SRX1500). A separate license key is not required on your device to download and install the AppID signature database updates, or to use other AppSecure features such as AppFW, AppQoS, and AppTrack.

Chassis Cluster

- When an SRX Series device is operating in chassis cluster mode and encounters any IA-chip access issue in an SPC or an I/O Card (IOC), a minor FPC alarm will be activated to trigger redundancy group failover.
- Starting in Junos OS Release 15.1X49-D20, for all SRX Series devices, reth interface supports proxy ARP.

CLI

- Starting in Junos OS Release 15.1X49-D30, when you upgrade from an existing release to Junos OS Release 15.1X49-D30, the following CLI commands will run with a no-op and a warning message is displayed that the configuration is obsolete:

```
set security forwarding-process application-services session-distribution-mode hash-based
```

```
set security forwarding-process application-services session-distribution-mode normal
```

```
set security forwarding-process application-services maximize-cp-sessions
```

Interfaces and Routing

- GRE keepalive time feature for SRX Series devices**—Starting in Junos OS Release 15.1X49-D30, the GRE keepalive time feature is supported on the GRE tunnel interface. You can configure the keepalives on a GRE tunnel interface using the **keepalive-time** and **hold-time** commands at the [edit protocols oam gre-tunnel interface interface-name] hierarchy level.

Layer 2 Features

- Enhanced Layer 2 CLI**—Starting with Junos OS Release 15.1X49-D10, enhanced Layer 2 CLI configurations are supported on SRX5400, SRX5600, and SRX5800 devices. Legacy Layer 2 transparent mode configuration statements and operational commands are not supported. If you enter legacy configurations in the CLI, the system displays an error and fails to commit the configurations.

For example, the following configurations are no longer supported:

- set bridge-domain**
- set interfaces ge-1/0/0 unit 0 family bridge**
- set vlans vlan-1 routing-interface**

Use the SRX L2 Conversion Tool to convert Layer 2 CLI configurations to enhanced Layer 2 CLI configurations.

The SRX L2 Conversion Tool is available at <http://www.juniper.net/support/downloads/?p=srx5400#sw>.

For more information, refer to the Knowledge Base article at <http://kb.juniper.net>.

[See [Enhanced Layer 2 CLI Configuration Statement and Command Changes](#).]

Screen

- In Junos OS releases earlier than Junos OS Release 15.1X49-D20, the firewall generates a log for every packet that exceeds the source-ip-based or destination-ip-based threshold and triggers the source or destination session limit. This can lead to a flood of logs if a large number of packets is received every second after the threshold has been reached. For example, if the source or destination session limit has been reached and 100 additional packets arrive in the next second, 100 log messages are sent to the system log server.

Starting in Junos OS Release 15.1X49-D20, the firewall generates only one log message every second irrespective of the number of packets that trigger the source or destination session limit.

This behavior also applies to flood protection screens with TCP-Synflood-src-based, TCP-Synflood-dst-based, and UDP flood protection.

System Management

- During a load override, to enhance the memory for the commit script, you must load the configuration by applying the following commands before the commit step:
set system scripts commit max-datasize 800000000
set system scripts op max-datasize 800000000
- On all SRX Series devices in transparent mode, packet flooding is enabled by default. If you have manually disabled packet flooding with the **set security flow bridge no-packet-flooding** command, then multicast packets such as OSPFv3 hello packets are dropped.

User Interface and Configuration

- You can configure only one rewrite rule for one logical interface. When you configure multiple rewrite rules for one logical interface, an error message is displayed and the commit fails.

VPN

- Dynamic VPN is not supported in Junos OS 15.1X49 releases. Dynamic VPN is supported only in Junos OS Releases 12.3X48 and earlier on SRX100, SRX210, SRX220, SRX240, SRX550, and SRX650 devices.

Related Documentation

- [New and Changed Features on page 5](#)
- [Known Behavior on page 13](#)
- [Known Issues on page 17](#)
- [Resolved Issues on page 20](#)
- [Documentation Updates on page 24](#)

- [Migration, Upgrade, and Downgrade Instructions on page 25](#)

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D30.

Application Identification and Tracking

- The application quality of service (AppQoS) feature is supported SRX5K-40GE-SFP I/O Card (IOC) and not supported on SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), and SRX5K-MPC3-40G10G (IOC3).
- On SRX Series devices, when you change the timeout value for the application system cache entries using the command **set services application-identification application-system-cache-timeout**, the cache entries need to be cleared to avoid inconsistency in timeout values of existing entries.

Attack Detection and Prevention (ADP)

- On all high-end SRX Series devices, the first path signature screen is performed first, followed by the fast path bad-inner-header screen.
- On all SRX Series devices, when a packet allow or drop session is established, the bad-inner-header screen is performed on every packet, because this screen is a fast path screen.

Chassis Cluster

- On SRX1500 devices in a chassis cluster, configuring LACP on a redundant Ethernet interface (reth) is not supported.
- On SRX1500 devices in a chassis cluster, using copper cables for connecting control ports is not supported. We recommend using 1-Gigabit Ethernet fiber cabling for connecting control ports between the nodes in a chassis cluster.

CLI

- On SRX5000 line devices, the following CLI statement is deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration:

```
set chassis fpc <fpc-slot> services offload
```

The following new CLI statement replaces the deprecated CLI statement:

```
set chassis fpc <fpc-slot> np-cache
```

- On SRX1500 devices, when the **show class-of-service interface <interface_name> | display.xml** command is executed, there is a change in the XML fields. Previously, the following was displayed: <i-logical-objects> <i-logical-object-type> <i-logical-object-name> <i-logical-object-subtype> <i-logical-object-index>

```
<i-logical-object-type> <i-logical-object-name> <i-logical-object-subtype>
<i-logical-object-index>.
```

Starting in Junos OS Release 15.1X49-D30, the following is displayed: <cos-objects>
<cos-object-type> <cos-object-name> <cos-object-subtype> <cos-object-index>
<cos-object-type> <cos-object-name> <cos-object-subtype> <cos-object-index>.

Flow-Based and Packet-Based Processing

- On SRX1500 devices, packet handling is only supported in polling mode; this scenario might cause high CPU usage.

Hardware

- On SRX550M devices, Layer 2 switching features are not supported.

Interfaces and Routing

- On SRX1500 devices, when the CPU utilization is very high (more than 95 percent), the connection between the aamw process and the pkid process breaks. When this situation occurs, the aawm process remains in initializing state until the connection is established.
- On SRX1500 devices, IPv6 might not work if the interface is configured in a virtual routing instance and inet6 is the only family configured on the interface. As a workaround, when an interface is configured in a routing instance with family inet6, the family inet should also be configured to avoid this issue.
- On SRX1500 devices, when SecIntel sends a data feed to the Packet Forwarding Engine card, the log message prints out an incorrect message indicating that the data feed is loaded to pic-1 instead of pic-0.
- On SRX1500 devices, by default, the speed of gr-0/0/0 interface is 800mbps.

```
user@host# run show interfaces gr-0/0/0
```

```
Physical interface: gr-0/0/0, Enabled, Physical link is Up
Interface index: 143, SNMP ifIndex: 517
Type: GRE, Link-level type: GRE, MTU: Unlimited, Speed: 800mbps
Link flags      : Scheduler Keepalives DTE
Device flags    : Present Running
Interface flags : Point-To-Point
Input rate      : 0 bps (0 pps)
Output rate     : 0 bps (0 pps)
```

When the interface speed exceed 100mbps, we use 100mbps to calculate CoS buffer allocation. For gre interface of SRX1500 device, we use 100mbps to calculate CoS buffer allocation.

For Example: Expected total Buffer = 1000000000 bits * 0.1 = 100000000 --> so
100m * 0.1 = 10000000

IP Monitoring

- On SRX5400, SRX5600, and SRX5800 devices, IP monitoring does not support MIC online/offline status.

J-Web

- On SRX1500 devices in a chassis cluster, when you use J-Web to configure and commit a configuration, ensure that all the other user sessions are logged out, including any CLI sessions.

Layer 2 Features

- **Layer 2 Bridging and Transparent Mode**— On all SRX Series devices, bridging and transparent mode are not supported on Mini-Physical Interface Modules (Mini-PIMs).

Network Address Translation (NAT)

- On high-end SRX Series devices, the number of IP addresses for NAT with port translation has been increased to 1M addresses since Junos OS Release 12.1X47-D10. The SRX5000 line, however, supports a maximum of 384M translation ports and cannot be increased. To use 1M IP addresses, you must confirm that the port number is less than 384. The following CLI commands enable you to configure the twin port range and limit the twin port number:
 - `set security nat source pool-default-twin-port-range <low> to <high>`
 - `set security nat source pool sp1 port range twin-port <low> to <high>`

Platform and Infrastructure

- The following software features are not supported on the SRX1500 Services Gateway:
 - Logical system
 - Secure wire with Layer 2 mode
 - Remote access VPN
 - FPGA Express Path
 - System snapshot
 - Packet mode and MPLS
 - On-box logging and reporting
 - Chassis cluster control link encryption
 - Unified ISSU
 - Layer 2 switching features
 - PPPoE

- On all high-end SRX Series devices, when you enable a global services offloading policy, the connections per second (cps) might be affected. You can use an IOC3 card to offload more sessions, or lower the session amount to ensure that the IOC2 is capable of handling it. As a workaround, identify the sessions that must be offloaded and only enable services offloading on those sessions.

Security Policies

- On SRX1500 devices, you cannot configure the aamw process with an action block and IDP together in the same firewall policy. However, you can still configure the aamw process with an action permit and IDP together in the same firewall policy.

Software Installation and Upgrade

- In-Service Software Upgrade (ISSU) is not supported for upgrading from earlier Junos OS releases to Junos OS Release 15.1X49. ISSU is supported for upgrading to successive Junos OS Release 15.1X49 releases and to major Junos OS releases.
- On all high-end SRX Series devices, unified ISSU is supported from Junos OS Release 12.1X45 to Junos OS Release 12.1X46 and from Junos OS Release 12.1X46 to Junos OS Release 15.1X49-D10. Unified ISSU is not supported from Junos OS Release 12.1X45 to Junos OS Release 15.1X49-D10.

System Logging

- If an attack is detected by the central point, a system log message is sent per second. If an attack is detected by the distributed central point, a system log message is sent per second per SPU; the number of SPUs define the number of system log messages per second.

VPN

- On a high-end SRX Series device, VPN monitoring of an externally connected device (such as a PC) is not supported. The destination IP address for VPN monitoring must be a local interface on the high-end SRX Series device.
- On SRX Series devices, configuring RIP demand circuits over VPN interfaces is not supported.

Related Documentation

- [New and Changed Features on page 5](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Issues on page 17](#)
- [Resolved Issues on page 20](#)
- [Documentation Updates on page 24](#)
- [Migration, Upgrade, and Downgrade Instructions on page 25](#)

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D30.

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

Chassis Cluster

- On all high-end SRX Series devices in a chassis cluster, the dhcp server loses the client information after failover. However, the pool information is not lost, so clients can get new addresses from the server. The issue happens only once during the failover. [PR1097132](#)
- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when you simultaneously reboot both the nodes of the device, the secondary node cannot respond after reboot until the IOCs on the other node are online.
As a workaround, reboot the secondary node 3 minutes after rebooting the primary node or after all FPCs on the primary node become online, whichever is shorter. [PR1104249](#)
- On all high-end SRX Series devices in a chassis cluster, the G-ARP is not sent with a static MAC address when chassis cluster failure occurs.
As a workaround do the following:
 1. Create a new sample redundancy group, move the reth interface (which has mac-address changed or configured) into the new sample redundancy group, and commit.
 2. Move the reth interface back to its original redundancy group as per your configuration, deactivate the sample redundancy group, and commit. (When you move reth to a new redundancy group, its MAC address is refreshed with the configured address.) [PR1115596](#)
- On all high-end SRX Series devices in a chassis cluster, after reboot if the secondary node (RG1) claim cold synchronize (CS) completes first, this might result in bidirectional RTO synchronization or incorrect direction for RTO synchronization.
As a workaround, when you reboot the device, set the reboot for the secondary node to occur 3 minutes after the primary cold node reboots, or after all FPCs on the primary node become online, whichever is shorter. [PR1138502](#)
- On SRX1500 devices acting as the primary node in a chassis cluster, when the FPCs go offline because of hardware failure on a node, traffic might be impacted until the data plane recovers. [PR1144996](#)

CLI

- On SRX5400, SRX5600, and SRX5800 devices, ICMP Out Errors with a rate of 10,000 per second are generated when you issue the `show snmp mib get decimal 1.3.6.1.2.1.5.15.0` command. [PR1063472](#)

- On SRX1500 devices, when the dual power modules are plugged in, and one of them does not have power, the **show chassis hardware** command displays the wrong power module status. [PR1138203](#)

Dynamic Host Configuration Protocol (DHCP)

- On all SRX Series devices configured as a DHCP server (using the `jdhcpd` process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (`authd`), the `jdhcpd` process communicates with `authd` process twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the `authd` process will indefinitely wait for the second authentication request. However, the `jdhcpd` process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the `authd` process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. [PR1042818](#)
- On SRX1500 devices, when the **show dhcpv6 client** command is issued, the CLI hangs after restarting the DHCP service with DHCPv6 clients. As a workaround, do not use the **restart dhcp-service** command when the DHCPv6 client interface still has an IPv6 address. [PR1142711](#)
- On SRX1500 devices, after you commit the DHCPv6 configuration, the DHCPv6 relay might not work, because the reply packet is dropped. [PR1142727](#)
- On SRX1500 devices, when multiple interfaces end up having the same DUID-EN format for the DHCPv6 client interface, some interfaces might not receive the address information from the DHCP server. [PR1142768](#)

Flow-Based and Packet-Based Processing

- On all high-end SRX Series devices, in some scenarios, the `flowd` process might generate core files due to stack overflow while running a log collection script on the device. [PR1020739](#)
- On all high-end SRX Series devices, the wrong IP information **Unknown IP version: 0** is displayed in some load-balancing thread (LBT) and packet-ordering thread (POT) logs that are triggered by fragmentation. [PR1032647](#)
- On SRX5400, SRX5600, and SRX5800 devices with an SRX5K IOC II, configuring a sampling feature (flow monitoring) might cause high kernel heap memory usage. [PR1033359](#)
- On all high-end SRX Series devices, when verifying the connections per second (cps) value using SNMP MIB walk `nxJsNodeSessionCreationPerSecond`, the device-polling mechanism gives a cps value that is an average of the values within the past 96 seconds. If the cps value is not constant, the reported cps number might not exactly equal the actual cps value. [PR1109767](#)
- On all high-end SRX Series devices, for a device running NAT traffic in high stress conditions, continuous chassis cluster failover might result in a minor central point session leak. However, other than the wasted sessions caused by the leak, this issue has no other effects on the device. [PR1124695](#) and [PR1141695](#)

J-Web

- On SRX5400, SRX5600, and SRX5800 devices, in J-Web, the contents of the DHCP monitor page are not visible, because the page is missing. [PR1148026](#)

Network Address Translation (NAT)

- On all high-end SRX Series devices in a chassis cluster, when NAT with port-block allocation is configured, duplicate system log messages might be generated for each port-block allocation and release. [PR1118563](#)

Platform and Infrastructure

- On SRX1500 devices, when the **request system power-off** command is executed, the system does not power off. You should physically power off the system. [PR1137960](#)
- On SRX1500 devices, when one of the fans fail, the system generates a major alarm and a system log message is generated. However, the state LED and the alarm LED are both shown as OFF instead of red. [PR1142191](#)
- On SRX1500 devices, when GR tunnel or IP tunnel queue shaping is enabled with the **set chassis fpc 0 pic 0 tunnel-queuing** command, some of the interfaces remain down because of fpc0 pic bounce. [PR1144474](#)
- On SRX1500 devices, when RPM probe is configured for hardware-timestamp, probes are dropped by the RPM probe source (client).
As a workaround, when you configure the RPM probe client, skip the hardware-timestamp configuration. [PR1147156](#)

Routing Policy and Firewall Filters

- On all high-end SRX Series devices, if there are two routing instances of instance type default and virtual router, when you change the instance type of one routing instance from default to virtual router after the routing policy is configured, the route is missing from the second routing instance.
As a workaround, deactivate the first routing instance and the routing policy, and then activate the first routing instance to correct the issue. [PR969944](#)
- On all high-end SRX Series devices, during route deletion on Packet Forwarding Engine, next-hop entries might not be deleted, these stale next-hops may continue to be used by sessions resulting in flowd process crash. [PR1017037](#)

Security Policies

- On all high-end SRX Series devices, the log buffer size is expanded to 30,000 in event mode. When the log buffer size was 1000, the Packet Forwarding Engine generated logs burst when there were more than 30 entries and more logs were dropped.
As a workaround, use the stream mode instead of the event mode for sending RTLOG. [PR1133757](#)

- On SRX1500 devices, the security intelligence block-drop action for C and C policy for custom_url_data feed does not work. [PR1141745](#)

Unified Threat Management (UTM)

- On all SRX Series devices, when the size of an attachment is larger than 20 MB, the SMTP antivirus scanning of UTM fails to transfer the attached file. [PR838503](#)
- On all high-end SRX Series devices, under high connections per second (cps) and UTM Sophos antivirus traffic, the device might ramp up to 99 percent CPU usage because of a central lock of object cache memory allocation. There is no clear boundary, because the allocation race condition varies.
As a workaroud, reducing traffic cps might lower the high CPU usage. [PR967739](#)

Related Documentation

- [New and Changed Features on page 5](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Behavior on page 13](#)
- [Resolved Issues on page 20](#)
- [Documentation Updates on page 24](#)
- [Migration, Upgrade, and Downgrade Instructions on page 25](#)

Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

Resolved Issues

Application Layer Gateways (ALGs)

- On all SRX Series devices with the H.323 ALG enabled, if dual NAT (the packets in the same call receive different NAT rules bidirectionally) is enabled, then the destination NAT for the payload is skipped during ALG processing. For example, the address payload in the H.225 gatekeeper confirm packet is not translated by the H.323 ALG. [PR1100638](#)

Chassis Cluster

- On all SRX Series devices in a chassis cluster, when you disable the member interface of a redundant Ethernet (reth) interface, and if the interface disabling action causes the related redundancy group failover, such as, the only member interface under reth interface on the primary node is disabled, or the number of operating member interfaces under a link aggregation group (LAG) redundant Ethernet (reth) interface on the primary node falls below the configured value of minimum-links, then the reth interface will flap. [PR1111360](#)

- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster with SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), or SRX5K-MPC3-40G10G (IOC3) installed, when VLAN tagging is configured on the reth interface and LACP is enabled, and if the logical reth interfaces with VLAN tagged are configured within separate security zones, then the LACP protocol fails. [PR1128355](#)

Flow-Based and Packet-Based Processing

- On all high-end SRX Series devices configured with chassis cluster and logical systems (LSYS), when the session number is close to the configured LSYS session limit, sessions might not be successfully created on the secondary node. The sessions will be created on the backup flow SPUs, but not on the central point. As a result, the backup flow SPUs will keep retrying until the SPUs are successful. When this situation continues, the session limit on the secondary node's SPU will reach the maximum limit value and this will affect the new session creation. (Note: The number of sessions on the secondary node SPU is usually higher than on the primary node SPU). [PR1061067](#)
- On all SRX Series devices, if 1:1 sampling is configured for J-Flow and the device processes a high volume of traffic, a race condition of an infinite loop of J-Flow entry deletion might be encountered, As a result, the flowd process crashes. [PR1088476](#)
- On all high-end SRX Series devices, if Services Offloading is enabled, in certain cases, such as packets flowing on an LAG interface or fragmented packets processing, duplicated packets might be randomly generated and forwarded out of the device. [PR1104222](#)
- On all SRX Series devices, if equal-cost multipath (ECMP) routing is configured, in a race condition of ECMP route updating, the flowd process might crash. [PR1105809](#)
- On all high-end SRX Series devices with IPsec VPN configured, if traffic is transmitted from one VPN tunnel to another VPN tunnel, and these two VPN tunnels are anchored on different SPUs, then this VPN traffic might be forwarded in a loop between these two SPUs. [PR1110437](#)
- On all SRX Series devices (except the SRX110) in a chassis cluster, when ECMP is configured across the interfaces on both nodes, packets are dropped intermittently. [PR1123543](#)
- On all SRX Series devices with multi-threaded forwarding engines that have the **tcp-session strict-syn-check** feature enabled, the initial packets of a TCP session might be dropped due to a race condition. [PR1130268](#)

Interfaces and Routing

- On all high-end SRX Series devices, when you modify a security zone that has many interfaces (for example, when adding or deleting an interface in such a zone), an abnormally high CPU load might occur upon commit. [PR1131679](#)

Intrusion Detection and Prevention (IDP)

- On all high-end SRX Series devices with IDP SSL inspection enabled, traffic with an RSA key size more of than 2000 might cause high CPU usage and performance degradation on the data plane. [PR1125387](#)

J-Web

- On all SRX Series devices in J-Web, the **default** option under **Security > Logging > Application Tracking** is enabled. This setting enables application tracking if any system log configuration is saved. [PR1106629](#)
- On all high-end SRX Series devices, when a logical system (LSYS) user logs in to J-Web, changes the configuration, and clicks the Compare button, the result window does not pop up. [PR1115191](#)

Layer 2 Ethernet Services

- On all SRX Series devices, if the device acts as a DHCP server using the jdhcpd process and if the DHCP client sends a discover message with a requested IP address, then the authd process uses the requested IP address to find the pool with priority. This causes the device to assign an IP address from an incorrect DHCP pool to the DHCP client when there is a DHCP pool that shares the same subnet with the requested IP address. However, it is not the expected pool of the DHCP client. [PR1097909](#)

Network Address Translation (NAT)

- On all high-end SRX Series devices, when NAT with PBA (port-block allocation) is configured on the device cluster, duplicate system log messages are generated for each port-block allocation and release. [PR1118563](#)

Platform and Infrastructure

- On all SRX Series devices, when SNMPv3 privacy and authentication passwords are set and updated, NSM fails to push the update to the device that is managed by NSM. [PR1075802](#)
- On all high-end SRX Series devices, the chassis cluster LED changes to amber after RGO failover, but the CLI indicates it is green. [PR1085597](#)
- On all high-end SRX Series devices, an SPU might become inaccessible from the Routing Engine because of a memory-buffer counter corruption. Because of this issue, a service outage occurs in certain scenarios, for example, when IPsec is configured with certificate-based authentication. [PR1102376](#)

- On all high-end SRX Series devices, starting in Junos OS Release 12.3X48-D20, the **set chassis fpc num sampling-instance name** command is required for J-Flow version 9 configuration. However, the commit fails when the **set chassis fpc num sampling-instance name** command is configured. [PR1108371](#)
- On all high-end SRX Series devices, you cannot configure more than one lt-0/0/0.x interface per logical systems (LSYS) on the following Junos OS maintenance releases:
 - 12.1X44-D35 through 12.1X44-D55
 - 12.1X46-D25 through 12.1X46-D40
 - 12.1X47-D10 through 12.1X47-D25
 - 12.3X48-D10 through 12.3X48-D15
 - 15.1X49-D10 through 15.1X49-D20You can configure more than one lt-0/0/0.x interface per LSYS if you have no interconnect LSYS configured. If the interconnect LSYS is configured, then you can have only one lt-0/0/0.x interface per LSYS. The issue is fixed in the following Junos OS maintenance releases: 12.1X44-D60, 12.1X46-D45, 12.1X47-D30, 12.3X48-D20, and 15.1X49-D30. [PR1121888](#)

Routing Policy and Firewall Filters

- When polling the following OIDs through SNMP, file Descriptor leak might be seen during the nsd process.
 - jnxLsysSpCPSummary
 - jnxLsysSpSPUSummary
 - jnxLsysSpCPUEntry
 - jnxLsysSpCPUTable

[PR1079629](#)

[Routing Protocols](#)

- On all SRX Series devices, if the device acts as a rendezvous point (RP) in a multicast environment and if the interface of the RP is configured in a custom logical system (LSYS) or routing instance, then the register-stop messages might be incorrectly sent out from the root LSYS or routing instance instead of from the custom LSYS or routing instance. [PR1062305](#)

[Switching](#)

- On all SRX Series devices, when you connect to the device through wireless AP the secure access port incorrectly allows access to the MAC addresses that are not in the list of allowed MAC addresses. [PR587163](#)

[User Interface and Configuration](#)

- On all SRX Series devices, when you commit the traffic selector (TS) configuration, it might fail and an ffp core file might be generated. [PR1089676](#)

[VPNs](#)

- On all high-end SRX Series devices, when the **alarm-without-drop** option is configured for the UDP Flood Protection screen, packets classified as attack packets might be sent out of order. This can result in performance degradation. [PR1090963](#)
- On all SRX Series device, if there are lots of IPsec VPNs configured, any configuration committing related to IPsec VPN might cause a pause in the kmd process, which might cause Dead-Peer-Detection (DPD) timeout and VPN tunnel renegotiation. [PR1129848](#)
- On all high-end SRX Series devices, downloading a large CRL over LDAP fails in some conditions, causing high CPU usage on the Routing Engine. [PR1130164](#)

Related Documentation

- [New and Changed Features on page 5](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Behavior on page 13](#)
- [Known Issues on page 17](#)
- [Documentation Updates on page 24](#)
- [Migration, Upgrade, and Downgrade Instructions on page 25](#)

[Documentation Updates](#)

This section lists the errata and changes in the software documentation.

Layer 2 Bridging and Transparent Mode for Security Devices

- Starting in Junos OS Release 15.1X49-D10, the *Layer 2 Bridging and Switching Feature Guide for Security Devices* guide is retitled to *Layer 2 Bridging and Transparent Mode for Security Devices*.
- Although Ethernet switching is not supported in Junos OS Release 15.1X49-D10, the *Layer 2 Bridging and Transparent Mode for Security Devices* guide retains content about Ethernet switching.
- Starting in Junos OS Release 15.1X49-D10, the term *bridge-domain* is changed to *VLAN*. However, the documents still use the term *bridge-domain* in topics.

Related Documentation

- [New and Changed Features on page 5](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Behavior on page 13](#)
- [Known Issues on page 17](#)
- [Resolved Issues on page 20](#)
- [Migration, Upgrade, and Downgrade Instructions on page 25](#)

Migration, Upgrade, and Downgrade Instructions

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.

- [Upgrade for Layer 2 Configuration on page 25](#)
- [Upgrading an AppSecure Device on page 25](#)
- [Network and Security Manager Support on page 26](#)
- [Upgrade and Downgrade Scripts for Address Book Configuration on page 26](#)

Upgrade for Layer 2 Configuration

Starting with Junos OS Release 15.1X49-D10 and later, enhanced Layer 2 CLI configurations are supported. If your device was configured earlier for Layer 2 transparent mode, then you must convert the legacy configurations to enhanced Layer 2 CLI configurations.

For details on how to migrate from Junos OS Release 12.3X48-D10 and earlier releases to Junos OS Release 15.1X49-D10 and later releases, refer to the Knowledge Base article at <http://kb.juniper.net>.

Upgrading an AppSecure Device

For devices implementing AppSecure services, use the **no-validate** option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the

configuration file to a signature database. This change in location can trigger an error during the validation step and interrupt the Junos OS upgrade. The **no-validate** option bypasses this step.

Network and Security Manager Support

Network and Security Manager (NSM) support for SRX Series Services Gateways with Junos OS 15.1X49-D10 is available only with NSM versions 2012.2R6 / 2012.1R10 and later. For additional information, see the [Network and Security Manager](#) documentation.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see [Figure 1 on page 27](#)).

- [About Upgrade and Downgrade Scripts on page 26](#)
- [Running Upgrade and Downgrade Scripts on page 27](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 28](#)

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.
- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

After upgrading to the zone-attached address book configuration:

- You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
- You cannot configure address books using the J-Web interface.

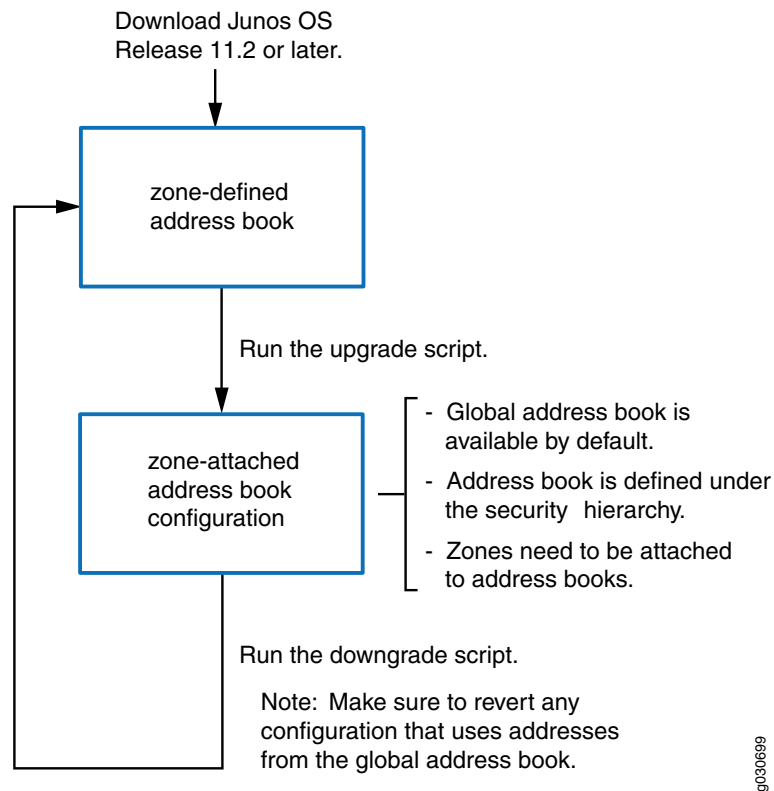
For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.



NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to

convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.



NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 <http://www.juniper.net/support/eol/junos.html>.

For additional information about how to upgrade and downgrade, see the [Installation and Upgrade Guide for Security Devices](#).

Related Documentation

- [New and Changed Features on page 5](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Behavior on page 13](#)
- [Known Issues on page 17](#)
- [Resolved Issues on page 20](#)

Product Compatibility

This section lists the product compatibility for any Junos SRX mainline or maintenance release.

- [Hardware Compatibility on page 29](#)
- [Transceiver Compatibility for SRX Series Devices on page 29](#)

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <http://pathfinder.juniper.net/feature-explorer/>.

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Finding More Information

For the latest, most complete information about known and resolved issues with the Junos OS, see the Juniper Networks Problem Report Search application at <http://prsearch.juniper.net>.

For regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products, see the [Juniper Networks Compliance Advisor](#).

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at <http://pathfinder.juniper.net/feature-explorer/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC 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.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- 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, visit us at <http://www.juniper.net/support/requesting-support.html>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at <http://www.juniper.net/techpubs/feedback/>.

Revision History

- 18, July 2017—Revision 9— Junos OS 15.1X49-D30 – SRX Series.
- 21, March 2017—Revision 8— Junos OS 15.1X49-D30 – SRX Series.
- 12, January 2017—Revision 7— Junos OS 15.1X49-D30 – SRX Series.
- 15, November 2016—Revision 6— Junos OS 15.1X49-D30 – SRX Series.
- 27, July 2016—Revision 5— Junos OS 15.1X49-D30 – SRX Series.
- 12, April 2016—Revision 4— Junos OS 15.1X49-D30 – SRX Series.
- 22, March 2016—Revision 3— Junos OS 15.1X49-D30 – SRX Series.
- 28, December 2015—Revision 2— Junos OS 15.1X49-D30 – SRX Series.
- 10, December 2015—Revision 1— Junos OS 15.1X49-D30 – SRX Series.

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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.