Release Notes

Published
2026-01-19

Connected Security Distributed Services Architecture Release Notes

Table of Contents

Introduction | 1

December 17, 2025 Release

What's New | 2

What's Changed | 3

Known Limitations | 4

Open Issues | 4

Resolved Issues | 4

July 17, 2025 Release

What's New | 5

What's Changed | 6

Known Limitations | 6

Open Issues | 6

Resolved Issues | 6

June 23, 2025 Release

What's New | 7

What's Changed | 8

Known Limitations | 8

Open Issues | 8

Resolved Issues | 8

December 20, 2024 Release

What's New | 10

Feature Support in Junos OS Release 24.4R1 | 10

Junos Node Unifier | 11

Junos Device Manager | 13

What's Changed | 15

Known Limitations | 15

Open Issues | 15

Resolved Issues | 16

March 31, 2024 Release

What's New | 17

What's Changed | 18

Known Limitations | 18

Open Issues | 18

Resolved Issues | 19

Requesting Technical Support

Self-Help Online Tools and Resources | 20

Creating a Service Request with JTAC | 20

Revision History | 20

Introduction

The Connected Security Distributed Services (CSDS) Architecture delivers a scalable, distributed security architecture design that fully decouples the forwarding and security services layers. The architecture enables the existing MX Series routers serve as intelligent forwarding engine supporting load balancing with path redundancy along with the SRX Series Firewalls expanding your data centers securely.

The CSDS Architecture consists of:

- MX Series in the forwarding layer.
- SRX Series Firewalls in the services layer.
- QFX Series or any other switches in the optional distribution layer.

You can use Junos Node Unifier (JNU) for centralized management of devices in the forwarding and services layers within the CSDS solution.

You can use Junos Device Manager (JDM) to orchestrate the deployment of vSRX Virtual Firewalls.

To provide deployment flexibility, the CSDS solution supports various components and platforms at the forwarding layer, services layer, and management layer.

December 17, 2025 Release

IN THIS SECTION

- What's New | 2
- What's Changed | 3
- Known Limitations | 4
- Open Issues | 4
- Resolved Issues | 4

Read the following sections to learn about the new features in Connected Security Distributed Services (CSDS) Architecture released on December 17, 2025.

- "What's New" on page 2

- "What's Changed" on page 3
- "Resolved Issues" on page 4

What's New

IN THIS SECTION

- Junos OS Platforms Support | 2
- Express Path for CSDS Architecture | 2
- Support for Juniper Security Director Cloud | 3

Learn about new features introduced in the Connected Security Distributed Services (CSDS) Architecture in this release.

Junos OS Platforms Support

Table 1: Junos OS Platforms and Releases

Junos OS Platform	Junos OS Devices	Junos OS Release
SRX Series Firewalls	SRX4300	24.4R2

To learn about the supported platforms in CSDS Architecture, see Supported Platforms.

Express Path for CSDS Architecture

- **Express Path support for CSDS Architecture (MX304 and vSRX 3.0)**—Starting in Junos OS Release 25.4R1, you can use Express Path in the router to directly process non-first packets of a session and bypass the firewall in the datapath. The firewall inspects the first packet of a session. After it accepts the flow and marks the session for offloading, the router handles and forwards subsequent traffic

without further inspection by the firewall. The CSDS Architecture uses Express Path to offload flow processing and optimize network performance.

Use the following configuration statements:

- `set chassis fpc slot service-offload` to enable the feature.
- `set chassis fpc slot service-offload flow-table-size unit` to optionally adjust the flow table size.

[See Express Path in CSDS Architecture, service-offload (CSDS), virtual-offload (CSDS), show security flow service-offload virtual-offload statistics, and clear security flow service-offload virtual-offload statistics.]

Support for Juniper Security Director Cloud

- **Monitor firewalls in CSDS Architecture using CSDS groups (SRX4300, SRX4600, SRX4700, SRX5400, SRX5600, SRX5800, and vSRX 3.0)**—You can use Connected Security Distributed Services (CSDS) groups to monitor SRX Series Firewalls within the CSDS Architecture. CSDS groups provide network topology visualization and performance metrics tracking. You can improve network visibility and retain data for trend analysis, ensuring optimal system performance. The feature also supports monitoring firewalls deployed in a Multinode High Availability (MNHA) configuration.

  To use the feature, deploy CSDS Architecture outside of Juniper Security Director Cloud. For more information, see Connected Security Distributed Services Architecture Deployment Guide.

  [See CSDS Groups Overview, Create and Manage CSDS Groups, View CSDS Groups Topology, Set Threshold for CSDS Groups, and Monitor SRX Series Firewalls in CSDS Groups for Juniper Security Director Cloud.]

What's Changed

Learn about changes to Connected Security Distributed Services (CSDS) Architecture in this release.

- **No support for enhanced-mode with Express Path (MX304 and vSRX 3.0)**—In the CSDS Architecture, vSRX Virtual Firewall cannot offload sessions to the MX Series router when you configure egress and ingress filters on the firewall. The firewall doesn't support the `enhanced-mode` option at the `[edit firewall inet filter filter-name]` hierarchy. The behavior of the Express Path in vSRX Virtual Firewall is similar to the functionality in SRX Series Firewalls without the `enhanced-mode` option.

- **Run CSDS CLI commands as root user (MX240, MX304, MX480, MX960, MX10004, and MX10008)**—Run CSDS CLI operations as the root user to ensure successful execution of maintenance commands for key exchange, authentication, and JDM interactions.

  Run the following commands as root user:

  - `request csds authenticate-host csds-instance-id` *`csds-instance-id`*
  - `request csds jdm add csds-instance-id` *`csds-instance-id`* `image` *`vsrx-image-with-path`*
  - `request csds add-vsrx csds-instance-id` *`csds-instance-id`* `image` *`image-name`*
  - `request csds extract-vsrx-keys csds-instance-id` *`csds-instance-id`*
  - `request csds sync-controller other-controller-ip` *`other-controller-ip`*
  - `request csds delete-vsrx csds-instance-id` *`csds-instance-id`*

  If a non-root user runs these commands, you'll see the following warning message:

  ```
  warning: Must be logged in as root to execute command.
  ```

  [See request csds add-vsrx, request csds authenticate-host, request csds delete-vsrx, request csds extract-vsrx-keys, request csds jdm, and request csds sync-controller.]

Known Limitations

There are no known limitations for Connected Security Distributed Services (CSDS) Architecture in this release.

Open Issues

There are no new open issues for Connected Security Distributed Services (CSDS) Architecture in this release.

Resolved Issues

Learn about the issues fixed in this release for Connected Security Distributed Services (CSDS) Architecture.

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

- In JDM, intermittently, the command `request csds extract-vsrx-keys csds-instance-id 0` fails with the error message `Extracting VSRX keys failed on vnf0`. PR1846684.

July 17, 2025 Release

IN THIS SECTION

- What's New | 5
- What's Changed | 6
- Known Limitations | 6
- Open Issues | 6
- Resolved Issues | 6

Read the following sections to learn about the new features in Connected Security Distributed Services (CSDS) Architecture released on July 17, 2025.

- "What's New" on page 5

What's New

IN THIS SECTION

- Junos OS Platforms Support | 6

Learn about new features introduced in the Connected Security Distributed Services (CSDS) Architecture in this release.

Junos OS Platforms Support

Table 2: Junos OS Platforms and Releases

Junos OS Platform	Junos OS Devices	Junos OS Release
SRX Series Firewalls	SRX4700	24.4R1-S3

To learn about the supported platforms in CSDS Architecture, see Supported Platforms.

What's Changed

There are no changes for Connected Security Distributed Services (CSDS) Architecture in this release.

Known Limitations

There are no known limitations for Connected Security Distributed Services (CSDS) Architecture in this release.

Open Issues

There are no new open issues for Connected Security Distributed Services (CSDS) Architecture in this release.

Resolved Issues

There are no resolved issues for Connected Security Distributed Services (CSDS) Architecture in this release.

June 23, 2025 Release

IN THIS SECTION

- What's New | 7
- What's Changed | 8
- Known Limitations | 8
- Open Issues | 8
- Resolved Issues | 8

Read the following sections to learn about new features and resolved issues in Connected Security Distributed Services (CSDS) Architecture released on June 23, 2025.

- "What's New" on page 7
- "Resolved Issues" on page 8

What's New

IN THIS SECTION

- Junos OS Platforms Support | 8

Learn about new features introduced in the Connected Security Distributed Services (CSDS) Architecture in this release.

Use Feature Explorer to confirm platform and release support for Connected Security Distributed Services (CSDS) Architecture.

Junos OS Platforms Support

- Support for Junos OS Release 25.2R1 and later.

What's Changed

There are no changes for Connected Security Distributed Services (CSDS) Architecture in this release.

Known Limitations

There are no known limitations for Connected Security Distributed Services (CSDS) Architecture in this release.

Open Issues

There are no new open issues for Connected Security Distributed Services (CSDS) Architecture in this release.

Resolved Issues

Learn about the issues fixed in this release for Connected Security Distributed Services (CSDS) Architecture.

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

- In Multinode High Availability solution, IPsec VPN tunnel distribution table on the Routing Engine (RE) is not cleaned up, leading to the crashing of SRX Series Firewall Packet Forwarding Engine and generation of core-dump file although DPD is configured. PR1850526.
- In Multinode High Availability solution with SRG1 IPsec VPN configuration, the layer 3 Interchassis link (ICL) IPsec encryption link goes down permanently after rebooting the connected router through which the ICL was established. During this state, the IKE process got stuck at ~70% on the Multinode High Available active node. PR1850967.

- The uid of jnuadmin changes when you delete and then add back the JNU configuration. PR1854326.
- Intermittently, when the schema.tar.gz failed to secure copy (scp) from the satellite to the controller, the jnud process continues synchronizing with the MX Series controller. PR1854356.
- In Multinode High Availability solution, the ICL link encryption must be used for connection between the pub-broker and sub-broker with loopback interface IP addresses to avoid IPsec session synchronization failure between the master and backup Multinode High Availability nodes. PR1840788.
- In Multinode High Availability solution with SRG1 IPsec VPN configuration, the command `show chassis high-availability information` shows SRG1 control plane state as `Ready` although the ICL connection between the Pub-Broker and Sub-broker is not established properly and the IPsec sessions are getting synchronized between the master and standby peers. PR1840803.

December 20, 2024 Release

IN THIS SECTION

- What's New | **10**
- What's Changed | **15**
- Known Limitations | **15**
- Open Issues | **15**
- Resolved Issues | **16**

Read further to learn about the new features, changed features, known limitations, open issues, and resolved issues in Connected Security Distributed Services (CSDS) Architecture released on December 20, 2024.

What's New

IN THIS SECTION

- Feature Support in Junos OS Release 24.4R1 | 10
- Junos Node Unifier | 11
- Junos Device Manager | 13

Feature Support in Junos OS Release 24.4R1

IN THIS SECTION

- Junos OS Platforms Support | 10
- Redundancy Support | 11
- CSDS Traffic Orchestrator with Routing Engine-Based Health Checks (MX304, MX10004, and MX10008) | 11

Learn about new features introduced in the Connected Security Distributed Services (CSDS) Architecture in this release.

Junos OS Platforms Support

The CSDS Architecture supports the following Junos OS platforms and releases with centralized management of devices in the topology:

Table 3: Junos OS Platforms and Releases

Junos OS Platform	Junos OS Devices	Junos OS Release
MX Series	MX240, MX304, MX480, MX960, MX10004, MX10008	24.4R1 or later
SRX Series Firewalls	SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0	24.4R1 or later

Redundancy Support

The CSDS Architecture additionally supports the following redundancy for load balancing:

Table 4: Redundancy Support

CSDS Components	Supported Redundancy
Forwarding layer with MX Series	• CSDS Traffic Orchestrator (CSDS-TO) with Routing Engine (RE)-based health-checks support for load balancing

CSDS Traffic Orchestrator with Routing Engine-Based Health Checks (MX304, MX10004, and MX10008)

The CSDS Traffic Orchestrator (CSDS-TO) for next-generation MX Series routers can now run the health check process on the Routing Engine too. This enhancement ensures that the traffic distribution and redirection management process connects to the local network monitoring process rather than the remote instance on the services PIC. The Routing Engine-based health checks support probe types such as ICMP, TCP, UDP, HTTP, and SSL.

Use the `set services traffic-load-balance routing-engine-mode` CLI command to enable this feature.

Modify the traffic load balancer configuration to use the loopback (lo0) interface instead of the service interface.

[See routing-engine-mode (CSDS), CSDS Traffic Orchestrator.]

Junos Node Unifier

IN THIS SECTION

- JNU Platform Support | 12
- Supported Features | 12
- Redundancy Support | 12

The Connected Security Distributed Services (CSDS) architecture supports centralized management of devices in CSDS topology using Junos Node Unifier (JNU) single touchpoint solution. You can run the Junos OS commands that are related to JNU satellites centrally from JNU controller.

JNU Platform Support

Table 5: Platform Support for JNU Topology

JNU Node	Supported Platform	Junos OS Device	Junos OS Release
JNU controller	MX Series	MX240, MX304, MX480, MX960, MX10004, and MX10008	24.4R1 or later
JNU satellite	SRX Series Firewall	SRX4600, SRX5400, SRX5600, SRX5800, and vSRX 3.0	24.4R1 or later
JNU satellite	Junos Device Manager	NA	24.4R1 or later

Supported Features

From the controller, you can perform the following operations on the satellites:

- Configure and manage the nodes using the Junos OS configuration commands.
- Run the Junos OS operational mode commands.

Redundancy Support

JNU supports the following redundancy for high availability.

Table 6: JNU Redundancy Support

JNU Component	Supported Redundancy
JNU controller	• Support for GRES with dual Routing Engine, *re0*, and *re1* on MX Series. • Two MX Series used as active-active controllers.
JNU satellite	• Not applicable.

RELATED DOCUMENTATION

Junos Node Unifier for CSDS

Junos Device Manager

IN THIS SECTION

- JDM Infrastructure Considerations | 13
- Supported Features | 14

The Connected Security Distributed Services (CSDS) architecture supports vSRX Virtual Firewalls for its services plane. Use Junos Device Manager (JDM) to orchestrate vSRX Virtual Firewalls in the CSDS services plane. JDM is a Linux container that offers a Junos OS-like CLI environment for the virtual machine (VM) life-cycle management. You can use JDM to deploy and manage vSRX Virtual Firewalls on Intel or AMD baremetal servers with Ubuntu OS..

You must use the MX Series Junos Node Unifier (JNU) controller to centrally manage JDM and vSRX Virtual Firewalls that server as the JNU satellites.

JDM Infrastructure Considerations

Table 7 on page 13 shows the list of supported baremetal servers for JDM. Table 8 on page 14 lists the vSRX Virtual Firewall platform support with JDM.

Table 7: Host Requirements for JDM

Server Profile	Host OS	Number of vSRX Virtual Firewalls Supported	Number of Cores Per vSRX Virtual Firewall
Intel Xeon Gold 6438N 2GHz with 32 cores	Ubuntu 22.04.4 LTS	1	31
Intel Platinum 8571N 2.4GHz with 52 cores	Ubuntu 22.04.4 LTS	1	51

Table 7: Host Requirements for JDM *(Continued)*

Server Profile	Host OS	Number of vSRX Virtual Firewalls Supported	Number of Cores Per vSRX Virtual Firewall
AMD EPYC 8534P 2.3GHz with 64 cores	Ubuntu 22.04.4 LTS	7	9
AMD EPYC 9554P 3.10GHz with 64 cores	Ubuntu 22.04.4 LTS	7	9
AMD EPYC 97542 2.5GHz with 128 cores	Ubuntu 22.04.4 LTS	7	18

Table 8: vSRX Virtual Firewall Platform Support with JDM

Junos OS Device	Junos OS Release
vSRX 3.0	24.4R1 or later

Use Feature Explorer to confirm platform and release support for specific features.

Supported Features

- Orchestrate vSRX Virtual Firewalls using JDM.
- Install, configure, and manage JDM and vSRX Virtual Firewalls that server as JNU satellites in JNU topology.
- Upgrade and downgrade JDM.

Table 9 on page 14 shows the platform support for JNU with JDM.

Table 9: JNU Topology Considerations with JDM

Supported Platform	JNU Node	Junos OS Device	Junos OS Release
Junos Device Manager	JNU satellite	NA	24.4R1 or later

Table 9: JNU Topology Considerations with JDM *(Continued)*

Supported Platform	JNU Node	Junos OS Device	Junos OS Release
SRX Series Firewall	JNU satellite	vSRX 3.0	24.4R1 or later
MX Series	JNU controller	MX240, MX304, MX480, MX960, MX10004, and MX10008	24.4R1 or later

RELATED DOCUMENTATION

Junos Device Manager for CSDS

What's Changed

There are no changes for Connected Security Distributed Services (CSDS) Architecture in this release.

Known Limitations

There are no known limitations for Connected Security Distributed Services (CSDS) Architecture in this release.

Open Issues

Learn about the known issues for Connected Security Distributed Services (CSDS) Architecture in this release.

- In JDM, intermittently, the command `request csds extract-vsrx-keys csds-instance-id 0` fails with the error message `Extracting VSRX keys failed on vnf0`. PR1846684.
- In Multinode High Availability solution, IPsec VPN tunnel distribution table on the Routing Engine (RE) is not cleaned up, leading to the SRX Series Firewall Packet Forwarding Engine (PFE) coredump although DPD is configured. PR1850526

- In Multinode High Availability solution with SRG1 IPsec VPN configuration, the layer 3 Interchassis link (ICL) IPsec encryption link goes down permanently after rebooting the connected router through which the ICL was established. During this state, the IKE process got stuck at ~70% on the Multinode High Available active node. PR1850967.
- The uid of jnuadmin changes when you delete and then add back the JNU configuration. PR1854326.
- Intermittently, when the schema.tar.gz failed to secure copy (scp) from the satellite to the controller, the jnud process continues synchronizing with the MX Series controller. PR1854356.
- In Multinode High Availability solution, the ICL link encryption must be used for connection between the pub-broker and sub-broker with loopback interface IP addresses to avoid IPsec session synchronization failure between the master and backup Multinode High Availability nodes. PR1840788.
- In Multinode High Availability solution with SRG1 IPsec VPN configuration, the command `show chassis high-availability information` shows SRG1 control plane state as `Ready` although the ICL connection between the Pub-Broker and Sub-broker is not established properly and the IPsec sessions are getting synchronized between the master and standby peers. PR1840803.

Resolved Issues

There are no resolved issues for Connected Security Distributed Services (CSDS) Architecture in this release.

March 31, 2024 Release

IN THIS SECTION

- What's New | **17**
- What's Changed | **18**
- Known Limitations | **18**
- Open Issues | **18**
- Resolved Issues | **19**

Read further to learn about the new features, changed features, known limitations, open issues, and resolved issues in Connected Security Distributed Services (CSDS) Architecture released on March 31, 2024.

What's New

IN THIS SECTION

- Supported Junos OS Platforms | 17
- Supported Features | 17
- Redundancy Support | 18

Learn about new features introduced in the Connected Security Distributed Services (CSDS) Architecture in this release.

Supported Junos OS Platforms

The CSDS Architecture supports the following Junos OS platforms and releases:

Table 10: Junos OS Platforms and Releases

Junos OS Platform	Junos OS Devices	Junos OS Release
MX Series	MX304, MX960	23.4R1 or later
SRX Series Firewalls	SRX4600, vSRX 3.0	23.4R1 or later

Supported Features

The CSDS Architecture supports the following security services:

- Stateful firewall

- IPsec VPN
- Carrier-grade NAT (CGNAT)

Redundancy Support

The CSDS Architecture supports the following redundancy for load balancing and high availability:

Table 11: Redundancy Support

CSDS Components	Supported Redundancy
Forwarding layer with MX Series	• ECMP-based Consistent Hashing for load balancing • SRD for redundancy between two MX Series
Services layer with SRX Series Firewalls	Multinode HA (MNHA)

What's Changed

There are no changes for Connected Security Distributed Services (CSDS) Architecture in this release.

Known Limitations

There are no known limitations for Connected Security Distributed Services (CSDS) Architecture in this release.

Open Issues

The following known issues are seen for Connected Security Distributed Services (CSDS) Architecture in this release.

- When you deploy CSDS with Dual MX Series using IPv6 address, the SRX Series Firewall drops a few packets during every BGP neighbor discovery refresh.

We recommend using static route in your configuration when you deploy CSDS with dual MX Series with IPv6 address.

Resolved Issues

There are no resolved issues for Connected Security Distributed Services (CSDS) Architecture in this release.

Requesting Technical Support

IN THIS SECTION

- Self-Help Online Tools and Resources | **20**
- Creating a Service Request with JTAC | **20**

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 JTACUser Guide located at https://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: https://www.juniper.net/customers/support/.
- Search for known bugs: https://prsearch.juniper.net/.
- Find product documentation: https://www.juniper.net/documentation/.
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/.
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/.
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/.
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/.

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

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

Revision History

- 17 Dec 2025—Revision 1, CSDS Architecture Release Notes - December 17, 2025 Release.
- 17 Jul 2025—Revision 1, CSDS Architecture Release Notes - July 17, 2025 Release.
- 23 Jun 2025—Revision 1, CSDS Architecture Release Notes - June 23, 2025 Release.

- 20 Dec 2024—Revision 1, CSDS Architecture Release Notes - December 20, 2024 Release.
- 8 July 2024—Revision 2, CSDS Architecture Release Notes - March 31, 2024 Release.
- 31 March 2024—Revision 1, CSDS Architecture Release Notes - March 31, 2024 Release.