Release Notes: Junos® OS Release 15.1X49-D75 for the SRX Series

Release 15.1X49-D75
25 April 2017
Revision 5

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-D75 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-D75 supports the following devices:

- Branch SRX Series devices: SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory (SRX550M)
- Mid-range SRX Series devices: SRX1500, SRX4100, and SRX4200. These mid-range devices are referred as SRX1500, SRX4100, and SRX4200 in this Release Notes.
- High-end SRX Series devices: 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).
- vSRX

For more details about SRX Series high-end hardware and software compatibility, please see http://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-D75 for the SRX Series devices.

Release 15.1X49-D75 Software Features

Dynamic Host Configuration Protocol (DHCP)

- Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI will be supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

  WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

  WARNING: Please see documentation for updated commands.

  To ensure uninterrupted service to existing user implementation of DHCP relay service, the following configuration items are identified as missing (edit and interface hierarchies) between the old DHCPD and the new JDHCPD configurations:

  set forwarding-options helpers bootp description
  set forwarding-options helpers bootp client-response-ttl
  set forwarding-options helpers bootp maximum-hop-count
  set forwarding-options helpers bootp minimum-wait-time
  set forwarding-options helpers bootp vpn
  set forwarding-options helpers bootp relay-agent-option
  set forwarding-options helpers bootp dhcp-option82

  and the interface hierarchy:

  set forwarding-options helpers bootp interface *interface-name* description
  set forwarding-options helpers bootp interface *interface-name* client-response-ttl
  set forwarding-options helpers bootp interface *interface-name* maximum-hop-count
  set forwarding-options helpers bootp interface *interface-name* minimum-wait-time
  set forwarding-options helpers bootp interface *interface-name* vpn
  set forwarding-options helpers bootp interface *interface-name* relay-agent-option
  set forwarding-options helpers bootp interface *interface-name* dhcp-option82

  NOTE: For Junos OS Release 15.1X49-D75, only the vpn option for JDHCPD is implemented.

Ethernet Switching

- **Ethernet switching feature support for SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting with Junos OS Release 15.1X49-D75, Ethernet switching supports Ethernet OAM connectivity fault management (CFM) in switching mode.

  CFM features can be configured on GE, XE, very-high-bit-rate digital subscriber line (VDSL), and Point-to-Point Protocol over Ethernet (PPPoE) interfaces. CFM includes fault monitoring, path discovery, fault isolation, and performance measurement functionalities.

  NOTE: To enable CFM on an Ethernet interface, you must configure maintenance domains, maintenance associations, and maintenance association end points (MEPs).

Interfaces and Routing

- **Path MTU support for IPv6 over GRE**—Starting with Junos OS Release 15.1X49-D75, path maximum transmission unit (PMTU) is supported on IPv6 GRE interfaces. IPv6 GRE tunnel PMTU uses the PMTU mechanism of the underlying IPv6 layer of the Junos stack. The underlying IPv6 PMTU discovery timeout has a default value of 10 minutes and is configurable; using the **ipv6-path-mtu-discovery-timeout** command option. The GRE tunnel layer PMTU discovery timeout has a fixed value of 13 minutes.

  When an IPv6 GRE interface receives an **ICMPv6 Packet Too Big message**, the MTU of the interface is reduced to either the MTU value in the message or to 1280 (IPv6 minimum link MTU), whichever is higher. A 13-minute timer is started at the tunnel layer. After tunnel timeout expiry, a check is made whether the IPv6 PMTU timeout has already occurred. If it has, the tunnel MTU reverts to the default value. If not, a new timer for 13 minutes is started for a subsequent check.

VPNs

- **Group VPNv2 servers and members supported on SRX4100 and SRX4200 devices**—Starting with Junos OS Release 15.1X49-D75, SRX4100 and SRX4200 devices can operate as Group VPNv2 servers or members that are compliant with RFC 6407, *The Group Domain of Interpretation (GDOI)*. You can configure SRX4100 or SRX4200 devices as Group VPNv2 server clusters; server clusters provide group controller/key server (GCKS) redundancy and scaling for Group VPNv2 members.

  [See Group VPNv2 Overview.]

Related Documentation

- Migration, Upgrade, and Downgrade Instructions on page 36
- Changes in Behavior and Syntax on page 7
- Known Behavior on page 20
- Known Issues on page 26

- Resolved Issues on page 32

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-D75.

AppSecure

- Starting with Junos OS Release 15.1X49-D70, the **show services ssl proxy statistics** command output is modified to include a new field **sessions bypassed: low memory**. This field displays the number of proxy sessions that are bypassed because the low memory on Packet Forwarding Engine.
- When you upgrade or downgrade an application signature package, an error message is displayed if there is any mismatch of application IDs (unique ID number of an application signature) between the protocol bundles and the applications associated with the IDs. This scenario occurs when AppFW and AppQoS rules are configured. An example message follows:

  ```
  Please resolve following references and try it again [edit class-of-service
  application-traffic-control rule-sets RS8 rule 1 match application junos:CCPROXY]
  ```

  As a workaround, disable AppFW and AppQoS rules before upgrading or downgrading an application signature package. You can reenable AppFW and AppQoS rules once the upgrade or downgrade procedure is complete.
- On SRX300, SRX320, SRX340, and SRX345 devices, AppSecure is part of Juniper Networks Secure Edge software or IPS subscription license. 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.

Authentication, Authorization and Accounting (AAA)

- Starting in Junos OS Release 12.1X47-D45, the **options no-hostname** is added to the dhcp-client configuration. You set the no-hostname if you do not want the DHCP client to send the hostname with the packets (DHCP option code 12).
- On SRX340 and SRX345 devices, the factory-default configuration has a generic HTTP configuration. To use **ge** and **fxp0** ports as management ports, you must use the **set system services web-management http** command. The Web management HTTP and HTTPS interfaces are changed to fxp0.0 and from **ge-0/0/1.0** through **ge-0/0/7.0**.

Chassis Cluster

- Starting in Junos OS Release 15.1X49-D70, the **set chassis routing-engine bios uninterrupt** command is introduced on SRX300, SRX320, SRX340, and SRX345 devices to disable user inputs at U-boot and boot loader stage.
- **Chassis cluster initial hold timer**—Starting with Junos OS Release 15.1X49-D60, the initial hold timer is extended from 30 seconds to 120 seconds in chassis clusters on SRX340 and SRX345 devices.
- **Chassis cluster new display value** Starting in Junos OS Release 15.1X49-D60, a new field, **security**, has been added to the **show chassis cluster interfaces** command to display the status of MACsec on control and fabric interfaces.
- **Chassis cluster ineligible timer**—Starting with Junos OS Release 15.1X49-D60, the ineligible timer is 5 minutes when MACsec on the chassis cluster control port is enabled on SRX340 and SRX345 devices.
- **802.1x-protocol-daemon**—Starting with Junos OS Release 15.1X49-D60, the 802.1x protocol process (daemon) does not support restart on SRX340 and SRX345 devices.
- 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.
- Starting with Junos OS Release 15.1x49-D70, there is a change in the method for calculating the memory utilization by a Routing Engine. The inactive memory is now considered free and is no longer included in the calculation of memory utilization. That is, the value for used memory shown in the output of the **show chassis routing-engine** command decreases and results in more memory to be available for other processes.

CLI

- **Discard option support with IP-monitoring**—Starting with Junos OS Release 15.1X49-D60, a new route option, **discard**, has been introduced to IP-monitoring to be able to discard a route instead.

  To enable the **discard** option, use the following CLI command:

  set services ip-monitoring policy *<policy-name>* **then preferred-route route** *<prefix>* **discard**

- 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.

Dynamic Host Configuration Protocol (DHCP)

- Starting with Junos OS Release 15.1X49-D60, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP

CLI will be supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

To ensure uninterrupted service to existing user implementation of DHCP relay service, the following configuration items are identified as missing (edit and interface hierarchies) between the old DHCPD and the new JDHCPD configurations:

set forwarding-options helpers bootp description
set forwarding-options helpers bootp client-response-ttl
set forwarding-options helpers bootp maximum-hop-count
set forwarding-options helpers bootp minimum-wait-time
set forwarding-options helpers bootp vpn
set forwarding-options helpers bootp relay-agent-option
set forwarding-options helpers bootp dhcp-option82

and the interface hierarchy:

set forwarding-options helpers bootp interface *interface-name* description
set forwarding-options helpers bootp interface *interface-name* client-response-ttl
set forwarding-options helpers bootp interface *interface-name* maximum-hop-count
set forwarding-options helpers bootp interface *interface-name* minimum-wait-time
set forwarding-options helpers bootp interface *interface-name* vpn
set forwarding-options helpers bootp interface *interface-name* relay-agent-option
set forwarding-options helpers bootp interface *interface-name* dhcp-option82

Ethernet Switching

- **VLAN Range for SRX300, SRX320, SRX340, SRX345, and SRX550M devices**—Starting with Junos OS Release 15.1X49-D75, the VLAN range from 1 to 4094 on inet interfaces and the VLAN range from 1 to 3967 on Ethernet switching interfaces. On Ethernet switching interfaces, VLAN range from 3968 to 4094 falls under the reserved VLAN address range, and the user is not allowed to configure VLANs in this range.

Flow-based and Packet-based Processing

- **Source address for SRX5400, SRX5600, and SRX5800 devices and vSRX2.0 instances**—Starting with Junos OS 15.1X49-D60, management traffic can originate from a specific source address for Domain Name System (DNS) names.

  Consider the following when you configure the source address for DNS:

  - Only one source address can be configured as the source address for each DNS server name.
  - IPv6 source addresses are supported for IPv6 DNS servers, and only IPv4 addresses are supported for IPv4 DNS servers. You cannot configure an IPv4 address for an IPv6 DNS server or an IPv6 address for an IPv4 DNS server.

  To have all management traffic originate from a specific source address, configure the system name server and the source address. For example:

```
user@host# set system name-server 5.0.0.1 source-address 4.0.0.3
```

General Packet Radio Service (GPRS)

- Starting with Junos OS Release 15.1X49-D70, the Serving GPRS Support Node (SGSN) and a Gateway GPRS Support Node (GGSN) of the GTPv1 or GTPv2 nodes cannot communicate with the GTPv0 node. If a device sends a GTPv1 or GTPv2 message to update the tunnels created by GTPv0, these messages are dropped and the GTPv0 tunnel will not be updated.

Installation and Upgrade

- Starting in Junos OS Release 15.1X49-D60, on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices, the following factory-default configurations are changed:
  - The **name-server** statement, used to configure one or more Domain Name System (DNS) name servers, is changed to 8.8.8.8 and 8.8.8.4. Previously, it was 208.67.222.222 and 208.67.220.220.
  - A new system service, NETCONF service over SSH, is introduced at the **[edit system services]** hierarchy:

    edit system services netconf ssh
  - The following configuration setting for HTTPS (secure management) access using the J-Web interface is changed. Now, there is no need to specify the interface details for J-Web management. With this configuration, you can manage the device from any interface through HTTPS.

    edit system services web-management https interface [irb.0]
  - A license autoupdate URL (https://ae1.juniper.net/junos/key_retrieval) is now supported under the **[edit system]** hierarchy:

    ```
    license {
      autoupdate {
        url https://ae1.juniper.net/junos/key_retrieval;
      }
    }
    ```
  - A new system log configuration is introduced to configure system log messages to record all commands entered by users and all authentication or authorization attempts under the **[edit system]** hierarchy:

    ```
    syslog {
      archive size 100k files 3;
      user * {
        any emergency;
      }
      file messages {
        any notice;
        authorization info;
      }
      file interactive-commands {
        interactive-commands any;
    ```

```
    }
}
```

- Factory-default configuration—Starting with Junos OS Release 15.1X49-D50, Layer 2 Ethernet switching is not supported on the same interface for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  The **system autoinstallation interfaces <interface names>** command and the **set interface <interface names> unit 0 family ethernet-switching** command cannot be configured on the same interface.

  NOTE: **USB auto-installation is not supported on SRX1500 devices and vSRX instances.**

  In Junos OS Release 15.1X49-D40 and earlier, configuring autoinstallation using USB and Layer Ethernet switching was supported on the same interface. However, the command caused the interface-control (dcd) process to exit, resulting in improper installation of the interface-related configurations.

- Starting in Junos OS Release 15.1X49-D50, the **request system scripts add *package-name* no-copy | unlink** command is updated to include the following options for installing AI Script install packages on SRX Series devices in a chassis cluster:

  - **master**- Install AI script packages on the primary node.
  - **backup**- Install AI script packages on the secondary node.

  This enhancement eliminates the need for separate AI script installations on the primary node and the secondary node.

Interfaces and Routing

- In Junos OS Release 15.1X49-D40 and earlier, on all SRX Series devices, GARP packets were sent out only for one IP address per IFL during RG1+ failover.

  Starting with Junos OS Release 15.1X49-D50, the IP address count per IFL during RG1+ failover has been enhanced to support up to eight IP addresses when sending GARP packets.

- **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.

- **Routing Policy and Firewall Filters**—Starting with Junos OS Release 15.1X49-D70, the **bfd-liveness-detection** command includes the description field. The description is an attribute under the **bfd-liveness-detection** object. This field is applicable only for the static routes.

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, the following new CLI options are introduced:
  - The **checksum-validate** option has been added to the following hierarchies:

    [**edit security idp custom-attack ipv4_cust attack-type signature protocol ipv4**]

    [**edit security idp custom-attack tcp_cust attack-type signature protocol tcp**]

    [**edit security idp custom-attack udp_cust attack-type signature protocol udp**]

    [**edit security idp custom-attack icmp_cust attack-type signature protocol icmp**]

    [**edit security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6**]

    To configure this option, use the following commands:

    set security idp custom-attack ipv4_cust attack-type signature protocol ipv4 checksum-validate

    set security idp custom-attack tcp_cust attack-type signature protocol tcp checksum-validate

    set security idp custom-attack udp_cust attack-type signature protocol udp checksum-validate

    set security idp custom-attack icmp_cust attack-type signature protocol icmp checksum-validate

    set security idp custom-attack icmpv6_cust attack-type signature protocol icmpv6 checksum-validate
  - The new **checksum-validate** option allows you to specify a particular checksum to match. The following example shows a command to validate the user-specified checksum of match equal value 0x20:

    ```
    set security idp custom-attack ipv4_cust attack-type signature protocol ipv4
     checksum-validate match equal value 0x20
    ```

  - The **routing-header** option and the **destination-option** option have been added to the [**edit security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header**] hierarchy. The **routing-header** option inspects the **routing-header** type field and reports a custom attack if a match with the specified value is found. The **destination-option** option inspects the header option type of **home-address** and **option-type** field in the extension header and reports a custom attack if a match is found.

    To configure these options, use the following commands:

    set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header routing-header

    set security idp custom-attack ipv6_cust attack-type signature protocol ipv6 extension-header destination-option

NOTE: For extension header of subtype routing-header, all type of inspections are supported as per RFC.

For extension header of subtype destination-option, the home-address and the option-type field type of inspections are supported.

- On all SRX Series devices, the following new CLI commands are introduced:
  - The new **ihl** option at the [**edit security idp custom-attack ipv4_custom attack-type signature protocol ipv4**] hierarchy level is used to inspect the length of the IPv4 header. To configure the **ihl** option, use the following command:

    ```
    set security idp custom-attack ipv4_custom attack-type signature protocol
    ipv4 ihl
    ```

  - The new **reserved** option at the [**edit security idp custom-attack tcp_custom attack-type signature protocol tcp**] hierarchy level is used to inspect the three reserved bits in the TCP header. To configure the **reserved** option, use the following command:

    ```
    set security idp custom-attack tcp_custom attack-type signature protocol tcp
     reserved
    ```

- On SRX Series devices, starting for Junos OS Release 15.1X49-D50, a new CLI option **drop-on-syn-in-window** is introduced for controlling the IDP behavior when SYN is seen in the TCP window. To enable this option use the **set security idp sensor-configuration re-assembler drop-on-syn-in-window** command.

  When the **sensor-configuration** option is:

  - Disabled (Not set (default))—Drops the packet and ignore current session.
  - Enabled (Set)—Drops the packet after IDS processing is complete.

Junos OS XML API and Scripting

- Starting in Junos OS Release 15.1X49-D60, the Rest API is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, SRX5400, SRX5600, and SRX5800 devices.

J-Web

- J-Web supports only the new CLI configurations. For more information, see https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16991

Layer 2 Features

- **LLDP and LLDP-MED for SRX300, SRX320, SRX340, SRX345, SRX550M and SRX1500 devices**—Starting with Junos OS Release 15.1X49-D60, Link Layer Discovery Protocol (LLDP) and LLDP-Media Endpoint Discovery (MFD) are enabled on SRX300, SRX320, SRX340, SRX345, SRX550M and SRX1500 devices.
- **IRB logical interface statistics**—Starting with Junos OS Release 15.1X49-D60, interface statistics are supported on the IRB logical interface for SRX300, SRX320, SRX340, SRX345, and SRX550M devices.

  To verify the IRB logical interface statistics, enter the **show interfaces irb.<index> extensive** and **show interfaces irb.<index>statistics** commands.
- **Global MAC limit**—Starting with Junos OS Release 15.1X49-D60, the maximum number of MAC addresses learned on all logical interfaces on the SRX1500 device is 24,575. When this limit is reached, incoming packets with a new source MAC address will be dropped.
- Starting in Junos OS Release 15.1X49-D50, the factory-default configuration of the SRX300, SRX320, SRX340, and SRX345 devices is switching mode. When these devices are loaded or reset with the factory-default configuration, they start up in switching mode.
- **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.]

MPLS

- Starting in Junos OS Release 15.1X49-D50, the **vrf-table-label** statement allows mapping of the inner label to a specific Virtual Routing and Forwarding (VRF). This mapping allows examination of the encapsulated IP header at an egress VPN router. For SRX Series devices, the **vrf-table-label** statement is currently supported only on physical interfaces. As a workaround, deactivate **vrf-table-label** or use physical interfaces.

Multicast

- Starting with Junos OS Release 15.1X49-D40, for all SRX Series devices, configuration of patterns in standard PCRE format is supported in the custom attacks.

NAT

- Starting with Junos OS Release 15.1X49-D60, when you delete or modify a NAT rule, a NAT pool, or an interface address, the related NAT bindings might not be deleted immediately. In addition, the related session scan for the NAT rule and NAT pool might not be deleted as quickly as in previous releases.
- In Junos OS Release 15.1X49-D45 and earlier, on SRX Series devices and in vSRX instances, the system log messages in IDP attack logs contained only IPv4-based NAT address fields.

  Starting in Junos OS Release 15.1X49-D50, the system log messages in IDP attack logs contain both IPv4-based and IPv6-based NAT address fields.
- Source NAT pool port configuration options—Starting with Junos OS Release 15.1X49-D40, the **port-overloading-factor** option and the **port-range** option at the [edit security nat source pool *source-pool-name* port] hierarchy level can be configured together. Prior to Release 15.1X49-D40, the options would overwrite each other.

  [See *port (Security Source NAT)*]

Network Time Protocol

- Starting in Junos OS Release 15.1X49-D10, on all SRX Series devices, when the NTP client or server is enabled in the [**edit system ntp**] hierarchy, the REQ_MON_GETLIST and REQ_MON_GETLIST_1 control messages supported by the monlist feature within the NTP client or server might allow remote attackers, causing a denial of service. To identify the attack, apply a firewall filter and configure the router's loopback address to allow only trusted addresses and networks.

Public Key Infrastructure

- Generating a public key infrastructure (PKI) signature of 512 bits for a digital certificate with Digital Signal Algorithm (DSA) or RSA encryption is being deprecated on SRX Series devices and vSRX instances:

  - Starting with Junos OS Release 15.1X49-D75, the **size 512** option is not supported in the CLI command **request security pki generate-key-pair certificate-id** *certificate-id-name* **type dsa**. Instead, the **size** must be **1024** (the default value), **2048**, or **4096**.
  - The **size 512** option is being deprecated in the CLI command **request security pki generate-key-pair certificate-id** *certificate-id-name* **type rsa** and will no longer be supported in a future release. Instead, the **size** must be **1024**, **2048** (the default value), or **4096**.

- The **request security pki local-certificate enroll** command now includes the **cmpv2** and **scep** keywords for CMPv2 and SCEP certificate enrollment. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **enroll** keyword. Starting with this release, SCEP enrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **enroll** keyword will be deprecated.

  The **auto-re-enrollment** configuration statement at the [**edit security pki**] hierarchy level now includes the **cmpv2** and **scep** keywords for automatic reenrollment of local certificates using CMPv2 or SCEP. Each keyword has configurable options. In previous releases, SCEP enrollment parameters were entered after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement. Starting with this release, SCEP reenrollment parameters should be entered after the **scep** keyword. In a future release, SCEP enrollment parameters after the **set security pki auto-re-enrollment certificate-id** *certificate-id-name* statement will be deprecated.

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 Logs

- Starting in Junos OS Release 15.1X49-D70, the **no-tls-certificate-check** parameter is visible and disabled by default. When you enable the **no-tls-certificate-check** parameter, the Lightweight Directory Access Protocol (LDAP) server certificate will not be validated.
- In Junos OS Release 15.1X49-D30 and earlier, the severity parameter for RT_SRC_NAT_PBA messages was “debug”.

Starting in Junos OS Release 15.1X49-D40, the severity parameter has changed. The RT_SRC_NAT_PBA messages are now fixed with severity as “info”.

The following example shows RT_SRC_NAT_PBA messages before Junos OS Release 15.1X49-D40:

16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity debug (7)

Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

The following example shows RT_SRC_NAT_PBA messages in Junos OS Release 15.1X49-D40, indicating the change in the severity parameter:

16:32:43.760393 In IP (tos 0x0, ttl 254, id 16957, offset 0, flags [none], proto: UDP (17), length: 218) 192.0.2.4.syslog > 192.0.2.2.syslog: SYSLOG, length: 190 Facility user (1), Severity info (6)

Feb 5 16:32:49 RT_NAT: RT_SRC_NAT_PBA_ALLOC: Subscriber 192.0.2.2 used/maximum [1/32] blocks, allocates port block [27200-27263] from 198.51.100.3 in source pool src-nat-pool-1 lsys_id: 0\012

- Starting in Junos OS Release 15.1X49-D70, new parameters are added to the structured log fields of the antivirus, antispam, content, and apppxy system log messages.

  The following example shows the structured log fields of **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages before Junos OS Release 15.1X49-D70:

  AntiVirus: Virus detected: from <source-address>:<source-port> to <destination-address>:<destination-port> source-zone <source-zone-name> <filename> file <temporary-filename> virus <name> URL:<url> username <username> roles <roles>

  AntiSpam: SPAM detected: <source-name> (<source-address>) <action> reason: <reason> username <username> roles <roles>

  Content Filtering: <argument> (<profile-name> from <source-address> is <action> due to <reason> username <username> roles <roles>

  ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <percentage-value> connections, which exceeded the maximum allowed <maximum-value> connectionsusername <username> roles <roles>

  ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>)

  The following example shows **AV_VIRUS_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT, CONTENT_FILTERING_BLOCKED_MT, APPPXY_RESOURCE_OVERUSED_MT, and APPPXY_SESSION_ABORT_MT** messages

in Junos OS Release 15.1X49-D70, indicating the newly added parameters in the structured log fields:

AntiVirus: Virus detected: <source-address>:<source-port>-><destination-address>:<destination-port> source-zone="<source-zone-name>" profile-name="<profile-name>" file="<filename>" temp_file="<temporary-filename>" virus="<name>" URL="<url>" username="<username>" roles="<roles>"

AntiSpam: SPAM detected: name="<source-name>" source-ip=(<source-address>) profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

Content Filtering: protocol="<argument>" <source-address>:<source-port>-><destination-address>:<destination-port> profile-name="<profile-name>" action="<action>" reason="<reason>" username="<username>" roles="<roles>"

ApplicationProxy: Suspicious client <source-address>:<source-port>->(<destination-address>:<destination-port>) used <current-connections> connections, which exceeded the maximum allowed <maximum-value> connections. policy-name <policy-name> username <username> roles <roles>

ApplicationProxy: session from <source-address>:<source-port> to <destination-address>:<destination-port> aborted due to <error-message> (code <error-code>), policy-name <policy-name>

- Starting in Junos OS Release 15.1X49-D75, on SRX1500, SRX4100, and SRX4200 Series devices and vSRX instances, the **set security log stream ${*stream_name*}** command is required to configure the stream log. The source address and source interface attributes are no longer required.

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 ethernet-switching no-packet-flooding** command, then multicast packets such as OSPFv3 hello packets are dropped.

Unified Threat Management (UTM)

- In Junos OS Release 15.1X49-D60 for SRX1500 devices and vSRX instances and in Junos OS Release 15.1X49-D70 for SRX4100 and SRX4200 devices:
  - The number of supported UTM policies, profiles, MIME patterns, filename extensions, and protocol commands is 500.

  - The number of supported custom URL patterns and custom URL categories is 1000.

- Starting with Junos OS Release 15.1X49-D60, on SRX1500 Services Gateways and vSRX instances, UTM policies, profiles, MIME patterns, filename extensions, and protocol-command numbers are increased to 500; custom URL patterns and custom URL categories are increased to 1000.

- In Junos OS Release 15.1X49-D45 and earlier, the structured log of Web filtering has inappropriate field names.

  Starting in Junos OS Release 15.1X49-D50, the structured log fields have changed. The corresponding fields in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are now fixed with the appropriate structured log fields.

  The following example shows WEBFILTER_URL_BLOCKED messages before Junos OS Release 15.1X49-D50:

  <12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071" destination-address="198.51.100.2" destination-port="80" name="cat1" error-message="BY_BLACK_LIST" profile-name="uf1" object-name="www.example.com" pathname="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked "192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

  The following example shows WEBFILTER_URL_BLOCKED messages in Junos OS Release 15.1X49-D50, indicating the change in structured log fields:

  <12>1 2016-02-18T01:32:50.391Z utm-srx550-b RT_UTM - WEBFILTER_URL_BLOCKED [junos@2636.1.1.1.2.86 source-address="192.0.2.3" source-port="58071" destination-address="198.51.100.2" destination-port="80" category="cat1" reason="BY_BLACK_LIST" profile="uf1" url="www.example.com" obj="/" username="N/A" roles="N/A"] WebFilter: ACTION="URL Blocked" 192.0.2.3(58071)->198.51.100.2(80) CATEGORY="cat1" REASON="BY_BLACK_LIST" PROFILE="uf1" URL=www.example.com OBJ=/ username N/A roles N/A

  The structured log field changes in the UTM Web filter logs WEBFILTER_URL_BLOCKED, WEBFILTER_URL_REDIRECTED, and WEBFILTER_URL_PERMITTED are as follows:

  - **name -> category**
  - **error-message -> reason**
  - **profile-name -> profile**
  - **object-name -> url**
  - **pathname -> obj**

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.

VPNs

- The **show security dynamic-vpn client version** command is not supported for dynamic VPN.
- Starting with Junos OS Release 15.1X49-D70, a warning message is displayed if you configure the **establish-tunnels immediately** option at the [**edit security ipsec vpn *vpn-name***] hierarchy level on AutoVPN hubs with point-to-point tunnel interfaces. Committing the configuration will succeed, however the **establish-tunnels immediately** configuration is ignored. The state of the point-to-point tunnel interface will be up all the time.

  The **establish-tunnels immediately** option is not appropriate for AutoVPN hubs with point-to-point tunnel interfaces because multiple VPN tunnels may be associated with a single AutoVPN configuration.

Zones and Interfaces

- System services configuration option—Starting with Junos OS Release 15.1X49-D40, the **system-services** option at the **[edit security zones security-zone *zone-name* host-inbound-traffic]** hierarchy level and the **system-services** option at the **[edit security zones security-zone *zone-name* interfaces *interface-name* host-inbound-traffic]** hierarchy level no longer support the configuration of the Session Initiation protocol (SIP) system service.

  [See *system-services (Security Zones Interfaces)* and *system-services (Security Zones Host Inbound Traffic)*]

Related Documentation

- New and Changed Features on page 5
- Resolved Issues on page 32
- Known Behavior on page 20
- Known Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 36

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 15.1X49-D75.

AppSecure

- When you delete or disable a custom application signature, and the configuration commit fails, the application system cache (ASC) entry is not cleared completely; instead, a base application in the path of custom application will be reported in ASC.
- 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.

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

Class of Service

The following limitations apply to CoS support on VPN st0 interfaces:

- Currently, the maximum number for software queues is 2048. If the number of st0 interfaces exceeds 2048, not enough software queues can be created for all the st0 interfaces.
- Only route-based VPN can apply st0 CoS. Table 1 on page 21 describes the st0 CoS feature support for different types of VPN.

Table 1: CoS Feature Support for VPN

Classifier Features	Site-to-Site VPN (P2P)	ADVPN/AutoVPN (P2MP)
Classifiers, policers, and rewriting markers	Supported	Supported
Queueing, scheduling, and shaping based on st0 logical interfaces	Supported	Not supported

Table 1: CoS Feature Support for VPN *(continued)*

Queueing, scheduling, and shaping based on virtual channels	Supported	Supported

- On branch SRX Series devices, one st0 logical interface can bind to multiple VPN tunnels. The eight queues for the st0 logical interface cannot reroute the traffic to different tunnels, so pre-tunneling is not supported.

  NOTE: The virtual channel feature can be used as a workaround on branch SRX Series devices.

- When defining a CoS shaping rate on an st0 tunnel interface, consider the following restrictions:
  - The shaping rate on the tunnel interface must be less than that of the physical egress interface.
  - The shaping rate only measures the packet size that includes the inner Layer 3 cleartext packet with an ESP/AH header and an outer IP header encapsulation. The outer Layer 2 encapsulation added by the physical interface is not factored into the shaping rate measurement.
  - The CoS behavior works as expected when the physical interface carries the shaped GRE or IP-IP tunnel traffic only. If the physical interface carries other traffic, thereby lowering the available bandwidth for tunnel interface traffic, the CoS features do not work as expected.
- On SRX550M, SRX5400, SRX5600, and SRX5800 devices, bandwidth limit and burst size limit values in a policer configuration are a per-SPU, not per-systerm limitation. This is the same policer behavior as on the physical interface.

Flow-based and Packet-based Processing

- On SRX340 and SRX345 devices, fabric interfaces must be configured such that the Media Access Control Security (MACsec) configurations are local to the nodes. Otherwise, the fabric link will not be reachable.
- The legacy DHCPD (DHCP daemon) will soon be deprecated. The DHCP CLI (jdhcpd process) is supported on all SRX Series devices. For more information, see https://kb.juniper.net/InfoCenter/index?page=content&id=TSB16991
- You can configure a security master password that allows you to encrypt shared secrets, such as RADIUS passwords and IKE preshared keys. Having a master password allows devices to encrypt passwords in such a way that only devices running Junos OS that have knowledge of the master password can decrypt the encrypted passwords. The following limitations apply:
  - The master password cannot be edited, deleted, or modified in the config-private mode.
  - For security reasons, the **deactivate system master-password** option is not supported.

  - Rolling back to a previous configuration that used a different master password is not allowed.

- On SRX Series devices, the default mode for processing traffic is flow mode. To configure an SRX Series device as a border router, you must change the mode from flow-based processing to packet-based processing. Use the **set security forwarding-options family mpls mode packet-based** statement to configure the SRX device to packet mode. You must reboot the device for the configuration to take effect.

General Packet Radio Service (GPRS)

- Starting in Junos OS Release 15.1X49-D40, the SCTP flow session utilizes a connection tag to more finely distribute SCTP traffic across SPUs on SRX5400, SRX5600, and SRX5800 devices that support the SCTP ALG. The connection tag is decoded from the SCTP vtag. A separate SCTP session will be created for each of the first three packets—that is, one session for INIT, INIT-ACK, and COOKIE-ECHO, respectively. Because, the reverse-direction traffic has its own session, the session can no longer match the existing forward-direction session and pass through automatically. Therefore, similar to the forward-direction policy, an explicit policy is needed for approving the reverse-direction SCTP traffic. In this scenario, the SCTP flow session requires a bidirectional policy configuration to be established for even a basic connection.
- On SRX5000 line 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

- For integrated user firewall in Junos OS 151.X49-D50 you cannot use the Primary Group, whether by its default name of Domain Users or any other name (if you happened to have changed it), in integrated user firewall configurations.

  When a new user is created in Active Directory, the user is added to the global security group Primary Group which is by default called Domain Users. The Primary Group is less specific than other groups created in Active Directory because all users belong to it. Consequently it can become very large.

IP Monitoring

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

Layer 2 Features

- In Junos OS Release 15.1X49-D75, the following are the limitations on SRX320, SRX340, SRX345, and SRX550M devices when configuring Ethernet connectivity fault

management (CFM) over very-high-bit-rate digital subscriber line (VDSL) or Layer 3 Interface:

- CFM Action Profiles are not supported on the Point-to-Point Protocol over Ethernet (PPPoE) logical interface.
- Synthetic loss measurement on demand is supported. Proactive synthetic loss measurement is not supported.
- When CFM over PPPOE is implemented, CFM should be applied on PPPoE logical interface and not on underlying interface.
- CFM over VDSL can be implemented as Maintenance Endpoint (MEP) and not as Maintenance Intermediate Point (MIP).
- CFM Higher level Pass-through over VDSL or Gigabit Ethernet interface in Layer 3 interface mode is not supported.
- For vlan tagged VDSL interface, CFM should always be applied on respective logical interface and not over physical interface.
- When CFM is enabled on VDSL, CFM packets are dropped randomly causing CFM sessions to flap based on timer when transit traffic exceeds line rate because VDSL mPIM cannot differentiate and prioritize CFM packets

- **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).
- In Junos OS Release 15.1X49-D40, the following features are not supported on SRX Series devices and vSRX instances:
  - Layer 2 transparent mode policer
  - Three-color policer

Multicast

- On all SRX Series devices, only 100 packets can be queued during pending (S, G) route. However, when multiple multicast sessions enter the route resolve process at the same time, buffer resources are not sufficient to queue 100 packets for each session.
- On all SRX Series devices, when a multicast route is not available, pending sessions are not torn down, and subsequent packets are queued. If no multicast route resolve comes back, then the traffic flow has to wait for the pending session to timed out. Then packets can trigger new pending session create and route resolve.

Platform and Infrastructure

- On all high-end SRX Series devices, when you enable a global services offloading policy utilizing IOC2 line-cards, the connections per second (CPS) rate might be reduced. It is recommended to utilize IOC3 line-cards to maximize the CPS rate, or alternatively, lower the session count to ensure that the IOC2 is capable of scaling. As a workaround, identify the sessions that must be offloaded and only enable services offloading on those sessions.

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.

USB autoinstallation

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

  NOTE: USB auto-installation is not supported on SRX1500 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.

VPN

- 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 SRX Series devices, configuring RIP demand circuits over P2MP VPN interfaces is not supported.
- On high-end SRX Series 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

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 7
- Known Issues on page 26
- Resolved Issues on page 32
- Migration, Upgrade, and Downgrade Instructions on page 36

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X49-D75.

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

- SRX5400, SRX5600, and SRX5800 devices support an additional check on the LDAP server's certificate during the TLS handshake for LDAP authentication by default. 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 server's certificate and accept the certificate without checking.

  PR1218357

Chassis Cluster

- On high-end SRX Series devices in chassis cluster, after reboot, if the secondary node (RG1) completes cold synchronize (CS) first, this might result in bidirectional RTO synchronization or incorrect direction for RTO synchronization. PR1138502
- On branch SRX Series devices in chassis cluster, when configuring Ethernet switching, the device reboots followed by a CLI warning message. Rebooting only one node in chassis cluster setup might lead to asynchronized chassis cluster status that is not supported, and this might result in the device to go to db mode. Reboot both the nodes in chassis cluster setup together to avoid the issue. PR1228473

Class of Service (CoS)

- On high-end SRX Series devices, when CoS on st0 interface is enabled and the incoming traffic rate destined for st0 interface is higher than 300K 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 to configure appropriate policer on the ingress interface to limit the traffic below 300K pps per SPU. PR1239021

Ethernet Switching

- On branch SRX Series devices in chassis cluster, Ethernet switching mode configurations do not work. PR1161372
- 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 branch SRX Series devices, the current Ethernet switching MAC aging is using software to age out bulk learned MAC addresses. You cannot age out specific MAC address learned at specific time immediately after the configured age. Theoretically, the MAC address might be aged out close to two times the configured age out time. PR1179089
- On SRX1500 devices configured in Ethernet switching mode, only few MAC entries are shown in the output of **show ethernet-switching table** command, even after MAC age out time. This issue is applicable only when MAC learning table has more than 17000 MAC entries. PR1194667
- On branch SRX Series devices, you cannot launch setup wizard after using the reset configuration button when the device is in Layer 2 Transparent mode. You can launch the setup wizard by using the reset configuration button on the device when the device is in switching mode. PR1206189
- On SRX1500 devices in Ethernet switching mode, an IRB interface located in a custom routing-instance is not reachable. PR1234000
- On SRX345 and SRX550M devices, frame carried with priority bit on Tag Protocol Identifier (TPID) will be lost when packet passes through with Layer 2 forwarding. PR1229021

Flow-based and Packet-based Processing

- On high-end SRX Series devices, when a device forwards traffic, a flowd core file is generated. This is a generic issue and does not impact any feature. PR1027306
- On SRX Series devices, default trusted-ca list (Trusted_CAs.pem) is not bundled with Junos. PR1044944
- On SRX550M devices, traffic processed by the serialization process is dropped when the maximum limit of serialization sessions (32,000) is exceeded. As a result, advanced services such as IDP, ALG, GTP, SCTP, and AppSecure are impacted. The limitation of maximum serialization sessions should be increased to 64000. PR1061524
- On branch SRX Series devices, the maximum-sessions value is displayed incorrectly. PR1094721
- On high-end SRX Series 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. PR1126885
- On SRX1500 devices, the log buffer size is increased 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. PR1133757
- On branch SRX Series devices, traffic does not pass with the maximum number of logical interfaces eight queues. PR1138997
- On SRX1500 devices, block-drop action option in Command and Control Spotlight Secure policy for custom_url_data feed does not work. PR1141745
- On SRX1500 devices, when CPU usage is very high (above 95%), there is possibility that the connection between AAMW process and PKID process can break. In this case, the AAMW daemon remains in initializing state until that connection is established. PR1142380
- On SRX1500 devices, after you change the revocation configuration of a CA profile, the change cannot be populated to the SSL-I revocation check. It is recommended to change SSL-I configuration to enable or disable certificate revocation list (CRL) checking instead of CA-profile configuration. PR1143462
- On SRX1500 devices in 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 enable the CRL checking again. PR1144280
- On high-end SRX Series devices, if revocation check is enabled in a CA-profile that does not have CRL information, then Packet Forwarding Engine (PFE) might stop working. PR1144836
- On SRX340 and SRX345 devices, half-duplex mode is not supported because BCM53426 does not support half-duplex mode. BCM5342X SoC port configurations, BCM53426 does not have QSGMII interface. Only the QSGMII port supports half-duplex mode. PR1149904

- On high-end SRX Series devices with SRX5K-MPC (IOC2) cards installed and np-cache feature enabled, low performance might be seen when fragmented traffic is present. PR1193769
- On SRX550M devices, when upgrading from Junos OS Release 15.1X49-D30 to a later version, upgrade fails. PR1237971

Integrated User Firewall

- On high-end SRX Series devices, if user or group name contains the following characters: **"*" (ASCII 0x2a), "(" (ASCII 0x28), ")" (ASCII 0x29), "\" (ASCII 0x5c) and NUL (ASCII 0x00)**, the query from the device to the LDAP server will time-out and might lead to high utilization of CPU. PR1157073

Interfaces

- 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. PR1133384
- On SRX300, SRX320, SRX340, and SRX345 devices, when you change the interface mode from **10m/no-auto-10m/no-auto** to **100m/no-auto-100m/no-auto**, interfaces might be down. PR1165942
- On SRX Series devices, the **show arp** command will show all the ARP entries learned from all interfaces. When Layer 2 global mode is switching, the ARP entries learned from IRB interface can only show one specific VLAN member port instead of the actual VLAN port learned in the ARP entries. PR1180949

J-Web

- 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. PR1140019
- On SRX Series devices in J-Web, when you login to the Web-authentication page, BAD_PAGE_FAULT will be seen. PR1180787
- On all branch SRX Series devices, error message is seen on J-Web when adding a custom-applications setting, while no error message is seen on the CLI for the same configuration. PR1183037
- On SRX1500 devices in J-Web, snapshot functionality **Maintain->Snapshot->Target Media->Disk ->Click Snap Shot** is not supported. PR1204587
- 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

Network Address Translation (NAT)

- On high-end SRX Series devices, security policies are not downloaded after performing ISSU from Junos OS Release 12.1X46-D40 to Junos OS Release 12.1X46-D45, 12.3X48-D10 or higher, when NAT is configured. PR1120951
- On SRX Series devices, internal IP addresses can communicate with each other on open ports when you use only **junos-persistent-nat** application in trust-to-trust policy with persistent NAT and Hairpin. This issue can be avoided when **destination-address drop-untranslated** is configured in the policy. PR1171160

Platform and Infrastructure

- On high-end SRX Series 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. PR1121262
- On high-end SRX Series devices, if 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 is caused 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 SRX Series devices, File Descriptor (FD) might leak on the httpd-gk process when system fails to connect to the mgd process management socket. PR1127512
- On SRX1500 devices, when RPM probe is configured for hardware timestamp-based probes, the RPM probes will be dropped by the RPM probe source (client). PR1147156
- On high-end SRX Series devices, flowd process might crash and cause traffic outage if the SPU CPU usage is higher than 80%. Therefore, some threads are in waiting status and the watchdog cannot be toggled timely causing the flowd process to crash. PR1162221
- On high-end SRX Series devices, in a rare occasion, after very long uptime (approximately above 650 days) the Network Processor (NP) component of the IO card might get stuck indeterminately. PR1175656
- On SRX Series devices, NP error occurs when service offline is enabled on NP-IOC. PR1210152
- On SRX4100 and SRX4200 devices, although the CLI is configurable, the following features are not supported:
  - GPRS
  - Group VPN and VPN Suite B
  - LACP with L2 Transparent Mode
  - Encrypted control links when in chassis cluster

  PR1214410

- On SRX4100 and SRX4200 devices, Layer 2 Link Aggregation Control Protocol (LACP) is not supported. PR1228371
- SRX4100 and SRX4200 devices does not support J-Flow Version 9 in chassis cluster configuration. PR1228375

Routing Policy and Firewall Filters

- On 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. PR969944
- On SRX5800 devices in chassis cluster, the flowd process crashes after a reboot with IPv6 security policies configured. PR1089272

Unified Threat Management (UTM)

- On 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 high-end SRX Series devices, under high CPS and UTM SAV interested traffic, the device might use 99% of CPU due to central lock of object cache memory allocation. There is no clear boundary since allocation race condition is varying. Basically, reducing traffic CPS could lower high CPU usage. PR967739
- On SRX Series devices with Sophos Antivirus (SAV) configured, some files that have size larger than the max-content-size might not go into fallback state. Instead, some protocols do not predeclare the content size. PR1005086
- On branch SRX Series devices, the statistics and counters of Security Intelligence and Sky Advanced Threat Prevention (ATP) might not be shown on CLI if frequent chassis cluster failovers are seen along with medium-high traffic going through for a long period of time. PR1234169

USB autoinstallation

- On branch SRX Series devices, when Juniper USB with part number RE-USB-4G-S (740-028898) is inserted in the USB slot while the device is ON, the device reboots. PR1214125

VPNs

- 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 branch SRX Series devices in chassis cluster, IPsec VPN tunnel which uses a PPPoE interface as the external interface will fail after RG0 failover. PR1143955
- On high-end SRX Series 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 SRX5600 devices, when tunnels are cleared between the client and SRX5600 cluster, and RG0 failover is seen on SRX5600 devices, there might be instances where tunnels do not come up initially. PR1227433
- On SRX5600 devices, if st0 interface is moved from one routing instance to another routing instance, there might be some traffic disruption. PR1241505

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 7
- Known Behavior on page 20
- Resolved Issues on page 32
- Migration, Upgrade, and Downgrade Instructions on page 36

Resolved Issues

This section lists the issues fixed in hardware and software in Junos OS Release 15.1X49-D75.

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 SRX Series devices, Trivial File Transfer Protocol (TFTP) ALG logging does not recognize the service TFTP, when both the source port and destination port are not known ports. PR1232026

Chassis Cluster

- On SRX Series devices in chassis cluster, PPPoE fails to establish session when RG0 and RG1 primary node is asymmetric. PR1230627
- On SRX550M devices in chassis cluster, the configuration synchronization monitoring might fail if the following configuration is enabled:
  - **set system encrypt-configuration-files**

  The configuration sync monitoring failure might result in disabling the secondary node after reboot. PR1235628
- On SRX5000 Series devices, when using Internet Key Exchange (IKE) in chassis cluster, memory buffer (mbuf) stall might trigger FPC alarms and RG failover. PR1236672
- On SRX4200 devices in a chassis cluster, the flowd process might crash and generate core dump under the following conditions:

- IPv6 IPsec VPN tunnel is established
- NAT is enabled for the IPv6 VPN traffic
- Performing failover for the VPN traffic related data-plane Redundancy Group (RG)

PR1237311

- On branch SRX Series devices in chassis cluster, secondary node fails to update AppID signature using scheduled update. PR1237421

Dynamic Host Configuration Protocol (DHCP)

- On branch SRX Series devices, **ndrapol** and **delegated-pool** cannot use the second range. PR1234243
- On branch SRX Series devices, use prefix-length mask-low or mask-high to configure **ndrapool** and **delegated pool**, and to open jdhcpd trace and core dump. PR1236167
- On SRX300 Series devices, the value of managed (M) bit cannot be reset if it is configured as true. PR1236548
- On high-end SRX Series devices, the flowd process might generate a core dump when running trace options for the cascaded DHCP with IPv6 prefix delegation. PR1242036

Ethernet Switching

- On SRX1500 devices, VLAN IDs ranging from 4073 to 4092 are reserved and should not be configured. However, when you create these VLANs, you will not be prompted for commit error as the system behavior is non predictable. PR1231457
- On SRX1500 devices, the CLI commands **request pppoe connect** and **request pppoe disconnect** does not work. PR1231804

Flow-based and Packet-based Processing

- Flowd core files are generated when NAT46 session activeness change from Z-mode operation to active-backup, at the same time fragment packet belonging to that session is being processed. PR1233879
- On SRX5400, SRX5600, and SRX5800 devices, Bidirectional Forwarding Detection (BFD) multihop for IPv6 does not work. PR1239016
- On SRX5600 devices, the flowd process might crash and generate core dump when the SecIntel (security-intelligence) is configured. PR1246679

General Routing

- On XL-based cards such as MPC or IOC3, PPE thread time-out errors are triggered when the FPC allocates illegal memory space for the forwarding state of routing operations. In certain cases, this results in packet loss depending on number of packets using this forwarding state. PR1100357

Interfaces

- On SRX300 and SRX320 devices, LACP is not supported. PR1165015
- On Q-in-Q port of branch SRX Series devices, IRB interface works on native VLAN ID. PR1225926
- On SRX1500 devices, front panel alarm LED does not turn amber even when the device has minor system alarm. PR1227138
- On SRX550M devices, when the **monitor traffic interface** command is executed for first time after reboot, and then stopped, forwarding in VPLS and Layer 2 circuits might stop. Forwarding is active again when the **monitor traffic interface** command is enabled, and stops when the **monitor traffic interface** command is disabled. PR1233209

J-Web

- On branch SRX Series devices in a J-Web configuration, commit fails when disabling the functions at "Authentication Source Priority Configuration". PR1241675

Network Management and Monitoring

- On high-end SRX Series devices, **set system time-zone** configuration does not affect time stamp in stream mode security log. PR1203833

Platform and Infrastructure

- On SRX5400, SRX5600, and SRX5800 devices, the log message **Warning! random engine is holding busy** is displayed frequently in /var/log/messages. PR1233408

Routing Policy and Firewall Filters

- On high-end SRX Series devices, when there is atleast one policy using the range address in a zone, the network security daemon (NSD) crashes after executing **show security shadow-policies** command. PR1232736

Simple Network Management Protocol (SNMP)

- On branch SRX Series devices, SNMP MIB OIDs **jnxOperating1MinAvgCPU** (Routing Engine CPU usage) always returns 100. PR1237331
- On SRX1500 devices, SNMP traps are not generated when power cable is unplugged, or when one of the PSU is plugged in or unplugged from the device. PR1242827

VPNs

- On branch SRX Series devices, the IRB interface cannot be used as an external interface with IPsec VPN. PR1166714
- Configuring IPsec authentication with manual SAs can cause SRX300 Series devices to crash. PR1230491

Related Documentation

- New and Changed Features on page 5
- Changes in Behavior and Syntax on page 7
- Known Behavior on page 20
- Known Issues on page 26
- Migration, Upgrade, and Downgrade Instructions on page 36

Documentation Updates

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

- In Junos OS Release 15.1X49-D70, content from the *Junos OS CLI User Guide* is available in Junos OS 15.1 CLI User Guide. On the 15.1X49-D70 page, click **CLI User Guide** to view information about the Junos OS command-line interface.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information; however, the Junos OS features described in the Junos OS 15.1 *CLI User Guide* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D70, content from the *Junos OS Installation and Upgrade Guide for Security Devices* is available in the*Junos OS 15.1 Installation and Upgrade Guide*. On the 15.1X49-D70 page, click **Installation and Upgrade** to view installation and upgrade information.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Installation and Upgrade Guide* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D70, content from the *Network Monitoring and Troubleshooting Guide for Security Devices* is available in the Network Management Administration Guide for Routing Devices. On the 15.1X49-D70 page, click **Network Monitoring and Troubleshooting** to view the *Junos OS 15.1 Network Management Administration Guide for Routing Devices*.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Network Management Administration Guide for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D70, the *Multicast Feature Guide for Security Devices* is available in *15.1 Multicast Protocols Feature Guide for Routing Devices*. On the 15.1X49-D70 page, click **Multicast** to view information on multicast concepts and configuration examples.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Multicast Protocols Feature Guide for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D60, content from the Junos OS *Routing Protocols Library for Security Devices* is available in the *15.1 Junos OS Routing Protocols Library for Routing Devices*. On the 15.1X49-D70 page, click **Routing Protocols** to view general routing protocol concepts and configuration information, including information about multitopology routing, interior gateway protocols (IS-IS, OSPF, RIP), and BGP.

  This guide does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in the Junos OS 15.1 *Junos OS Routing Protocols Library for Routing Devices* are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D70, information about MIBs is available in SNMP MIBS Explorer. On the 15.1X49-D70 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.

- In Junos OS Release 15.1X49-70, content from the *Junos OS Standards Reference*, APIs, and scripting guides are available in *15.1 Standards Reference* and API and Scripting section ofJunos OS Release 15.1 page. On the 15.1X49-D70 page, click **Standards Reference** or **APIs and Scripting** to view information about standards and APIs and scripting, respectively.

  The Junos OS 15.1 *Standard Reference* does not indicate SRX Series device support in the Supported Platforms list and other related support information. However, the Junos OS features described in this guide are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, refer to Feature Explorer.

- In Junos OS Release 15.1X49-D70, information about system log messages is available in System Log Explorer. On the 15.1X49-D70 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 on page 37
- Upgrade and Downgrade Scripts for Address Book Configuration on page 37

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 http://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 38).

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.

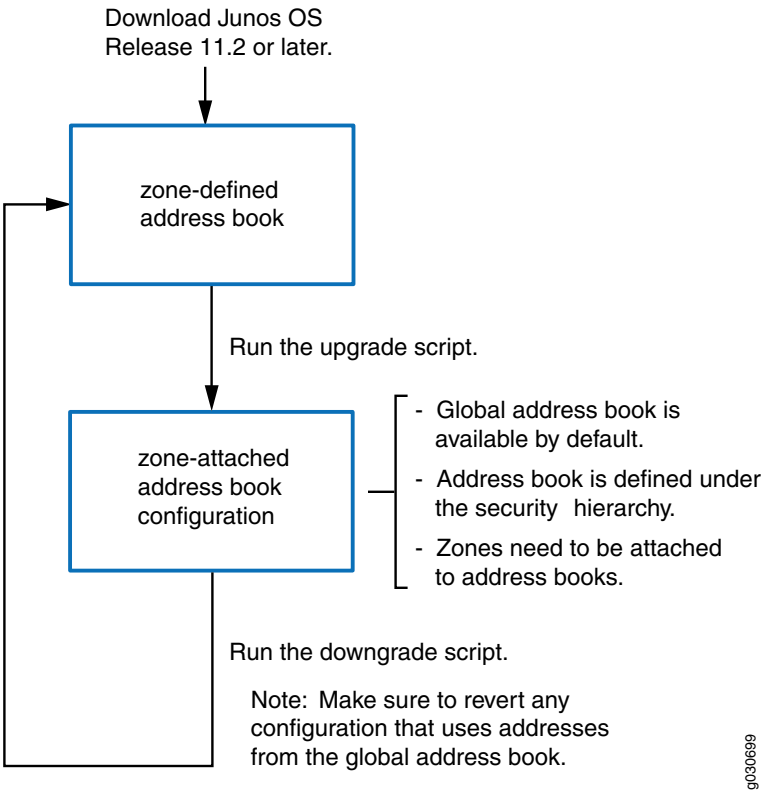
- You cannot configure address books using the J-Web interface.

  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 12.1X44, 12.1X46, and 12.3X48 are EEOL releases. You can upgrade from Junos OS Release 12.1X44 to Release 12.1X46 or even from Junos OS Release 12.1X44 to Release 12.3X48. 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 http://www.juniper.net/support/eol/junos.html.

For information about software installation and upgrade, 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 7
- Known Behavior on page 20
- Known Issues on page 26
- Resolved Issues on page 32

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 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, see http://www.juniper.net/support/requesting-support.html.

Revision History

25, April 2017—Revision 5— Junos OS 15.1X49-D75 – SRX Series.

23, February 2017—Revision 4— Junos OS 15.1X49-D75 – SRX Series.

16, February 2017—Revision 3— Junos OS 15.1X49-D75 – SRX Series.

27, January 2017—Revision 2— Junos OS 15.1X49-D75 – SRX Series.

23, January 2017—Revision 1— Junos OS 15.1X49-D75 – SRX Series.