Release Notes

Published
2026-08-11

Junos OS Evolved 25.4X300-D10

Juniper Networks | Engineering Simplicity

Table of Contents

Introduction

Junos OS Evolved runs on the following Juniper Networks® hardware: ACX Series, PTX Series, QFX Series and SRX Series. Use these release notes to find new and updated features, software limitations, and open issues for Junos OS Evolved Release 25.4X300-D10 for SRX Series.

You can find release notes for all Junos OS Evolved releases at Junos OS Evolved Documentation | Juniper Networks

Junos OS Evolved Release Notes for SRX Series

IN THIS SECTION

What's New

IN THIS SECTION

Learn about new features introduced in this release for SRX Series.

Hardware

New SRX400 line of Firewalls (SRX400, SRX440, and SRX440-2AC)—The SRX400 line of Firewalls integrates routing, and switching with next-generation firewall capabilities, advanced threat mitigation, and SD-WAN. Leverage this integration to secure and optimize connectivity across distributed enterprise locations while reducing cost and operational complexity.

Features Supported on SRX400 Line of Firewalls:

Feature	Description
Class of service (CoS)	• Support for CoS. [See Understanding Class of Service.] • The following features are not supported: • CoS classification on Label-Switched Interface for MPLS and VPLS • Queuing, Rewrite, Shaping and Scheduling on Secure Tunnel Interface (st0) for IPSec and FTI interface for GRE and IP-IN-IP tunnel. • CoS features on ae interfaces.

(Continued)

Feature	Description

Layer 7 advanced security features	• Support for application identification (AppID). [See Application Identification on SRX Series Firewalls.]
	• Support for advanced policy-based routing (APBR). [See Advanced Policy-Based Routing.]
	• Support for application quality of service (AppQoS). [See Application QoS.]
	• Support for application quality of experience (AppQoE). [See Application Quality of Experience.]
	• Support for Content Security.
	[See Content Security Overview.]
	  • The following functionality is not supported:
	  • Avira Antivirus
	• Support for security policies. [See Security Policies User Guide for Security Devices.]
	• Support for screen options for attack detection and prevention.
	[See Screens Options for Attack Detection and Prevention.]
	• Support for Juniper ATP Cloud. [See File Scanning Limits.]
	• Support for intrusion detection and prevention (IDP). [See Intrusion Detection and Prevention User Guide.]
	  • The following feature is not supported:
	  • Packet Capture

(Continued)

Feature	Description

Hardware	• SRX400 line of Firewalls secure small branch and retail offices, addressing current security needs while providing scalability for future growth.
	  • These firewalls support:
	  • Eight 10/100/1000BASE-T RJ-45 ports and two 1GbE SFP ports for flexible connectivity.
	  • Ports 8 and 9 supply PoE PSE up to 30 W per port.
	  • SRX400 and SRX440 Firewalls include one AC 180 W power supply adapter. SRX440-2AC Firewalls come equipped with two AC 180 W power supply adapters. [See SRX440 Documentation and SRX400 Documentation.]

SSL proxy	• Support for SSL proxy. [See SSL Proxy.]

Services Applications	• Support for Network Address Translation (NAT). [See NAT Configuration Overview.]
	  • The following feature is not supported:
	  • NAT Proxy ARP
	• Support for Application Layer Gateway (ALG). [See ALG Overview.]
	• Support for on-box logging and reporting. [See Overview.]
	• Support for Public Key Infrastructure (PKI). [See Public Key Infrastructure User Guide.]
	• Support for flow monitoring. [See Flow-Based and Packet-Based Processing User Guide for Security Devices.]
	  • The following features are not supported:
	  • `services-offload` option in configuration for traffic processing.
	  • TWAMP light configuration on the test packets.

Remote access	• Support for remote access VPN using Juniper Secure Connect. [See Juniper Secure Connect User Guide.]

(Continued)

Feature	Description
MACsec	• Support for Media Access Control Security (MACsec) in static connectivity association key (CAK) mode. [See Configuring MACsec.]

Install and Upgrade	• Support for Zero Touch Provisioning (ZTP). [See Zero Touch Provisioning.]
	  • The following features are not supported on ZTP:
	  • Phone-Home Client
	  • J-Web-based provisioning
	• Support for secure zero-touch provisioning (SZTP). [See Secure Zero Touch Provisioning.]
	• Support for Switching between ZTP and SZTP. [See Switching between Secure Zero Touch Provisioning and Zero Touch Provisioning.]

High availability (HA) and resiliency	• Support for Multinode High Availability (MNHA) in active/backup mode in routing, hybrid, and default gateway deployments. [See Multinode High Availability.]
	  • The following features are not supported:
	  • Multiple Service Redundancy Group (SRGs)
	  • Dynamic Host Configuration Protocol (DHCP)

Chassis

Enhanced chassis management (SRX400, SRX440, and SRX440-2AC)—Support for chassis management features such as hardware operations, optics detection, system, port and LED management, thermal and voltage sensors, and EM policy for fan speed and power supply modules (PSM). [See Chassis-Level Features Overview | Junos OS | Juniper Networks.]

Platform resiliency support (SRX400, SRX440, and SRX440-2AC)—We support hardware resiliency to maintain service continuity. The system monitors and responds to failures across the control and forwarding planes. It detects faults, raises alarms, logs details, sends SNMP traps and LED indicators, and initiates a reboot or triggers high availability failover. You can verify chassis health with CLI commands such as `show chassis environment`, `show chassis alarms`, and `show interfaces diagnostics optics`. [See Platform Resiliency.]

Identity Aware Firewall

Support for user identity, SRX firewall user authentication, and SAML-based firewall authentication (SRX400, SRX440, and SRX440-2AC)—Enforce identity-based access control by authenticating users and binding sessions to user identity. Integrate external authentication servers to improve security and ensure compliance.

The following feature is not supported:

- Secure LDAP

[See Identity-Aware Firewall, Active Directory as Identity Source, External Authentication Servers, External User Authentication (CLI Procedure), and SAML Authentication in Juniper Secure Connect.]

Interfaces

Interfaces Support (SRX400, SRX440, and SRX440-2AC)—You can configure two SFP ports and eight RJ-45 ports on SRX400 and SRX440 firewalls. SFP ports support 1 Gbps and RJ-45 ports support 1 Gbps, 100 Mbps, and 10 Mbps. See Port Speed on SRX Series Firewalls.

J-Web

Support for web-based management interface (SRX400, SRX440, and SRX440-2AC)—You can monitor, configure, troubleshoot, and manage your Firewalls using J-Web.

Junos Telemetry

Junos telemetry support (SRX400, SRX440, and SRX440-2AC)—Stream operational statistics to external data collectors for enhanced real-time visibility, troubleshooting, and capacity planning. Subscribe to the following root resource paths for information on events, task memory, interfaces, and component health:

- `/junos/events/`
- `/junos/task-memory-information/`
- `/interfaces/`
- `/components/`

Configure telemetry subscriptions to stream data to your collector, see Telemetry Data Subscriptions over gNMI, and Establish a Dial-in Telemetry Connection. View supported sensors in the Junos YANG Data Model Explorer.

[See Establish a Dial-in Telemetry Connection and Junos YANG Data Model Explorer.]

Software Installation and Upgrade

Support for Hardware Root of Trust (HRoT) and secure U-Boot (SRX400, SRX440, and SRX440-2AC)—Use the firewall's secure boot feature to ensure system integrity and prevent unauthorized code execution by unauthorized entities. HRoT validates the U-Boot bootloader before execution. U-Boot then validates the kernel and initial RAM file system (initramfs) before continuing the boot process.

[See Boot Junos OS Evolved by Using a Bootable USB Drive, Upgrade Junos OS Evolved Using a PXE Boot Server, and Upgrade Firmware on Junos OS Evolved Devices.]

Unsupported Features

Chassis cluster (SRX400, SRX440, and SRX440-2AC)—Chassis cluster (legacy high-availability) is not supported on this platform. Instead it supports Multinode High Availability (MNHA), which is the supported redundancy mechanism.

jnxLEDLastChange SNMP OID not supported (SRX400, SRX440, and SRX440-2AC)—The architectural shift to distributed sysfs-based LED management prevents support for the jnxLEDLastChange SNMP OID.

SNMP OIDs do not display USB and RE details (SRX400, SRX440, and SRX440-2AC)—The 'jnxFilledDescr' and 'jnxContentsType' SNMP OIDs do not show details for USB hub slots or Routing Engine (RE) components.

Logging access behavior change (SRX400, SRX440, and SRX440-2AC)—System and application logs previously accessed using the `show log` command are now available through `show trace application` and selective show log outputs. For example, use `show trace application cosd` and `show trace application jdhcpd` for cosd and jdhcpd logs, and `show trace application configd` for configd logs. Use `show log messages` or /var/log/messages for configuration activity and other logs.

The `show log` command now provides only generic system logs, excluding logs for applications such as authd. This change improves logging structure and scalability.

Support the Debug Collector instead of Request System Information (RSI) (SRX400, SRX440, and SRX440-2AC)—All commands previously supported through RSI will be migrated to the Debug Collector. The Debug Collector can be invoked from the CLI using the command 'request system debug-info', which generates a file containing all the relevant debug outputs.

[See request system debug-info.]

Firewall filter match conditions (SRX400, SRX440, and SRX440-2AC)—On SRX400, when configuring a firewall filter with the port match condition, also configure the protocol match condition.

[See Firewall Filter Match Conditions for IPv4 Traffic.]

System management (SRX400, SRX440, and SRX440-2AC)—On Junos OS Evolved SRX Firewalls, you can encrypt the configuration files data using an encryption key. This encryption key is generated using the 'set system master-password' command.

[See master-password.]

Logging access behavior change (SRX400, SRX440, and SRX440-2AC)—System and application logs previously accessed using the `show log` command are now available through `show trace application` and selective show log outputs. For example, use `show trace application cosd` and `show trace application jdhcpd` for cosd and jdhcpd logs, and `show trace application configd` for configd logs. Use `show log messages` or /var/log/messages for configuration activity and other logs.

The `show log` command now provides only generic system logs, excluding logs for applications such as authd. This change improves logging structure and scalability.

System information (SRX400, SRX440, and SRX440-2AC)—The `restart forwarding` cli command is changed to `restart srxpfe` command.

GRE and IPIP Tunnel (SRX400, SRX440, and SRX440-2AC)—Starting from this release, GRE and IPIP tunnels operate only when IPv4 or IPv6 forwarding is configured in flow-based mode. When packet-based mode is configured for IPv4 traffic (`set security forwarding-options family inet mode packet-based`) or for IPv6 traffic (`set security forwarding-options family inet6 mode packet-based`) GRE and IPIP tunnels do not pass traffic, even though the underlay IP connectivity is up.

Features not supported on SRX400 line of firewalls (SRX400, SRX440, and SRX440-2AC)—

- Configure Power on Ethernet (PoE) Interfaces
- Multicast
- DHCPv6
- VRRP
- VPLS
- IPv6
- EVPN/VxLAN

VPNs

IPsec VPN using st0 interface (SRX400, SRX440, and SRX440-2AC)—Configure IPsec VPN service using the default iked process, which replaces earlier kmd-based implementations. Use the `st0` logical secure tunnel interface to carry IPsec traffic. The IPsec VPN service supports the features available on other next-generation firewall platforms that use the iked process.

[See IPsec VPN User Guide.]

What's Changed

IN THIS SECTION

Learn about what's changed in this release for SRX Series.

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

Platform and Infrastructure

- On Junos OS Evolved SRX Firewalls, use the show system software command to see output for external packages and lists.

  [See show system software and How Junos OS Evolved Differs from Junos OS.]

VPNs

- SRX400 and SRX440 support only route-based VPN using iked. Policy-based VPN is not supported; therefore, any policy-based VPN configuration commands are deprecated and not supported.

- **Removal of weak algorithms in IPsec VPN with iked process**—The following algorithms are no longer available as CLI options:

  - `des-cbc` and `3des-cbc` as encryption algorithms in IKE proposal and IPsec proposal at the `[edit security ike proposal encryption-algorithm]` and `[edit security ipsec proposal encryption-algorithm]` hierarchy levels respectively.

  - `md5` and `sha1` as authentication algorithms in IKE proposal at the `[edit security ike proposal authentication-algorithm]` hierarchy level.

- group1, group2, and group5 as DH groups in IKE proposal and Perfect Forward Secrecy (PFS) groups at the [edit security ike proposal dh-group] and [edit security ipsec policy perfect-forward-secrecy keys] hierarchy levels respectively.
- hmac-md5-96, hmac-sha1-96, and hmac-sha-256-96 as authentication algorithms in IPsec proposal at the [edit security ipsec proposal authentication-algorithm] hierarchy level.
- basic, compatible, and standard as IKE proposal sets and IPsec proposal sets at the [edit security ike policy proposal-set] and [edit security ipsec policy proposal-set] hierarchy levels respectively.

For MNHA HA link encryption and standalone VPNs, using hmac-sha1-96 as the IPsec authentication algorithm at the [edit security ipsec proposal proposal-name authentication-algorithm] hierarchy level results in a commit error. Configure stronger algorithms to enhance IPsec VPN security.

[See proposal (Security IKE), proposal (Security IPsec), policy (Security IKE), and policy (Security IPsec).]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for SRX Series.

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

J-Web

- J-Web becomes unreachable when a local self-signed certificate with weak digital signature is assigned to the HTTPS PKI configuration.

  PR1955001

Platform and Infrastructure

- Automatic removal of debug logs during storage maintenance (SRX400 and SRX440 Firewalls). -As part of the EVO framework design, storage cleanup removes debug logs instead of retaining them,

unlike SRX300 Series firewalls, where they are retained. Export or archive required debug logs before starting storage maintenance to preserve diagnostic data.

PR1919223

Open Issues

IN THIS SECTION

Learn about open issues in this release for SRX Series.

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

General Routing

- On SRX4xx series devices, when a policer is configured using a bandwidth percentage (bw percent) and applied through an interface-specific firewall filter, the policer is not programmed with the correct bandwidth value in the datapath on the first commit. As a result, traffic is not policed to the configured rate and may be forwarded without rate limiting. User-created (non-interface-specific) filters program the value correctly. PR1962577
- On SRX4xx series devices, flexible VLAN tagging with outer and inner VLANs (QinQ) is not supported in L3 mode PR1952806
- On SRX4xx series devices, after clearing a DHCP client binding via CLI command, the DHCP client state may intermittently remain stuck in LOCAL_CLIENT_STATE_WAIT_INTERFACE_DELETE. This is an intermittent issue, has no impact on DHCP client functionality PR1958746

- On SRX4xx series devices, DHCP server on the SRX4xx series management interface (re0:mgmt-0.0) does not work in factory default state.DHCP server on revenue interface work as expected. PR1960037

Infrastructure

- On SRX4xx series devices, when a manual IPsec security association is configured in transport mode using the AH protocol with hmac-sha-256-128 authentication and if any BGP session is bound to that SA (ipsec-sa under the BGP group), the BGP session fails to establish --- the peer remains in Connect/TryConnect state PR1961209

J-Web

- When J-Web retrieves message logs in JSON format, certain syslog entries containing special or control characters might cause the response to be parsed incorrectly. As a result, the Messages log view in J-Web Monitor might not display log entries for any selected time duration, although the logs are available from the CLI.

  PR1962290

- After recent Firefox browser updates, J-Web UI may not be accessible when the device is accessed using its hostname (FQDN) if the device is configured with a self-signed HTTPS certificate. Firefox enforces HTTP Strict Transport Security (HSTS) for such connections and does not allow users to bypass certificate validation, resulting in the browser blocking access. Accessing J-Web using the device's IP address continues to work because Firefox allows users to accept the risk and proceed for non-HSTS connections.

  PR1957069

Platform and Infrastructure

- Legacy download manager support is deprecated as we move to Junos OS Evolved because Junos OS Evolved already provides the native utilities like FTP/SFTP/SCP/WGET/FETCH, which provides similar functionalities as part of the OS. We do not need the explicit daemon to take care of these.

  PR1922526

- Used routing instance with linked physical interface and with static route option. set groups top services monitoring rpm owner Custom_RPM_apps test Cust-CNN routing-instance Custom_RPM set groups top routing-instances Custom_RPM instance-type virtual-router set groups top routing-instances Custom_RPM routing-options static route 0.0.0.0/0 next-hop 5.5.0.254 set groups top routing-instances Custom_RPM interface ge-0/0/3.0 set groups top services monitoring rpm owner Custom_ICMP_RPM_apps test Cust-ICMP routing-instance wan0 set groups top routing-instances wan0 instance-type virtual-router set groups top routing-instances wan0 routing-options static route 0.0.0.0/0 next-hop 5.4.0.254 set groups top routing-instances wan0 interface ge-0/0/2.0

PR1958674

- The SRX4xx series platforms already ships with a 200 MB or more configuration database by default, so the extending the configuration database size is not supported. As a result, the system configuration-database extend-size configuration hierarchy is disabled.

  PR1941275

- On SRX4xx series devices running in packet (bypass) mode, telnet traffic to a device interface or telnet initiated from the device to an external interface fails when the source and destination IP addresses reside in different routing instances. The issue has no service impact beyond the affected telnet session. PR1940848

Services Applications

- On SRX4xx series devices, restarting the ike-key-management (iked) and ike-config-management (ikemd) daemons at the same time may cause IKE and IPsec security associations to be deleted, bringing down established VPN tunnels. PR1958903

- On SRX4xx series devices, the Application Identification (appid) process may generate a core file during a software image upgrade. This occurs only while the process is shutting down as part of the upgrade reboot and has no impact on application-identification functionality, on traffic, or on the upgrade itself --- the upgrade completes normally. PR1961889

- After recent Firefox browser updates, J-Web UI may not be accessible when the device is accessed using its hostname (FQDN) if the device is configured with a self-signed HTTPS certificate. Firefox enforces HTTP Strict Transport Security (HSTS) for such connections and does not allow users to bypass certificate validation, resulting in the browser blocking access. Accessing J-Web using the device's IP address continues to work because Firefox allows users to accept the risk and proceed for non-HSTS connections. PR195

VPNs

- Data traffic through IPsec tunnel will dropped if the IPsec tunnel uses a AES-CBC family cipher and has extended sequence number enabled. PR1940605

Resolved Issues

IN THIS SECTION

Learn about resolved issues in this release for SRX Series.

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

Infrastructure

- On all Junos OS Evolved platforms, due to linux kernel issue, periodical sync from system time to RTC (Real-Time Communication) every 11min stops working when system time moves to backwards. PR1939674

J-Web

- On SRX4xx series devices, when syslog events are requested in JSON format using the get-syslog-events RPC with the <print-json/> and <pretty/> options, the RPC output may be malformed if a syslog message contains special characters such as double quotation marks (') or backslashes (\). As a result, applications that parse the RPC output ? including the J-Web Monitor > System Log page ? may fail to display log entries. As a result, applications that parse the RPC output, including log monitoring pages, might fail to display the log entries. As a workaround, request the syslog events without JSON formatting or view the logs from the CLI.

  PR1959603

Platform and Infrastructure

- On Junos Evolved based SRX4xx platforms, the output of `show chassis hardware extensive` is showing model number of all Field Replaceable Unit (FRU) as SRX4XX. This is a cosmetic issue with no service impact.

  PR1949768

- On Security Director Cloud, downloading an IDP signature package (sigpack) in offline mode fails due to plaform mismatch

  PR1962685

User Interface and Configuration

- On SRX Series platforms, which do not verify the syntax and integrity of the saved rescue configuration file when performing a configuration check, rescue configuration check fails.

  PR1907238

Migration, Upgrade, and Downgrade Instructions

For products impacted, see Feature Explorer.

Follow these steps to upgrade your Junos OS Evolved software:

1. Using a Web browser, navigate to the All Junos Platforms software download URL on the Juniper Networks webpage: Downloads.
2. In the Find a Product box, enter the Junos OS platform for the software that you want to download.
3. Select Junos OS Evolved from the OS drop-down list.
4. Select the relevant release number from the Version drop-down list.
5. In the **Install Package** section, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by a Juniper Networks representative.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

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

For more information about software installation and upgrade, see Software Installation and Upgrade Overview (Junos OS Evolved). For more information about EOL releases and to review a list of EOL releases, see Junos OS Evolved Dates & Milestones - Juniper Networks.

Documentation Updates

There are no documentation updates for this release.

Licensing

In 2020, Juniper Networks introduced a new software licensing model. The Juniper Flex Program comprises a framework, a set of policies, and various tools that help unify and thereby simplify the multiple product-driven licensing and packaging approaches that Juniper Networks has developed over the past several years.

The major components of the framework are:

- A focus on customer segments (enterprise, service provider, and cloud) and use cases for Juniper Networks hardware and software products.
- The introduction of a common three-tiered model (standard, advanced, and premium) for all Juniper Networks software products.
- The introduction of subscription licenses and subscription portability for all Juniper Networks products, including Junos OS and Contrail.

For information about the list of supported products, see Juniper Flex Program.

Finding More Information

- **Feature Explorer**—Juniper Networks Feature Explorer helps you to explore software feature information to find the right software release and product for your network.

  Feature Explorer

- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved.

  index?page=prsearch.

- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms.

  https://apps.juniper.net/hct/home

  NOTE: To obtain information about the components that are supported on the devices and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

  Compliance Advisor.

Requesting Technical Support

IN THIS SECTION

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit Product Warranty Policy - Support - Juniper Networks.
- 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: Support
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: Documentation
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: Support
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: Elevate - Elevate Community

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

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: Support
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: Documentation
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: Support
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: Elevate - Elevate Community

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

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit Juniper Support Portal: Case Management, Product Support & More

- 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 Contact - Support - Juniper Networks.

You can create a service request with JTAC on the Web or by telephone.

- Visit Juniper Support Portal: Case Management, Product Support & More
- 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 Contact - Support - Juniper Networks.

Revision History

07-Jul-26 - Revision 2, Junos OS Evolved Release 25.4X300-D10.

30-Jun-26 - Revision 1, Junos OS Evolved Release 25.4X300-D10.