# Release Notes

Published
2022-09-14

## Contrail Service Orchestration 6.2.0 Release Notes

# Table of Contents

Introduction | 1

Software Support | 2

Accessing the CSO GUIs | 24

What's New

New and Changed Features in Contrail Service Orchestration Release 6.2.0 | 25

Known Behavior | 28

Known Issues | 33

Resolved Issues | 39

Documentation Feedback | 39

Requesting Technical Support | 40

# Introduction

Juniper Networks offers Contrail Service Orchestration (CSO) Release 6.2.0 as a cloud-based service. CSO Release 6.2.0 supports the following types of accounts:

- OpCo accounts (for multitenant, managed service providers)—OpCo (operating company) administrators can add tenants and enable services such as software-defined WAN (SD-WAN), and next-generation firewall for the OpCo network. They can also manage profiles and policies for traffic, SLA policies, breakout policies, and firewall management.
- Tenant accounts (for enterprise customers that want to use CSO for managing their sites)—Tenant administrators can add sites to and enable services such as SD-WAN, and next-generation firewall for their networks. They can also configure SLA policies, firewall policies, and breakout policies.

The following list provides an overview of the features in CSO Release 6.2.0.

- SD-WAN
  - Support for configuring routing policies in LAN segments
  - ADSL/VDSL Annex J support on SRX300 Series devices
  - MTU support on WAN and LAN interfaces
  - Support for editing tenant-owned public IP pool
  - Support for vSRX cluster in SD-WAN deployments
- Licensing
  - Support for golden license to onboard SRX Series devices
- Miscellaneous
  - CSO usability enhancements
  - Support for alternate partition snapshot
  - Support for tenant-specific SSO server
  - Support to edit bootstrap and image upgrade time for SRX Series and NFX150 devices

# Software Support

IN THIS SECTION


- Software Downloads | 2
- Software Installation Requirements for NFX Series Network Services Platform | 24


# Software Downloads

Table 1 on page 2 displays the supported versions and download links for software components associated with CSO Release 6.2.0.

**NOTE**:

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.
- All new site onboarding must be with Junos Release 20.4R3-S2.

**Table 1: Software Components Associated with CSO Release 6.2.0**

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| Juniper Identity Management Service (JIMS) | 1.1.5R1 | Pre-bundled with CSO. |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| NFX150 CPE device | Junos OS Release 20.4R3-S2 | • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145154.html<br>• Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145128.html |
| | Junos OS Release 20.4R3-S1 | • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140857.html<br>• Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140830.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| NFX250 CPE device | Junos OS Release 20.4R3-S2<br><br>Junos OS Release 18.4R3-S5.4 | Junos OS Release 20.4R3-S2:<br><br>• vSRX Upgrade TGZ: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145244.html<br><br>• vSRX KVM Appliance: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145251.html<br><br>Junos OS Release 18.4R3-S5.4:<br><br>• Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114821.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1<br><br>Junos OS Release 18.4R3-S5.4 | Junos OS Release 20.4R3-S1:<br><br>• vSRX Upgrade TGZ: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140968.html<br><br>• vSRX KVM Appliance: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140975.html<br><br>Junos OS Release 18.4R3-S5.4:<br><br>• Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114821.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| SRX Series CPE devices | Junos OS Release 20.4R3-S2 | SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145122.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145121.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145169.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145209.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145123.html<br>SRX4100, SRX4200 USB: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| CSO 6.2.0 | 6.2.0 | Cloud Hosted |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145170.html<br><br>SRX4100, SRX4200 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145210.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145125.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145177.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145212.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1 | SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140824.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140823.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140872.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140927.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140825.html<br>SRX4100, SRX4200 USB: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| CSO 6.2.0 | 6.2.0 | Cloud Hosted |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140873.html<br><br>SRX4100, SRX4200 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140928.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140827.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140886.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140930.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| SRX Series next-generation firewall devices | Junos OS Release 20.4R3-S2 | SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145122.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145121.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145169.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145209.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145123.html<br>SRX4100, SRX4200 USB: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145170.html<br><br>SRX4100, SRX4200 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145210.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145125.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145177.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145212.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1 | SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140824.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140823.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140872.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140927.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140825.html<br>SRX4100, SRX4200 USB: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| CSO 6.2.0 | 6.2.0 | Cloud Hosted |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140873.html<br><br>SRX4100, SRX4200 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140928.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140827.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140886.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140930.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| SRX Series provider hub devices | Junos OS Release 20.4R3-S2 | SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145121.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145169.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145209.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145123.html<br>SRX4100, SRX4200 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145170.html<br>SRX4100, SRX4200 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145210.html<br>SRX4600: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| CSO 6.2.0 | 6.2.0 | Cloud Hosted |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145125.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145177.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145212.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1 | SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140823.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140872.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140927.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140825.html<br>SRX4100, SRX4200 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140873.html<br>SRX4100, SRX4200 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140928.html<br>SRX4600: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| CSO 6.2.0 | 6.2.0 | Cloud Hosted |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140827.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140886.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140930.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| SRX Series enterprise hub devices | Junos OS Release 20.4R3-S2 | SRX380:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145122.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145121.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145169.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145209.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145123.html<br>SRX4100, SRX4200 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145170.html<br>SRX4100, SRX4200 PXE: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145210.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145125.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145177.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145212.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1 | SRX380:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140824.html<br>SRX1500:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140823.html<br>SRX1500 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140872.html<br>SRX1500 PXE:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140927.html<br>SRX4100, SRX4200:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140825.html<br>SRX4100, SRX4200 USB:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140873.html<br>SRX4100, SRX4200 PXE: |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | | • https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140928.html<br><br>SRX4600:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140827.html<br><br>SRX4600 USB:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140886.html<br><br>SRX4600 PXE:<br><br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140930.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| vSRX3.0 for SD-WAN devices, next-generation firewall, and hub devices | Junos OS Release 20.4R3-S2 | vSRX3.0 Upgrade TGZ:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145245.html<br>vSRX3.0 KVM Appliance:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145255.html<br>vSRX3.0 Hyper V Image:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145257.html<br>vSRX3.0 VMware Appliance with SCSI virtual disk (.ova):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145256.html<br>vSRX3.0 VMware Appliance with IDE virtual disk (.ova):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/145254.html |

**Table 1: Software Components Associated with CSO Release 6.2.0 *(Continued)***

| Product | Supported Version | Download Link |
|---|---|---|
| **CSO 6.2.0** | **6.2.0** | **Cloud Hosted** |
| | Junos OS Release 20.4R3-S1 | vSRX3.0 Upgrade TGZ:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140969.html<br>vSRX3.0 KVM Appliance:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140979.html<br>vSRX3.0 Hyper V Image:<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140981.html<br>vSRX3.0 VMware Appliance with SCSI virtual disk (.ova):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140980.html<br>vSRX3.0 VMware Appliance with IDE virtual disk (.ova):<br>• https://webdownload.juniper.net/swdl/dl/secure/site/1/record/140978.html |

# Software Installation Requirements for NFX Series Network Services Platform

When you set up a distributed deployment with an NFX150 or an NFX250 device, you must use Administration Portal or the CSO API to:

1. Upload the software image to CSO.

   **NOTE**: If you are an OpCo administrator or a tenant administrator and if you need to upload the required software image, contact Juniper Networks Technical Assistance Center (JTAC).

2. Specify this image as the boot image when you configure activation data.

For more information on NFX series documentation, see https://www.juniper.net/documentation/product/en_US/nfx150 and https://www.juniper.net/documentation/product/en_US/nfx250.

# Accessing the CSO GUIs

**NOTE**: We recommend that you use Google Chrome (Version 60 or later) or Firefox (Version 78 or later) to access the CSO GUIs.

For more information, see Access the Contrail Services Orchestration (CSO) GUIs in the CSO Deployment Guide.

# What's New

**IN THIS SECTION**


- New and Changed Features in Contrail Service Orchestration Release 6.2.0 | **25**

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 6.2.0.

You can view and read the features that are available in the CSO Releases 5.1.2, 5.2.0, 5.3.0, 5.4.0, 6.0.0, and 6.1.0 through the following links:

- CSO 5.1.2 Release Notes
- CSO 5.2.0 Release Notes
- CSO 5.3.0 Release Notes
- CSO 5.4.0 Release Notes
- CSO 6.0.0 Release Notes
- CSO 6.1.0 Release Notes

## New and Changed Features in Contrail Service Orchestration Release 6.2.0

### SD-WAN

- **Support for configuring routing policies in LAN segments**—Starting in CSO Release 6.2.0, you can define routing policies for more control over the route advertisements in a LAN segment. You can use a combination of the **LAN Route(s) to Overlay** option, **Overlay Route(s) to LAN** option, and policies to determine the routes that can be advertised between the LAN router and the SD-WAN overlay.

  You can configure:

  - Export policies for granular control of the routes that a CPE device advertises to the SD-WAN overlay.
  - BGP or OSPF import policies for granular control of the routes that a CPE device accepts from the list of routes advertised by the LAN router.
  - BGP or OSPF export policies for granular control of the routes that a CPE device advertises to the LAN router.

- **ADSL/VDSL Annex J support (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in CSO Release 6.2.0, we support Annex J specification by means of *x*DSL SFP modules for ADSL2, ADSL2+, and all VDSL2 profiles on SRX300 Series devices deployed as branch-site CPE devices. You can configure this feature by enabling the **ADSL/VDSL SFP Annex** option for management interfaces or WAN links when creating sites, adding new WAN links, or granting Return Material Authorization (RMA).

- **MTU support on WAN and LAN interfaces**—Starting in CSO Release 6.2.0, you can configure the maximum transmission unit (MTU) size for the media or protocol on the following interfaces:
  - WAN interfaces of a branch site, enterprise hub, cloud spoke, or a provider hub. The supported MTU range varies depending on the device type and the interface type (Ethernet, ADSL, VDSL, or LTE).
  - LAN interfaces of SRX Series devices, after the site zero-touch provisioning (ZTP) process is complete. The MTU size configured on an SRX Series device must be within the MTU range supported by the switch or router connected to the SRX.

  The MTU configuration is applicable only to IPv4 addresses.
- **Support for editing tenant-owned public IP pool**—Starting in CSO Release 6.2.0, you can add, edit, or delete the public IPv4 subnets that are part of the tenant's pool of public IPv4 addresses. If you modify the IP address pool of a tenant, CSO runs a job to automatically update and reprovision the tenant sites. We consider the tenant IP pool addresses to be public IP addresses that represent public LAN subnets in SD-WAN branch sites.
- **Support for vSRX cluster in SD-WAN deployments**—Starting in CSO Release 6.2.0, you can configure a vSRX cluster as a spoke in SD-WAN deployments. To configure a vSRX cluster as a spoke, the vSRX instances must run Junos OS Release 20.4R3-S1.

### Licensing

- **Support for golden license to onboard SRX Series devices**—Starting in CSO Release 6.2.0, tenants can onboard all SRX Series devices in their network using a single license, referred to as the *golden license*. Using the golden license simplifies the license deployment and management process. Tenants can procure and install only a single license file instead of installing individual device licenses. The golden license is unique to a tenant.

### Miscellaneous

- **Usability enhancements**—Starting in CSO Release 6.2.0, you can:
  - Use site locations and site groups as keywords to search for sites on the **Site Management** page. You can also save these keywords as quick filters.
  - View the WAN link's SLA performance from the WAN tab of a site.
  - View a job summary, which provides the number of sites where a job succeeded or failed. The summary section on the Job Status page lists all the sites where the job failed, with hyperlinks to the site-specific logs containing the job details that include the reason for the failure. When you run a job on multiple sites together, you can quickly identify the sites where the job failed and take actions, if required.

- **Support for alternate partition snapshot (SRX300, SRX320, SRX340, SRX345, and SRX380)**—Starting in CSO Release 6.2.0, you can copy the device image and configuration from the primary (active) partition to the alternate partition of an SRX300 Series device so that both the partitions have the same Junos OS version and device configuration. To update the alternate partition, you can use one of the following methods:

  - Enable the **Snapshot Alternate Partition** option (which is disabled by default) on the device image deployment screen. CSO automatically triggers a separate job to copy the image and the device configuration from the primary partition to the alternate partition only after the image is successfully deployed on the primary partition.

  - Use the **Snapshot Alternate Partition** action from the device list. We recommend this option as it allows you to verify the behavior of the primary partition before copying the image to the alternate partition.

- **Support for tenant-specific SSO server**—Starting in CSO Release 6.2.0, tenants can determine the authentication method for their users. Tenants can either use the authentication method configured by the operating company (OpCo) or change the authentication method for their users from the Authentication page (**Administration > Authentication**). Additionally, tenants can also configure their own SSO server to authenticate users.

  Similar to OpCos, tenants can now select one of the following methods to authenticate their users:

  - Local—CSO maintains the tenant user accounts locally and authenticates users.

  - Authentication by using an SSO server—Tenants use an SSO server (for example, Microsoft Azure Active Directory) to maintain the user identity accounts, while the service provider (CSO) maintains the authorization information. Users are authenticated by using the credentials stored in the SSO server.

  - Authentication and authorization by using an SSO server—Tenants use an SSO server to maintain the user identity accounts and their permitted roles. Users are authenticated by the SSO server and authorized by CSO using Security Assertion Markup Language (SAML) role attributes.

- **Support to edit bootstrap and image upgrade time for SRX Series and NFX150 devices**—Starting in Release 6.2.0, CSO provides the flexibility to configure the bootstrap and image upgrade time for SRX Series and NFX150 devices. By default, the bootstrap time is 30 minutes and the image upgrade time is 60 minutes. Based on the network operation and performance, global or tenant administrators can choose to either increase or decrease the time.

# Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 6.2.0.

**Device Management**

- The SRX4100, SRX4200, and SRX4600 devices support all existing SD-WAN features, except the following:
  - Phone-home client (PHC)—The devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX4100, SRX4200, and SRX4600 devices, and then committing the stage-1 configuration.
  - LTE and xDSL interfaces.
- LTE and xDSL interfaces are not supported on dual CPE devices.
- You cannot remotely access a cloud spoke device and edit the configuration.
- You can install and use only an external LTE Vodafone K5160 dongle to the NFX250 device.
- NFX150 is not supported in cluster mode.
- UTM Web filtering is not supported in an active-active SRX Series cluster device.
- ADSL and VDSL are not supported on an NFX250 device running Junos OS Release 18.4R.
- Prestaging is required for ZTP over PPPoE-enabled WAN link.
- For SRX series devices, you must manually install the device certificates after the ZTP is complete. To manually install the certificate, select the SRX series device on the **Resources > Devices** page and click **More > Install Certificates**.

**Dynamic VPN (DVPN)**

- Creation and deletion of DVPN tunnels based on the DVPN create and delete thresholds are governed by the **MAX_DVPN_TUNNELS** and **MIN_TUNNELS_TO_START_DVPN_DEACTIVATE** parameters, respectively. However, **MAX_DVPN_TUNNELS** and **MIN_TUNNELS_TO_START_DVPN_DEACTIVATE** are not honored when when site-to-site tunnels are created or deleted from the CSO UI. This might cause the total active DVPN tunnels count on the **Site > WAN** tab to show a greater value than the **MAX_DVPN_TUNNELS** value configured for that site.
- DVPN create and delete thresholds are based on the **APPTRACK_SESSION_CLOSE** messages. When **APPTRACK_SESSION_CLOSE** messages reach the specified threshold, an alarm is generated for

creating or deleting a DVPN tunnel. However, the alarms are not cleared until the **APPTRACK_SESSION_CLOSE** message count goes below the threshold (for create alarms) or above the threshold (for delete alarms) to trigger a fresh cycle. This causes the create and delete alarms to remain active and prevent further alarms and to, thus, slow down the creation or deletion of tunnels.

- Passive probes created by an SD-WAN policy time out because of inactivity in 60 seconds. This causes CSO to close the corresponding sessions and trigger **APPTRACK_SESSION_CLOSE** messages. The **APPTRACK_SESSION_CLOSE** messages are tracked and added to the number of sessions closed. The sessions closed count is used to calculate the DVPN delete threshold.

**Policy Deployment**

- An SD-WAN policy deployment is successful even if there is no matching WAN link meeting the SLA. This is expected behavior and it ensures that when a WAN link matching the SLA becomes available, traffic is routed through that link.
- The policy intents defined for a firewall or an SD-WAN policy must not have conflicts with other policy intents in that policy because such conflicts lead to inconsistent behavior. For example:
  - You cannot define an SD-WAN policy with one policy intent for application X and SLA profile S-1 and another policy intent for application X and SLA profile S-2.
  - You cannot define two firewall policy intents with the same source and destination endpoints but one with action Allow and another with action Deny.
- The SD-WAN policy intents do not support selecting 'none' in the Apps field as an application endpoint.
- For every SD-WAN policy intent with a specific address or service, you must define a firewall intent with the same name as the SD-WAN policy intent.

**SD-WAN**

- You cannot change the MTU values for the logical interfaces. For example, if you create two LAN segments on the same physical port with two different VLANs, the MTU values on both the VLANs are the same as that of the physical port. You cannot configure different MTU values for the VLANs.
- CSO explicitly disables the long-lived graceful restart capability for BGP peering sessions with provider edge (PE) and data center or LAN routers. Disabling long-lived graceful restart ensures that the CPE device does not differentiate the route advertisements to the peering router irrespective of the peering router's long-lived graceful restart capability.
- If WAN link endpoints are not of similar type but overlay tunnels are created based on matching mesh tags, the static policy for site-to-site or central Internet breakout traffic gives preference to the remote link type.

- Advanced SLA configurations, such as CoS rate limiting, are not supported during local breakout if no specific application is selected; that is, if Application is set to ANY. Choose specific applications if you want to enable advanced SLA configurations, such as CoS rate limiting.

- If two or more SD-WAN policy rules are configured for the same application with different levels of granularity, such as all, sites, and departments, then CSO applies the CoS rate limiter in the same order in which you have created the intents.

- On the SD-WAN Events page, when you hover the mouse over the Reason field of link switch events, sometimes Above Target is displayed instead of the absolute SLA metric value for very large values (for example, for an SLA metric value that is 100 times the target value).

- Active-Active mode is not supported with cloud breakout for GRE tunnels.

- You cannot add a LAN segment to a Dual SRX site in CSO upgraded to Release 6.0.0 if the site has not been upgraded.

  So, to add a LAN segment to a site, you must first do the following:

  - Upgrade the site (SeeUpgrading Sites.)

  - Update the Dual_SRX_Platform template with the correct FAB interface details (See Configuring Template Settings in a Device Template.)

  After the above steps, add the LAN segment to the site from Device page on the LAN tab. While adding the LAN segment details, remember to create RETH interface and enable LACP. See Add a Branch Site with SD-WAN Capability.

**Site and Tenant Workflow**

- An NFX250 site is automatically upgraded to the current CSO version after performing RMA of an old site (prior to site upgrade). Prior to site upgrade on an NFX dual-CPE site, RMA is supported only at the cluster level, not at the node level.

- In the Add Site workflow, use IP addresses instead of hostnames for the NTP server configuration. If you are using hostnames instead of IP addresses, ensure that the hostname is DNS-resolvable; if the hostname is not DNS-resolvable, ZTP for the device fails.

- CSO uses RSA-key-based authentication when establishing an SSH connection to a managed CPE device. The authentication process requires that the device has a configured root password, and you can use Administration Portal to specify the root password in the device template.

  To specify a root password for the device:

  1. Log in to Administration Portal.

  2. Select **Resources > Device Templates**.

3. Select the device template and click **Edit**.
4. Specify the plain text root password in the **ENC_ROOT_PASSWORD** field.
5. Click **Save**.

- When you try to deploy a LAN segment on an SRX Series spoke device, the CSO GUI allows you to select more than one port for a LAN segment. However, for SRX Series devices, only one port for a LAN segment can be deployed; multiple ports in a LAN segment can be deployed only on NFX Series devices.
- In case of multiple LAN segments under the same department (VPN) configured with OSPF protocol, the Overlay Route(s) to LAN knob should be configured in the same way for all of them (either ON or OFF).
- On a site with an NFX Series device, if you deploy a LAN segment without the VLAN ID specified, CSO uses an internal VLAN ID meant for internal operations and this VLAN ID is displayed in the LAN section of the Site Detail View page. There is no impact on the functionality.
- Do not create departments that have names starting with **default**, **default-reverse**, **mpls**, **internet**, or **default-hub** because CSO uses the following departments for internal use:
  - Default-*vpn_name*
  - Default-reverse-*vpn_name*
  - mpls-*vpn_name*
  - internet-*vpn_name*
  - Default-hub-*vpn_name*
- Site edit fails if you try to edit the MTU WAN value for a site that is running CSO 6.1.0 or an earlier release.

**User Interface**

- When you use Mozilla Firefox to access the CSO GUIs, a few pages do not work as expected. We recommend that you use Google Chrome version 60 or later to access the CSO GUIs.
- When you copy and paste a stage–1 configuration from Chrome version 71.0.3578.98, insert a new line, as shown in the following example, in the private key text:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,1F6A1336016A8239
```

```
ADD A NEW LINE HERE
2C638z/Lgr/g4Kw7r9lys9XWnUGbGnPpT1cc5jGq1Qbb8Nu286QsVGfrUy7Qh9sU
FJkIQI9bOMNadLL7wklsnwBCVAoAYjX+haizSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWFgWcwUi+ijUKp/h9NfE5c2W5m2VBdmRjBfjWo9jcH
HV5gkkoG0Gdx7Kv60HKOMDl2YkjL4zfAzBS8J8BMmk5x6sY+GqNQOdgs7m4oXYCH
1loOYS6n9l0WDZcxXYWWeINlu6zOSIlZYVIdwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

If you do not insert the new line, the private key fails.

### General

- The site deletion process is split into two phases to minimize the overall time required to delete a site:
  - Site deletion (phase 1)—The device is zeroized, all activation information is removed from CSO, and the site is deleted from the GUI. After deletion, you can onboard the site using the same name or a different name.
  - Site cleanup (phase 2)—The cleanup process is triggered after the site is deleted. This process removes all the configuration associated with the site from the provider or enterprise hub, a spoke site to which this site is connected, and virtual Route Reflectors (vRRs).

    **NOTE**: For optimization purposes, configurations on spoke sites might not be deleted during the cleanup phase. In such cases, the configurations are deleted during the next commit operation on the spoke devices.

- On an NFX Series device:

  To activate a virtualized network function (VNF), perform the following steps:

  1. Add the VNF to the device.
  2. Initiate the activation workflow and ensure that the job is 100% completed.

  To retry the activation of a VNF that failed, perform the following steps:

  1. Deactivate the VNF.
  2. Remove the VNF.
  3. Add the VNF to the device.
  4. Initiate the activation workflow and ensure that the job is 100% completed.

- Enterprise hub is not supported for cloud spoke sites.

- CSO internally uses IP addresses starting from 100.112.0.0 through 100.127.255.255. You must avoid using these IP addresses in LAN subnets.
- NFX250 uses some IP addresses in the 192.0.2.0/24 subnet for VNF management. You must avoid using these IP addresses in a LAN. For more information about the usage of this subnet, see the NFX250 documentation.
- Starting from CSO Release 6.2.0, you can use VLAN IDs in the following ranges to configure LAN segments:
  - SRX Series devices (single and dual CPE) and vSRX: 1 – 4094 (in releases prior to CSO Release 6.2.0, the range is 1 – 4049)
  - NFX250 (single and dual CPE) and NFX150 devices: 1 - 4049
- If a tenant has an overlapping IP address configured across departments, then to access the resources in the enterprise hub's data center, you must apply a source NAT rule with source as the trust zone and destination as the data center department zone on the enterprise hub device.
- If an overlapping IP address is configured on the same site across departments, hosts in the overlapping subnet are unable to deterministically access data center routes behind nonprimary enterprise hubs.
- The end-to-end traffic cannot be established if two LAN hosts within a tenant have traffic such that all the 5 tuples are exactly the same and the destination IP address is in the data center that is hosted behind nonprimary enterprise hubs.
- If you initiate the Sync Alarm operation from the Alarms page, the timestamp of the synchronized alarms changes to the time the Sync Alarm operation is initiated.

# Known Issues

This section lists known issues in Juniper Networks CSO Release 6.2.0.

**SD-WAN**

- In case of SRX3xx chassis cluster, data tunnels on secondary node are reported as down. Traffic continues to flow through tunnels connected to the primary node.

  Workaround: There is no known workaround.

  Bug Tracking Number: PR 157491

- When an SD-WAN controller is down or not reachable from CSO, you cannot delete a site or tenant from CSO.

  Workaround: Recover the SD-WAN controller and retry deleting the site or tenant.

  Bug Tracking Number: CXU-43724

- When configuring a DVPN tunnel between two devices, if one device is not functional while the other is functional, the DVPN tunnel should not be configured on the device that is functional.

  Workaround: If a DVPN tunnel is configured on the functional device, delete the tunnel manually.

  Bug Tracking Number: CXU-46188

- VNFs are not coming up in NFX150 running on Junos OS Release 19.3R2-S3 due to non availability of the required number of CPUs.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-49268

- If you are an OpCo administrator and edit the OAM and CONTROL traffic profiles after your tenants have deployed SD-WAN policy intents, then the changes are not immediately applied on your tenant devices.

  Workaround: The changes are applied to the device only when your tenants redeploy the SD-WAN policy.

  Bug Tracking Number: CXU-52482

- You must specify the same value for the Loss Priority field on the SLA Profile page and the Traffic Type Profile page; otherwise, the Loss Priority parameter might not be applied during the traffic congestions.

  Workaround: Ensure that you specify the same value for the Loss Priority field on the SLA Profile and Traffic Type Profile pages.

  Bug Tracking Number: CXU-52516

- CSO does not create tunnels in redundant sparse mode between primary and backup WAN links. The WAN links added as redundant sparse links must be either backup links or primary links in both the sites.

  Workaround:

  - To connect a branch site to its parent enterprise hub: On the site edit screen, disable the **Use Mesh Tags to Connect Ehub** option, enable the **Connects to Enterprise Hubs** option, and manually select the end points.

  - To connect a branch site to another branch site: Edit the mesh tags so that one overlay tunnel is formed over each WAN link.

  Bug Tracking Number: CXU-59071

- Traffic does not flow from the primary to the secondary enterprise hub if the CSO version is different on both the hubs.

  Workaround: Ensure that the CSO version is the same on both the hubs.

  Bug Tracking Number: CXU-58666

### High Availability

- On an SRX4200 chassis cluster, LAN segment with aggregated interface with LLDP enabled fails.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-54985

### Security Management

- On NFX150 and NFX250 devices, firewall policies are not applied automatically after RMA.
  Workaround: After the RMA is done, you must apply the policy configurations again after adding the necessary licenses, certificates, and signatures.

  Bug Tracking Number: CXU-51335

- If UTM Web-filtering categories are installed manually (by using the `request system security UTM web-filtering category install` command from the CLI) on an NFX150 device, the intent-based firewall policy deployment from CSO fails.
  Workaround: Uninstall the UTM Web-filtering category that you installed manually by executing the `request security utm web-filtering category uninstall` command on the NFX150 device and then deploy the firewall policy.

  Bug Tracking Number: CXU-23927

- When you try to deploy a firewall policy with the destination application as **none**, the deployment fails with the error message `junos-defaults should be configured along with dynamic-application`.
  Workaround: Create the firewall policy with the destination application as **none**, service as **any**, and deploy the policy.

  Bug Tracking Number: CXU-60302

### Site and Tenant Workflow

- Remote console from the CSO GUI to an SRX4200 or SRX1500 device sometimes uses Read-Write user even if Read-only option was selected while launching the remote console.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-57051

- If service provisioning job for a site is in progress, you should not attempt Edit Site or Delete Site operation.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-53721

- When the non-preferred link-type for an application transitions from SLA violated to SLA met, during the time when the non-preferred link-type is being used. The application flow does not transition to preferred link type even if it is available. This happens till the time non-preferred link-type again transitions to SLA violated.
  Workaround: Bounce the non-preferred link type.

  Bug Tracking Number: CXU-55353

- Site edit might fail in case of conflicting user defined templates deployed on the device.
  Workaround: Undeploy the user defined templates prior to edit operations and re-deploy the user defined templates post edit.

  Bug Tracking Number: CXU-55399

- When you enable Local Internet Breakout (LBO) on the WAN by using site edit workflow, the underlay traffic might drop.
  Workaround: Deploy new firewall policy post WAN edit operation.

  Bug Tracking Number: CXU-53095

- If you delete an SD-WAN intent on a site that has a modelled LAN segment, then the configuration is not deleted from the device.
  Workaround: Deploy or delete the modelled LAN segment.

  Bug Tracking Number: CXU-59863

### General

- When upgrading a vSRX cluster, only the primary node of the cluster is upgraded.
  Workaround: Upgrade each node in the cluster individually, using the steps below:

  1. Initiate an image deploy job on the device to upgrade the current primary node (node0).
     After the image deployment is completed and the node0 is rebooted, the secondary node (node1) takes over as the primary node.

  2. Initiate another image deployment job on the device to upgrade the new primary node (node1).

  Bug Tracking Number: CXU-59997

- The `show class-of-service interface <ifl>` command does not show the correct CoS profiles when the command is applied using wildcard configurations.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-57580

- Zoom calls will be shown under zoom-voice-video or not as zoom-voice and zoom video due to platform dependency.

  Workaround: There is no known workaround.

  Bug Tracking Number: PR1589933

- When a power failure occurs, CAN becomes unhealthy.

  Workaround: Contact customer support.

  Bug Tracking Number: CXU-58306

- Configuration template deployment for common-dnssplit-hub on hub and common-dnssplit-spoke on site might fail.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-54299

- Bootstrap job waits until it tries for a few times to send the bootstrap complete message to CSO. After the bootstrap job fails from CSO side, it tries to connect to CSO on the device side, and then the ZTP job starts.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-57280

- If more than one alarm of the type Chassis/Fan/PEM/Control_board/ RE/Configuration/License/ Temperature is active on the device, only one alarm is shown in the CSO GUI summarizing with a count mentioned in the alarm description.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-57280

- On an SRX4600 device, the same 40G (et) interface can be shared with two WAN links only if both the WAN interfaces are VLAN tagged. If any one of the WAN interface is untagged, the deployment fails.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-58158

- Load recovery configuration fails with ***warning: The cso_telemetry_agent package is not allowed by the candidate configuration.** message if the device or site is reused without deleting from CSO.

  Workaround: Run the command, `request system software delete cso_telemetry_agent` on the device, and then initate the commit of recovery configuration.

  Bug Tracking Number: CXU-57924

- When a Spoke's Primary-EHUB (EHUB1) is not site-upgraded and Secondary-EHUB (EHUB2) is site-upgraded, then traffic from Spoke to Secondary-EHUB Datacenter may not work.

Workaround: You can do one of the following:

- Upgrade both the Primary and Secondary EHUB.
- Advertise same routes from both Primary and Secondary E-Hub Datacenter, then traffic continues to take the Primary Datacenter.

Bug Tracking Number: CXU-58124

- In some cases, bootstrap job is not triggered if SRX ZTP is executed over LTE WAN link with factory default configuration. On SRX345 devices running CSO, ZTP fails with factory-default configuration if the internet connectivity is through the LTE interface.
  Workaround: Run the `delete chassis auto-image-upgrade` command from the factory-default configuration and commit.

  Bug Tracking Number: PR 1569595

- On NFX150 Series devices, Class of Service (CoS) does not work for PPP interface.
  Workaround: There is no known workaround.

  Bug Tracking Number: PR 1581489

- Even after you change the Site name by using site-edit option, some of the job logs might still refer to the old site-name. However, this does not affect the service.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-54355

- You should not select OPCO name in SRX-HUB-BREAKOUT template and deploy. The template deployment fails in such cases.
  Workaround: You should remove the OPCO name selected in in SRX-HUB-BREAKOUT template and redeploy the template.

  Bug Tracking Number: CXU-54312

- On an SRX Series device, the deployment fails if you use the same IP address in both the Global FW policy and the Zone policy.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-41259

- Tenant owned Public IP Pool can be edited until the first SD-WAN site is onboarded in that tenant. After you onboard an SD-WAN site, Tenant owned Public IP Pool cannot be edited.
  Bug Tracking Number: CXU-41139

- When you upgrade the image for SRX4200 dual CPE device, the job status is displayed as Success even though the reboot is in progress for the secondary node.

Workaround: Check the status of the cluster and the FPC status on the primary node before proceeding with any other activity on the CPE device.

Bug Tracking Number: CXU-52974

- Ubuntu service chaining instance fails on NFX150.
  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-52512

# Resolved Issues

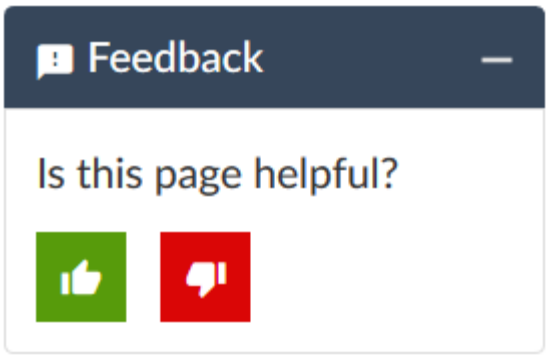
The following issues are resolved in Juniper Networks CSO Release 6.2.0:

- Changing the **Password Expiration Days** parameter does not impact existing users of a tenant.
  Bug Tracking Number: CXU-54818

# Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:




  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable)

# Requesting Technical Support

IN THIS SECTION


- Self-Help Online Tools and Resources | 40
- Creating a Service Request with JTAC | 41


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 https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

# Self-Help Online Tools and Resources

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

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://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/
- Create a service request online: https://myjuniper.juniper.net/

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 https://myjuniper.juniper.net/
- 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/.