Release Notes: Junos® OS Release 15.1X49-D120 for the SRX Series

Release 15.1X49-D120
13 March 2018
Revision 4

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-D120 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-D120 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-D120 for the SRX Series devices. For New and Changed Features information starting with Junos OS Release 15.1X49-D10 to Junos OS Release 15.1X49-D110, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

Release 15.1X49-D120 Software Features

Class of Service (CoS)

- **Support for applying IEEE802.1 rewrite rules to both inner and outer VLAN tags (SRX Series, vSRX)**—SRX Series devices already support applying an IEEE802.1 rewrite rules to the outer VLAN tag. Starting with Junos OS Release 15.1X49-D120, you can apply an IEEE802.1 rewrite rule to both the inner and outer VLAN tags. You can do this by setting the **vlan-tag** option to **outer-and-inner** at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules ieee-802.1 *rewrite-name*]**.

  [See rewrite-rules (CoS Interfaces).]

Sky Advanced Threat Prevention (ATP)

- **IMAP E-Mail Attachments**—Starting in Junos OS Release 15.1X49-D120, e-mail management for IMAP lets enrolled SRX Series devices transparently submit potentially malicious e-mail attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score from 0 through 10 with 10 being the most malicious. In addition, e-mails are checked against administrator-configured blacklists and whitelists. If an e-mail matches the blacklist, it is considered to be malicious and is handled the same way as an e-mail with a malicious attachment.

  Please refer to the Supported Platforms Guide for IMAP support on various SRX Series devices.

  [See Email Management Overview.]

VPN

- **Packet size configuration for IPsec datapath verification (SRX Series, vSRX)**—Starting in Junos OS Release 15.1X49-D120, you can configure the size of the packet that is used to verify an IPsec datapath before the st0 interface is brought up. The configurable packet size ranges from 64 to 1350 bytes; the default is 64 bytes.

  [See Understanding IPsec Datapath Verification.]

Related Documentation

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.

AppSecure Services

- Starting from Junos OS Release 15.1X49-D120, on all SRX Series devices, the default time interval for application identification statistics collection time is changed from 1 minute to 1440 minutes.
- Starting in Junos OS Release 15.1X49-D120, you can limit the maximum number of entries in the IMAP cache and specify the timeout value for the entries in the cache by using the following commands:

  set services application-identification imap-cache imap-cache-size ***size***

  set services application-identification imap-cache imap-cache-timeout ***time in seconds***

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

Class of Service (CoS)

- If you configure a shaping rate as a percent in a scheduler, the effective shaping rate is calculated based on the following hierarchy:

  1. Logical interface shaping rate, if configured
  2. Physical interface shaping rate, if configured
  3. Physical interface bandwidth

  With SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, and vSRX 2.0 devices, you can configure both logical interface shaping rates and physical interface shaping

rates on the same physical interface. On all other models, you can only configure one or the other on a particular physical interface.

Flow-based and Packet-based Processing

- Starting with Junos OS Release 15.1X49-D120, to support more scenarios of cross-VR host traffic, the to-host traffic uses a local interface based on its source interface Virtual Router (VR). In earlier releases, the host traffic used local interface based on the default VR. The from-host traffic follows the similar process to select the ingress interface to avoid a session mismatch. The Routing Engine generates from-host traffic and receives to-host traffic.

MIB

- In Junos OS Release 15.1X49-D110, duplicated entries and errors while loading MIBs on Manage Engine 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.]

Platform and Infrastructure

- TPM Firmware Update (SRX300, SRX320, SRX340, and SRX345) – Starting with Junos OS Release 15.1X49-D120, Trusted Platform Module (TPM) firmware has been updated. The upgraded firmware version provides additional secure cryptography and improves security. Updated TPM firmware is available along with the Junos OS package. For updating TPM Firmware, see Upgrading TPM Firmware on SRX-Devices.

  To confirm the TPM firmware version, use the **show security tpm status** command. The following additional new output fields are introduced:

  - **TPM Family**— Displays Trusted Computing Group's (TCG) TPM family version.

- **TPM Firmware *version*—** Displays the firmware version loaded in TPM.

System Logging

- Starting from Junos OS Release 15.1X49-D120, the maximum length of the syslog message in stream mode is increased from 1024 bytes to 1340 bytes.

VPN

- Starting with Junos OS Release 15.1X49-D120, you can configure the CLI option **reject-duplicate-connection** at the [**edit security ike gateway *gateway-name* dynamic**] hierarchy level to retain an existing tunnel session and reject negotiation requests for a new tunnel with the same IKE ID. By default, an existing tunnel is tear down when a new tunnel with the same IKE ID is established. The **reject-duplicate-connection** option is only supported when **ike-user-type group-ike-id** or **ike-user-type shared-ike-id** is configured for the IKE gateway; the **aaa access-profile *profile-name*** configuration is not supported with this option.

NOTE: Use the CLI option reject-duplicate-connection only when you are certain that reestablishment of a new tunnel with the same IKE ID should be rejected.

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 7
- Known Issues on page 9
- Resolved Issues on page 11
- Migration, Upgrade, and Downgrade Instructions on page 14

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D120.

Installation and Upgrade

- Starting in Junos OS Release 15.1X49-D120, on SRX300, SRX320, SRX340, SRX345, and SRX550M devices, telnet and xnm-clear-text are not part system services in factory-default configurations.

Interfaces and Routing

- When a DSL access multiplexer is invoked for a link fault management remote loopback in drop mode, the VDSL PPPoE interface goes down.
- On SRX1500 devices, when a 1G SFP-T is used on 1G SFP ports (ge-0/0/12 to ge-0/0/15), the ge interface does not operate at 100-Mbps 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.**

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Issues on page 9
- Resolved Issues on page 11

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D120.

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 is available for 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, TLS1.0 and TLS1.1 SSL protocols are blocked because of reported security vulnerabilities. This change might affect users accessing J-Web, web authentication GUI or using Dynamic VPN through Pulse client, when using an older OS or lower version browsers where TLSv1.2 protocol is not supported. This change affects Junos OS Release 12.3X48-D55, 15.1X49-D100 and all higher SRX releases. PR1283812

Chassis Cluster

- On SRX1500 devices in a chassis cluster with Sky Advanced Threat Prevention (ATP) solution deployed, if you disable and then re-enable CRL checking of certificate validity, the system does not re-enable CRL checking. PR1144280
- 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 is 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 is active on node 0. It causes multicast session active or backup not aligned with traffic forwarding. PR1295893
- On SRX1500 devices, when ISSU is used, if LACP and interface monitoring are configured, the process might fail. PR1305471

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

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, 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 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, sometimes the Dashboard widgets applications, Threat map, 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

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 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 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 SRX Series devices, Network Time Protocol (NTP) synchronous got failed minutes after synchronizing NTP. PR1296236

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 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, in case multiple traffic-selectors are configured for a peer with IKEv2 reauthentication, 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 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Resolved Issues on page 11
- Migration, Upgrade, and Downgrade Instructions on page 14

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D120. For Resolved Issues information starting with Junos OS Release 15.1X49-D10 to Junos OS Release 15.1X49-D110, refer to the Release Notes listed in the Release 15.1X49 section at Junos OS for SRX Series page.

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

Application Layer Gateways (ALGs)

- HTTP ALG listed within show security match-policies, when the HTTP ALG does not exist. PR1308717

Chassis Cluster

- When a **FI: Cell underflow** or a **FI: Aliasing on allocates** error message appears, the device only logs error messages but does not create a **CMERROR** to raise an alarm. PR1076299
- Warning messages are tagged with Error tag wrongly in RPC response from SRX device when you configure change via netconf. PR1286903
- After software upgrade, the cluster goes to short split-brain when rebooting RG0 secondary, multiple errors and issues are seen. PR1288819

Integrated User Firewall

- On SRX Series devices running User Firewall feature, under some condition, flowd-core or useridd-core might be triggered, PFE restarted, RG1+ failover. PR1299494

J-Web

- Configuration upload via J-Web does not work on Junos OS Release 15.1X49-D100. PR1300766
- J-Web does not display all global address book entries. PR1302307
- On J-Web, when logical system added to a custom-applications, the applications **any** do not present in **Logical System Configure > Security > Security Policy > Add Policy**. PR1303260
- J-Web removes the back slash character on source identity object when commit changes. PR1304608
-

Layer 2 Ethernet Services

- DHCPv6 prefix delegation does not start with the first available subnet. PR1295178

Network Address Translation (NAT)

- Traffic loop is seen with MSTP for untag traffic from IxNetwork ports. PR1259099
- On SRX Series devices, the periodic execution of the **show security zones detail** command causes the NSD process to fail in releasing unused memory, causes to the memory leak situation. PR1269525
- On SRX Series devices, Stream Control Transmission Protocol (SCTP) packet is having incorrect SCTP checksum after the payload reaches NAT. PR1310141

Network Management and Monitoring

- On SRX Series devices, when J-flow is enabled, for multicast traffic and installs **extern nexthop** during installing the multicast Composite Nexthop. However, when you uninstall the composite Nexthop, it does not free the **extern nexthop**, which results in the jtree memory leak. PR1276133

Platform and Infrastructure

- Memory leak occurs on SRX Series devices chassis cluster when em0 or em1 interface is down. PR1277136
- XLP lost heartbeat (SPU hang) is not detected timely by hardware monitoring, too long until RG1+ failover. PR1300804

Routing Policy and Firewall Filters

- On SRX550M devices, MAC entries in VPLS instance never aged out. PR1295962
- On SRX1500 devices, the IS-IS adjacency remains down when using IRB interface. PR1300743
- DHCP relay stops working if DHCP server configuration is deactivated on the same device. PR1302910
- The Domain Name System (DNS) configured in the address-book fails to resolve the IP address. PR1304706

System Logging

- The logs from syslog **RT_FLOW: FLOW_REASSEMBLE_SUCCEED: Packet merged** might cause high CPU usage on RE. PR1278333

User Access and Authentication

- SRX device fails to upgrade Junos image when you use unlink and partition option at the same time. PR1299859

VPN

- On SRX Series devices, **show host server name-server host** command fails when source address is specified under name server configuration. PR1307128

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 9
- Migration, Upgrade, and Downgrade Instructions on page 14

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X49-D120 for the SRX Series documentation.

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 and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases on page 14

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 12.3X48, 15.1X49, 17.3 and 17.4 are EEOL releases. You can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4. 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 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 7
- Known Issues on page 9
- Resolved Issues on page 11

Product Compatibility

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

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.

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://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 https://www.juniper.net/documentation/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 https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://www2.juniper.net/kb/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/

- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- 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://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 https://www.juniper.net/documentation/feedback/.

Revision History

13, March 2018—Revision 4— Junos OS 15.1X49-D120 – SRX Series.

18, December 2017—Revision 3— Junos OS 15.1X49-D120 – SRX Series.

15, November 2017—Revision 2— Junos OS 15.1X49-D120 – SRX Series.

08, November 2017—Revision 1— Junos OS 15.1X49-D120 – SRX Series.