Release Notes: Junos® OS Release 15.1X49-D110 for the SRX Series

Release 15.1X49-D110
28 January 2019
Revision 6

Contents

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-D110 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/documentation/software/junos/.

NOTE: Junos OS Release 15.1X49-D110 supports the following devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M), SRX1500, SRX4100, SRX4200, 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), and vSRX.

For more details about SRX 5400, SRX5600, and SRX5800 devices hardware and software compatibility, please see https://kb.juniper.net/KB30446. 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-D110 for the SRX Series devices.

Release 15.1X49-D110 Hardware Features

Hardware

- **SRX345 Services Gateway (with dual AC power supplies)—**The SRX345 Services Gateway now includes a model with dual AC power supplies for power redundancy. The power supplies are internal and are not field-replaceable. The dual AC model supports the same features as those supported on the existing SRX345 Services Gateway with a single AC power supply. The minimum Junos OS release supported on the dual AC model is 15.1X49-D110.

  [See SRX345 Services Gateway Description.]

Release 15.1X49-D110 Software Features

High Availability

- **Support for Dedicated Bidirectional Forwarding Detection (BFD)**—Starting with Junos OS Release 15.1X49-D110, dedicated microkernel is now supported on SRX550M; in addition to existing support on SRX340, SRX345, and SRX1500 to improve BFD performance. This is an enhancement to the distributed mode. Enabling dedicated microkernel completely offloads the BFD daemon to the Packet Forwarding Engine (PFE) microkernel by dedicating one CPU core to this process. This significantly improves the BFD failure detection performance. Since we are allocating one of the PFE CPU core to the BFD daemon as a result, the device throughput performance is reduced.

  To enable dedicated BFD on the SRX550M, use the **set chassis dedicated-ukern-cpu** command.

  [See Understanding BFD for Static Routes for Faster Network Failure Detection, Understanding Distributed BFD, dedicated-ukern-cpu (BFD), and realtime-ukern-thread (BFD).]

Ethernet Switching

- **Layer 2 switching capability support on SRX1500 devices**—Starting with Junos OS 15.1X49-D110, Layer 2 switching capability includes Ethernet switching features on both nodes of a chassis cluster. Ethernet ports on either node can be configured for family Ethernet-switching. You can configure a Layer 2 VLAN domain with member ports from both nodes and the Layer 2 switching protocols on both devices. To ensure that Layer 2 switching works seamlessly across chassis cluster nodes, a dedicated physical link called a switching fabric interface (swfab) is required to connect the nodes.

  [See Layer 2 Ethernet Switching Capability in Chassis Cluster Mode.]

Flow-based and Packet based Processing

- **TCP out-of-state packet drop logging (SRX Series)**—Starting in Junos OS Release 15.1X49D110, SRX Series devices support logging of unsynchronized TCP out-of-state packets that are dropped by the flow module.

Within any packet-switched network, when demand exceeds available capacity, the packets are queued up to hold the excess packets until the queue fills, and then the packets are dropped. When TCP operates across such a network, it takes any corrective actions to maintain error-free end-to-end communications.

This feature enables packet recovery by logging the out-of-sync packets for error-free communication, and avoids database servers going out of sync.

TCP packet drop logging occurs when:

- TCP packets that trigger session creation are not synchronized.
- TCP three-way handshake in flow fails.
- TCP sequence check in flow fails.
- TCP SYN packets are received in TCP FIN state.

The unsynchronized TCP out-of-state packet drop log is a packet-based log, not a session-based log.

NOTE: **TCP packets that are dropped by TCP-proxy and IDP are not logged.**

[See TCP Out-of-State Packet Drop Logging Overview

Interfaces

- **Support for remote loopback feature for VDSL interfaces on SRX320, SRX340, SRX345, and SRX550M devices**— Starting with Junos OS Release 15.1X49-D110, the Junos OS CLI provides support for remote loopback feature in Ethernet OAM link fault management on VDSL interfaces.

  [See Example: Configuring Remote Loopback Mode on VDSL Interfaces

J-Web

- **J-Web Support for SRX345 Devices**—Starting with Junos OS Release 15.1X49-D110, J-Web supports two SKUs of SRX345 device, that is, SRX345-DC and SRX345-Dual-AC.
- **J-Web support for Reporting Enhancements (vSRX, SRX300, SRX320, SRX320-PoE, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 Devices)**—Starting with Junos OS Release 15.1X49-D110, the following new reports are added in the existing Reports page in J-Web:
  - Top URL categories by bandwidth
  - Top URLs by user
  - Top users by bandwidth
  - Top Source Zone by volume
  - Top applications by sessions
  - Top applications by user

- **J-Web support for IKE path fragmentation (vSRX and SRX series)**—Starting with Junos OS Release 15.1X49-D110, in the Add Gateway page under Configure > Security > IP Sec VPN > IKE (Phase I) the following options are added:
  - Option to enable or disable fragment if IKE version is IKEv2.
  - Option to provide the size of the IKE fragment if it is enabled.
- **J-Web alarms feature enhancement (vSRX and SRX series)**—Starting with Junos OS Release 15.1X49-D110, the alarms page in J-Web is enhanced to support configuration and monitoring of different types of alarms, such as, chassis alarms and system alarms.
- **J-Web Device Management Feature Enhancements (vSRX, SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 Devices)**—Starting with Junos OS Release 15.1X49-D110, J-Web allows you to change the existing device settings for one or more devices in the Configure > Device Setup > Basic Settings > Management Access page, Configure > Network > OSPF page, and Configure > Network > BGP page.
- **J-Web support for SRX/NCP Pathfinder v1 and multiple proxy IDs for route-based VPNs (vSRX and SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, and SRX4200 Devices)**—Starting with Junos OS Release 15.1X49-D110,
  - J-Web supports SRX/NCP Pathfinder v1, wherein, the NCP Secure Client can use Port 443 of the firewall, which allows for a holistic IPSec-based implementation of the security policy.
  - J-Web supports multiple proxy IDs or traffic selectors to be used to identify and direct traffic to the correct tunnel when there are multiple tunnels to the same peer.

Monitoring and Troubleshooting

- **Two Way Active Measurement Protocol (TWAMP) support on server and client**—Starting in Junos OS Release 15.1X49-D110, the Two-Way Active Measurement Protocol (TWAMP) is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices. TWAMP is a standard protocol framework that defines control and test session separation based on the client/server architecture. The TWAMP-Control protocol is used to set up performance measurement sessions between a TWAMP client and a TWAMP server, and the TWAMP-Test protocol is used to send and receive performance measurement probes.

Security Intelligence

- **Support Feed-Based URL Redirection for SecIntel C&C**— Starting with Junos OS Release 15.1X49-D110, a **feed-name** option is added to the **set services security-intelligence profile** CLI command. This option lets you perform an action based on feeds, such as URL redirection.

  [See set services security-intelligence.]

Security Policy

- **Advanced policy-based routing (APBR) with enhancements (vSRX and SRX Series)**—Starting with Junos OS Release 15.1X49-D110, SRX Series Services Gateways support advanced policy-based routing (APBR) with an additional enhancement to apply the APBR in the middle of a session (midstream support). With this enhancement, you can apply APBR for a non-cacheable application and also for the first session of the cacheable application.

  You can fine-tune the outbound traffic with APBR configuration (for example, limiting route changes and terminating sessions) to avoid issues such as excessive transitions due to frequent route changes.

  The enhancement provides more flexible traffic-handling capabilities that offer granular control for forwarding packets.

  [See Understanding Advanced Policy-Based Routing.]

User Access and Authentication

- **Support configuration file integrity on SRX300, SRX320, SRX340, and SRX345 devices**— Starting with Junos OS Release 15.1X49-D110, the Junos OS configuration integrity feature enhances the current functionality where certain sensitive data is encrypted and protected by the Trusted Platform Module (TPM) using a master encryption password.

  This enhancement generates a SHA256 hash of the configuration file that is protected by the master encryption password, meaning that if someone tampers with the configuration, the system will not be able to boot up.

If the system is compromised, the administrator can recover the system by clearing the TPM ownership in u-boot and then installing the image in the boot loader using TFTP or USB (if USB port is not restricted).

See Using Trusted Platform Module to Bind Secrets on SRX Series Devices.

- **Support for secure copy (scp) on the Junos OS CLI on SRX300, SRX320, SRX340, SRX345, and SRX550M devices**— Starting with Junos OS Release 15.1X49-D110, the Junos OS CLI provides support for secure copy with the **scp** command.

  See scp.

Unified Threat Management (UTM)

- **User messages and redirect URLs for Enhanced Web Filtering (EWF) on SRX Series devices**—Starting with Junos OS Release 15.1X49-D110, a new **custom-message** option is added for the **custom-objects** command. Custom messages are used to notify users when the URL is blocked or quarantined for each EWF category. The **custom-message** option allows you to fine-tune messages to support your polices:
  - **user-message**: User messages indicate that website access has been blocked by an organization's access policy.
  - **redirect-url**: Redirect URLs redirect a blocked or quarantined URL to a user-defined URL.

  [See Understanding Enhanced Web Filtering Process.]

Related Documentation

- Changes in Behavior and Syntax on page 10
- Known Behavior on page 13
- Known Issues on page 17
- Resolved Issues on page 22
- Migration, Upgrade, and Downgrade Instructions on page 26

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-D120.

Authentication, Authorization and Accounting (AAA)

- Starting with Junos OS Release 15.1X49-D110, you can configure the **nas-identifier** option (RADIUS attribute 32) for authentication and accounting requests on SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  To configure RADIUS attribute 32, include the **nas-identifier** option in the [set access] hierarchy level. For example,

  ```
  set access profile profile radius options nas-identifier
  ```

- Starting with Junos OS 15.1X49-D80, the **wins-server** option at the [**edit access profile** ***profile-name***] hierarchy level allows you to configure the IPv4 address of a Windows Internet Name Service (WINS) server.

Chassis Cluster

- Starting with Junos OS Release 15.1X49-D110, on SRX5400, SRX5600, and SRX5800 devices in chassis cluster, the initial hold time (the duration that a newly added node waits for, before transferring from hold state to secondary state) is increased from 60 seconds to 120 seconds.

CLI

- Starting with Junos OS Release 15.1X49-D60, the **modem1** option has been added to the **show wireless-wan adapter <adapter-name> modem** command. The **modem1** option displays details of the integrated modems on the CBA850 3G/4G/LTE Wireless WAN Bridge.

Flow-based and Packet-based Processing

- Starting with Junos OS Release 15.1X49-D100, for the SRX300, SRX320, SRX340, SRX345, and SRX550M devices, the maximum capture size for packet captures is expanded to 1520 bytes to allow for captures of 1500 bytes of data and the 12-byte Juniper Ethernet header.

Layer 2 Ethernet Services

- Starting with Junos OS Release 15.1X49-D100, on SRX300, SRX320, SRX340, SXR345, SRX550M, and SRX550M devices, the default Layer 2 global mode configuration is changed from transparent-bridge to switching mode.

NOTE: You must explicitly configure Layer 2 transparent-bridge mode for the SRX300, SRX320, SRX340, SRX345, SRX550, and SRX550M devices that work in transparent mode. Use the command **set protocols l2-learning global-mode transparent-bridge** before rebooting the devices with Junos OS 15.1X49-D100 image.

MIB

- In Junos OS Release 15.1X49-D110, duplicated entries and errors while loading MIBs on ManageEngine MIB browser are fixed for the following MIB files:
  - jnx-chas-defines.mib
  - jnx-gen-set.mib
  - jnx-ifotn.mib

- jnx-optics.mib
- jnx-smi.mib

[See MIB Explorer.]

Network Monitoring and Troubleshooting

- Starting with Junos OS Release 15.1X49-D110, on SRX5400, SRX5600, and SRX5800 devices, a new option **secure-gateway** is added to the existing **request support information** command. This new option displays all the required information that is relevant for secure gateway deployment scenarios. In Junos OS Release 15.1X49-D100 and earlier, request support information displays the information about all features that might not be relevant for secure gateway deployments.

System Services

- Starting with Junos OS Release 15.1X49-D110, you can configure the **routing-instance** option at the [**edit system name-server *x.x.x.x***] hierarchy. This allows DNS queries to be originated for a specific source address and routing instance. This configuration resolves a domain name specified in the **set security ike gateway *gateway-name* address *domain-name*** configuration to an IP address. Only one source address can be configured for each name server. A routing instance can be configured for each source address. IPv6 source addresses are only supported for IPv6 DNS servers. You cannot configure an IPv6 source address for an IPv4 DNS server or an IPv4 source address for an IPv6 DNS server.

Unified Threat Management (UTM)

- Starting with Junos OS Release 15.1X49-D110, on all SRX Series devices, the "*" in wildcard syntax, required to create URL pattern for web filtering profile, matches all sub-domains. For example, *.example.net matches:
  - http://a.example.net
  - http://example.net
  - a.b.example.net

Related Documentation

- New and Changed Features on page 5
- Known Behavior on page 13
- Known Issues on page 17
- Resolved Issues on page 22
- Migration, Upgrade, and Downgrade Instructions on page 26

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D110.

Ethernet Switching

- On SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, VPLS traffic forwarding stops working after enabling ethernet switching configuration. This is current limitation. VPLS and ethernet-switching should not be configured together on the same device on the mentioned devices. As a workaround avoid using ethernet-switching configuration on these platforms when VPLS is enabled.

Firewall Authentication

- Firewall authentication cannot retrieve domain information from access profile configuration, such that firewall authentication will not push user domain information to juniper identity management service server in case user authenticates through web-authentication, pass-through, or web-redirect with a LDAP access profile.

Flow-based and Packet-based Processing

- OSPF over GRE over IPSec is not supported on SRX platforms with standalone CP.
- Advanced anti malware (AAMW) established sessions always use the configured AAMW parameters during the time of session establishment. Configuration changes do not affect the established sessions. For example, a sessions established when the verdict threshold is 5 will always have 5 as threshold, even if the verdict threshold changes to any other values during that sessions lifetime.
- FIPS core file is seen when you perform a firmware upgrade or downgrade. In a FIPS version Junos, file integrity checking application veriexec treats the new updated firmware file as corrupted Junos file. This is an expected behavior by design.
- On SRX Series device, if advanced anti-malware service (AAMW) is enabled, and SMTP(s) is configured in the AAMW policy, and fallback permit is enabled, under the long network latency between SRX device and AWS running Sky ATP service, there may be a file submission time-out. When the sending timeout occurs, there is a potential chance that the e-mail sent out from Outlook might stay in the outbox of the sender, and the receiver might not receive the e-mail.
- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, after certain period of enabling dot1x, multiple first message EAP frames with the same timestamp are transmitted. However, this does not affect any dot1x functionality.
- On SRX5400, SRX5600, and SRX5800 devices, in central point architecture, system logs are sent per second per SPU. Hence, the number of SPUs define the number of system logs per second.

General Packet Radio Service (GPRS)

- On SRX5000 Series devices, when you use the GTP inspection feature, during an ISSU from Junos OS Release 15.1X49-D10, 15.1X49-D20, or 15.1X49-D30 to Junos OS Release 15.1X49-D40 or later, GTPv0 tunnels will not be synchronized to the upgraded node.

  For GTPv1 and GTPv2, the tunnels will be synchronized, but the timeout gets restarted.

  Beginning with Junos OS Release 15.1X49-D40, ISSU is fully supported with the GTP inspection feature enabled.

Integrated User Firewall

- The SRX Series integrated user firewall feature for both ClearPass and active directory authentication will manage up to 2048 sessions for each user for whom there is a user identity and authentication entry in the authentication table. There might be additional sessions associated with a user beyond the 2048 supported sessions, but they are not managed by integrated user firewall. When an authentication entry in an authentication table is deleted, integrated user firewall only closes sessions that are associated with that entry. It will not close sessions that it does not manage. That is, sessions that are not associated with the authentication entry are not closed.

Interfaces and Routing

- When a Digital Subscriber Line Access Multiplexer (DSLAM) is invoked for link fault management remote loopback in drop mode, the VDSL PPPOE interface goes down.
- On SRX1500 devices, when 1G SFP-T is used on the 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100M speed.
- On SRX320, SRX340, SRX345, and SRX550M devices with LTE Mini-Physical Interface Module (Mini-PIM) for 4G/LTE wireless connection, modem profile is not active until a profile is defined. You need to define a profile before selecting a profile.
- You cannot create profiles for CL-1/0/0 using J-Web and CLI. An error message, **Interface not found** is displayed. It is recommended to use only one LTE mPIM in the supported SRX Series devices.

J-Web

- On SRX550M and SRX1500 devices, there is no option to configure Layer 2 firewall filters from J-Web, irrespective of the device mode.
- On SRX Series devices in chassis cluster, if you want to use J-Web to configure and commit the configurations, you must ensure that all other user sessions are logged out including any CLI sessions. Otherwise, the configurations might fail.
- If 2000+ global addresses are added at a time to SSL Proxy profile exempted addresses then J-Web page does not respond.

Software Installation and Upgrade

- On SRX5000 Series devices, 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.

  NOTE: SRX300 Series devices and SRX550M devices do not support ISSU.

Platform and Infrastructure

- On SRX5800 devices, if global SOF policy (all session service-offload) is enabled, the connections per second (CPS) will be impacted due to IOC2 limitation. It is recommended to use IOC3 card if more sessions are required for SOF or lower the SOF session amount to make sure IOC2 is capable of handling it.

USB Autoinstallation

- On SRX300 Series Services Gateways on which the USB autoinstallation feature is enabled (the default configuration), removal of a USB storage device immediately after insertion is not supported.

  NOTE: USB autoinstallation is not supported on SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices.

  After you insert a USB storage device, Junos OS scans the device to check whether it contains the USB autoinstallation file. This process might take up to 50 seconds to complete depending on the quality of the USB storage device and the number and size of the files in the device. Removing the USB storage device while this process is running might cause the services gateway to reboot, the USB port to stop working, and data loss on the USB. We recommend that after inserting a USB storage device, you wait for at least 60 seconds before removing it.

  By issuing the **set system autoinstallation usb disable** command (which disables the USB autoinstallation feature) before you insert the USB device, you can reduce the waiting interval between insertion and removal of a USB storage device from 60 seconds to 20 seconds.

Unified Threat Management (UTM)

- Transport of IPv6 packets between the SRX Series devices and cloud servers (Sophos antivirus, Enhanced Web filtering, Websense redirect, and Antispam filtering servers) is not supported.
- Websense redirect and antispam filtering do not support IPv6 traffic.

VPN

- The group VPN server daemon might generate a coredump when the group VPN server configuration is committed for the first time or when the SRX device starts up with the group VPN server configuration.
- ISSU with VPN configuration is not supported when upgrading from a Junos OS release prior to 15.1X49-D75 to Junos OS Release 15.1X49-D75 and later releases. You can use ISSU with VPN configuration when upgrading from Junos OS Release 15.1X49-D75 to later releases. You can also use ISSU with VPN configuration to upgrade from Junos OS Release 15.1X49-D10 up to Junos OS Release 15.1X49-D70.
- On SRX5400, SRX5600, and SRX5800 devices, do not use ISSU if upgrading from Junos OS Release 15.1X49-D30 through Junos OS Release 15.1X49-D60, if using any VPN configurations.

  As a workaround deactivate or remove all the VPN commands from the configuration before executing ISSU. If the workaround is used, all VPN tunnels and VPN traffic will be dropped during ISSU upgrade. Once ISSU has completed you may then re-enable the VPNs as before.

Related Documentation

- Changes in Behavior and Syntax on page 10
- New and Changed Features on page 5
- Known Issues on page 17
- Resolved Issues on page 22

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D110.

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

Authentication and Access Control

- On SRX5400, SRX5600, and SRX5800 devices, by default, support an additional check on the LDAP servers certificate during the TLS handshake for LDAP authentication. If the validation of the server certificate is not required, you can use the **set access profile profile-name ldap-server ldap-server-ip-address no-tls-certificate-check** command to ignore the validation of servers certificate and accept the certificate without checking. PR1218357
- On SRX Series devices, httpd blocks TLS1.0 and TLS1.1 SSL protocols because of reported security vulnerabilities. This issue might affect users accessing web authentication GUI using lower version browsers where TLS v1.2 or SSLv3 protocols are not supported. TLS v1.2 and SSLv3 protocols are recommended while opening secure connection through HTTPS. PR1283812

Chassis Clustering

- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then reenable CRL checking of certificate validity, the system does not reenable CRL checking. PR1144280
- On SRX550M devices in a chassis cluster, traffic loss for about 10 seconds is seen when there is power failure on the active chassis cluster node. PR1195025
- On SRX Series devices with chassis cluster enabled, the issue occurs when multicast traffic goes across logical systems. The ingress interface of the multicast session in the first logical system is reth2.0 which belongs to redundancy group 2. Redundancy group 2 is active on node 1. The ingress interface of the multicast session in the second logical system will be PLT interface which belongs to redundancy group 1. Redundancy group 1 is active on node 0. So the multicast session in the second logical system will be active on node 0. It will cause multicast session active or backup not aligned with traffic forwarding. The workaround is to make Redundancy group 1 and redundancy group 2 active on the same node. PR1295893

Class of Service (CoS)

- On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, for IFLS (logical interface) scaling:
  - Without per-unit-scheduler configured, total IFL number is limited to 2048.
  - With per-unit-scheduler configured on the IFD interface, total IFL number is limited to CoS scheduler sub-unit upper limit (2048).

  So, IFL **max-number** for **per-unit scheduler** should be 2048 minus the number of physical interface (which is up with at least one logical interface up, max number is 128). PR1138997

Flow-based and Packet-based Processing

- On SRX345 devices, Filter-based Forwarding (FBF) does not work when applied on IPsec tunnel interface (st0.*). PR1290834
- On SRX4100 and SRX4200 devices, packet loss is observed when packet per second (PPS) through the device is very high. This occurs due to update of **application interval statistics** command which has a default timer value of 1 minute. You can avoid this issue by setting the interval to maximum using the following configuration: **set services application-identification statistics interval 1440**. PR1290945

Interfaces and Routing

- On SRX550M devices, when the LTE signal is weak, the connection drops to 3G and in certain cases, the modem flaps and the connection might be lost. PR1291395

Installation and Upgrade

- On SRX550M devices, when upgrading from Junos OS Release 15.1X49-D30 to a later version, upgrade fails. PR1237971

J-Web

- On SRX Series devices in J-Web, when you login to the Web-authentication page, the following error message is displayed: **BAD_PAGE_FAULT**. PR1180787
- On SRX Series devices, DHCP relay configuration under Configure > Services > DHCP > DHCP Relay page is removed from J-Web in Junos OS Release 15.1X49-D60. The same DHCP relay can be configured using the CLI. PR1205911
- On SRX Series devices, DHCP client bindings under Monitor is removed for Junos OS Release 15.1X49-D60. The same bindings can be seen in CLI using the **show dhcp client binding** command. PR1205915
- On SRX4100 devices, a security policy page in J-Web does not load when it has 40000 firewall policy configuration. Navigate to Configure> Security> Security Policy page. PR1251714
- On SRX Series devices, login to J-Web and navigate to Monitor>Services>DHCP> DHCP SERVER & DHCP RELAY. When you click the help page icon, the Online help page will display a 404 error message. PR1267751
- On SRX Series devices, adding of 2000 or more global addresses at a time to the SSL proxy profile exempted addresses can cause the web page to be unresponsive. PR1278087
- On SRX Series devices, sometimes the Dashboard widgets applications, Threatmap, and Firewall Top Denies shows no data available when the device is having huge data. PR1282666
- On SRX Series devices, sometimes the time range slider does not work for all events, as well individual events in Google Chrome or Firefox browser. PR1283536
- On SRX Series devices, the CLI terminal does not work for Google Chrome version greater than 42. We can use Internet Explorer 10 or 11 or Firefox 46 browsers to use the CLI terminal. PR1283216

Layer 2 Ethernet Services

- On 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 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 does not send the second request, because the process detects that the first authentication did not occur. This delay causes memory leak on the authd process and the memory might be exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. PR1042818

- On SRX300 devices, the delegated subnet will start with the least significant bit set, causing one subnet to be wasted. PR1295178

Platform and Infrastructure

- On SRX Series devices, when a USB flash device with a mounted file system is physically detached by a user, the system might panic. PR695780
- On SRX5400, SRX5600, and SRX5800 devices with IOC2 or IOC3 cards, when FPC gets offline and online in a race condition, other FPCs might not be able to connect with this FPC, and the following error message might be displayed: **xmchip_dstat_stream_wait_to_drain**. PR1052472
- On SRX5800 devices, if the system service REST API is added to the configuration, though commit can be completed, all the configuration changes in this commit will not take effect. This occurs as the REST API daemon fails to come up and the interface IP is not available during bootup. The configuration is not read on the Routing Engine side. PR1123304
- On SRX300, SRX320, SRX340, and SRX345 devices, when the protocol packets are flooded into the device, the CPU usage is exhausted to process the BPDU frame which has higher priority than Layer 3 protocol, such as, ICMP and IPv4. On the device, the CPU processes to receive maximum number of frames. So, it is possible that the CPU exhausts during high traffic. PR1259793

Routing Policy and Firewall Filters

- On 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. PR969944

Unified Threat Management (UTM)

- On SRX Series devices, if advanced anti-malware service (AAMW) is enabled, and SMTP is configured in the AAMW policy, and if fallback permit is enabled under the long network latency between the devices and AWS running Sky ATP service, there might be a file submission timeout. When sending timeout occurs, there is a possibility that the email sent out from Outlook will stay in the outbox of the sender, and the receiver will not receive the email. PR1254088

VPN

- On SRX Series devices, if IPsec VPN tunnel is established using IKEv2, due to bad SPI, packet drop might be observed during CHILD_SA rekey when the device is the responder for this rekey. PR1129903
- On SRX5800 devices, when upgrading from Junos OS Release 15.1X49-D30 to 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 and from 15.1X49-D35, 15.1X49-D40, and 15.1X49-D50 to 15.1X49-D60 release, the ISSU fails for AutoVPN/ADVPN/DEP IPsec VPN tunnels. PR1201955
- On SRX5400, SRX5600, and SRX5800 devices, when CoS on **st0** interface is enabled and the incoming traffic rate destined for **st0** interface is higher than 300000 packets per second (pps) per SPU, the device might drop some of the high priority packets internally and shaping of outgoing traffic might be impacted. It is recommended that you configure appropriate policer on the ingress interface to limit the traffic below 300000 pps per SPU. PR1239021
- On SRX Series devices, a loopback interface using two IP addresses can be used to create IPsec tunnels to two different remote peers on an Active/Passive SRX5000 Series cluster devices as long as the **local-address** parameter is defined under the IKE configuration with the appropriate loopback IP address for each remote peer. PR1266915
- On SRX Series devices, in case multiple traffic-selectors are configured for a peer with IKEv2 reauthenticaiton, only 1 traffic-selector will rekey at the time of IKEv2 reauthentication. The VPN tunnels of the remaining traffic selectors will be cleared without immediate rekey. New negotiation of those traffic-selector might trigger through other mechanisms such as traffic or by peer. PR1287168

Related Documentation

- New and Changed Features on page 5
- Migration, Upgrade, and Downgrade Instructions on page 26
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 13

- Resolved Issues on page 22

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D110.

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

Chassis Clustering

- On SRX5400, SRX5600, and SRX5800 devices with chassis cluster Z-mode scenario, the TTL (Time To Live) for few Z-mode packets are reduced to zero by error if IOC2 or IOC3 interface is configured as HA (High Available) fabric port, and some Z-mode packets with size greater than 212 bytes might be sent to SPC1 (Services Processing Card 1) causing the traffic to be dropped. PR1270770
- On SRX Series devices, during configuration changes on the device through NETCONF or Junos Space, the device returns a warning message with a wrong tag that prevents the configuration from being committed and the device fails to get added to Junos Space. PR1286903
- On SRX devices running in chassis cluster, FTP data session gets stuck after two back to back RG1+ failovers. PR1286547
- On SRX5400, SRX5600, and SRX5800 devices, when one cluster node boots up, in some cases both cluster nodes may become primary due to an unexpected control link flap affecting the traffic. This issue is not applicable for Junos OS Release 12.3X48 and earlier releases. PR1288819

CLI

- On SRX Series devices, when running operational command for creating rescue configuration, some errors are reported but rescue configuration is created. PR1280976

Flow-based and Packet-based Processing

- On SRX5400, SRX5600, and SRX5800 devices, the traceroute traffic might be dropped when the traceroute traffic is processed by NAT. PR1266611
- SRX Series devices might coredump if the mirror-filter port is down. PR1270724

General Packet Radio Service (GPRS)

- On SRX 5400, SRX5600, and SRX5800 devices, in cases where XUDT mandatory variable parameters are not in strict order, the device will drop the SCTP packets. PR1285089
- On SRX5400, SRX5600, and SRX5800 devices with GTP inspection configured, a GTP control plane packet is dropped if it contains any information element (IE) more

than once. For example when the RFSP index IE appears twice in an SGSN Context Response, the packet will be dropped. PR1284311

In-Service Software Upgrade (ISSU)

- On SRX5000 Series devices, during ISSU with special data pattern, the number of invalid authentication entry is around 5000 and the pending authentication entry is reaching the maximum number on the device. When ISSU is ongoing the related traffic will go through device with some number and at this situation ISSU might fail. PR1284561

Interfaces

- On SRX320 devices, IPv6 traffic triggered dial-on-demand from configured static route is not supported on Junos OS Release 15.1X49-D100. PR1273532
- On SRX devices in chassis cluster mode, Point-to-Point protocol (PPP) session is not established when Point-to-Point protocol is configured under reth interface using the LACP interface. PR1276177
- On SRX1500 device, SFP+-10G-CU3M DAC cable connects to the xe interface, xe interface is not coming UP physically. PR1279182
- On SRX Series devices, when using the LTE mPIM, the APN profile password is displayed in clear text. This behavior is now modified to obfuscate the password with asterisks (*). PR1295274

Integrated User Firewall

- On SRX Series devices, useridd might consume high CPU. Traceoptions of integrate user firewall will be full of UGCALC_AD_MEMBER_UPDATE messages. PR1280783
- On SRX Series devices with user firewall feature, the users sometimes fails to authenticate from LDAP server and gets the authorized group though the group mapping shows correctly for that particular user. PR1282744

J-Web

- On SRX345 platform, for every commit performed using J-Web, commit goes through, but the J-Web pages always prompt the following message: **The configuration on the device is too large for J-Web to handle. Please use CLI to manipulate the configuration**. PR1286996
- On all SRX Series devices, source NAT pool configuration from J-Web cannot be committed unless an address range is entered. The Add or Delete buttons available in J-Web to add or delete source NAT pool address range is not visible now. You can perform this operations only through CLI:

  1. Navigate to Configure -> Security -> NAT -> Source.
  2. Click **Source NAT Pools** tab and enter the pool name.
  3. While entering address range details for pool addresses, add or delete buttons are missing from the window.

4. You will not be able to commit unless address range is entered.
5. You can configure through CLI using the following commands:

   To Add source NAT pool address ----> **set security nat source pool <poolname> address <ip_addr> to <ip_addr>**

   To Delete source NAT pool address ---> **delete security nat source pool <poolname> address <ip_addr> to <ip_addr>**

- On SRX devices with Junos OS Release 15.1X49-D100, the device cannot be upgraded using the Junos image through J-Web. PR1297362

Network Address Translation (NAT)

- On SRX1500, SRX4100, SRX4200, SRX5400, SRX5600, and SRX5800 devices, after performing a Redundancy Group 0 (RG0) failover, traffic that relies on the use of **proxy-arps** may no longer work, causing an outage. PR1289614

Network Management and Monitoring

- On SRX340 devices, after power on or Redundancy Group 0 (RG0) failover at the cluster, one RE does not reply for SNMP request. PR1240178

Platform and Infrastructure

- On SRX Series devices, the routes activated by IP monitoring are not getting cleared after the probe status changes from **Fail** to **Pass**. The **show services ip-monitoring status** command will display routes **NOT-APPLIED**, but the **show route** command will display IP monitoring route active (static route with preference 1). PR1263078
- On SRX Series devices, DNS cache is not getting populated in multiple virtual router (VR) environments. When doing recursive route lookup in different routing instances, the route to the DNS server would be ignored in one of the following scenarios: If the route points to an interface not in the same routing instance or the route points to another routing instance. Conversely if one of the VRs has a route for the DNS, pointing to a wrong interface in the same routing instance, further lookup in other routing instances would not occur. PR1275792
- On SRX Series devices, the PFE CPU utilization reached 100% in every 10 minutes even though the session count has not increased. PR1284971

System Logging

- On SRX550 devices, remove logs from syslog **RT_FLOW: FLOW_REASSEMBLE_SUCCEED: Packet merged**. If lots of fragmented packets are processed, and the force-ip-reassembly option is enabled or fragments merge is required by some Advanced Services (such as UTM, AppSecure, IDP, ALGs, GTP, SCTP, and etc.), if the logs from syslog **RT_FLOW: FLOW_REASSEMBLE_SUCCEED: Packet merged** are seen then this might cause high CPU usage on Routing Engine (RE). PR1278333

Unified Threat Management (UTM)

- On all SRX Series devices, incorrectly formed HTTP traffic contain non-standard HTTP boundary format, it will cause SRX UTM/SAV hold traffic/mbuf, later cause failover. PR1283806

VPN

- On SRX Series devices, when a local certificate which is used for IPSec VPN is revoked by the CA, and CRL checking is enabled, the PKID daemon might crash. PR1290218

Related Documentation

- New and Changed Features on page 5
- Migration, Upgrade, and Downgrade Instructions on page 26
- Changes in Behavior and Syntax on page 10
- Known Behavior on page 13
- Known Issues on page 17

Documentation Updates

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

- Information about MIBs is available in SNMP MIBS Explorer. On the Junos OS for SRX Series page, click **SNMP MIB Explorer** to view MIBs information. Use the MIBs Explorer to search for and view information about various MIBs, MIB objects, and SNMP notifications that are supported on Juniper Networks devices.
- Information about system log messages is available in System Log Explorer. On the Junos OS for SRX Series page, click **System Log Explorer** to view system log information. Use the System Log Explorer to search for and view information about various system log messages.

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

Starting with Junos OS Release 15.1X49-D10 and later, only 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 Layer 2 next-generation 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 https://kb.juniper.net/InfoCenter/index?page=content&id=KB30445.

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 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:

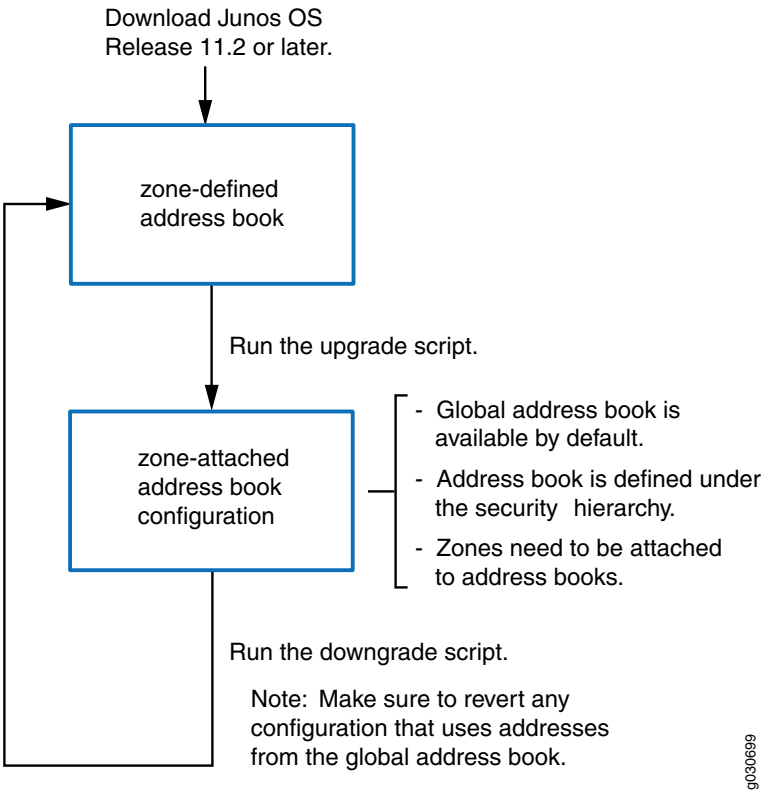
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  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 Release 12.3X48 is an EEOL release. You can upgrade from Junos OS Release 12.1X46 to Release 12.3X48 or even from Junos OS Release 12.3X48 to Release 15.1X49-D10. For upgrading from Junos OS Release 12.1X47-D15 to Junos OS Release 15.1X49-D10, ISSU is supported. 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://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, see the Installation and Upgrade Guide for Security Devices.

For information about ISSU, see the Chassis Cluster Feature 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 22

Product Compatibility

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

- Hardware Compatibility on page 29
- Transceiver Compatibility for SRX Series Devices on page 30

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 https://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 https://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.

To access Software Release Notifications for Junos OS Service Releases, visit our Knowledge Center at https://support.juniper.net/support/. You'll need to log in to your Juniper Account. From the Knowledge Center, search by the specific release number, for example 17.4R1-S2. Use the Software Release Notifications to download software, and learn about known and resolved issues for specific service releases.

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 https://apps.juniper.net/feature-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 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://support.juniper.net/support/
- Search for known bugs: https://kb.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://support.juniper.net/support/downloads/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://forums.juniper.net
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

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 https://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 https://support.juniper.net/support/requesting-support/.

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 https://www.juniper.net/documentation/feedback/.

Revision History

28, January 2019—Revision 6— Junos OS 15.1X49-D110 – SRX Series.

09, November 2017—Revision 5— Junos OS 15.1X49-D110 – SRX Series.

02, November 2017—Revision 4— Junos OS 15.1X49-D110 – SRX Series.

05, October 2017—Revision 3— Junos OS 15.1X49-D110 – SRX Series.

19, September 2017—Revision 2— Junos OS 15.1X49-D110 – SRX Series.

11, September 2017—Revision 1— Junos OS 15.1X49-D110 – SRX Series.