Contrail Service Orchestration Release Notes

Release 5.3.0
October 8, 2020
Revision 5

These Release Notes accompany Release 5.3.0 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction

You can use CSO Release 5.3.0 as a cloud-based service.

CSO Release 5.3.0 supports the following types of accounts:

- OpCo accounts (for multitenant, managed service providers)—OpCo (operating company) administrators can add tenants to and enable services such as SD-WAN, LAN, 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 account (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, LAN, and next-generation firewall for their networks. They can also configure SLA policies, firewall policies, and breakout policies, and also apply the policies to the sites.

The following are the highlights of the features available in CSO Release 5.3.0:

- **SD-WAN features**
  - Support for adding configuration templates while creating site templates
  - Enhancement to the edit site properties feature
  - PPPoE support for WAN Ethernet interfaces
- **SD-LAN features**
  - Enhancements to the on-premises spoke site and site template workflow
- **Miscellaneous**
  - Support for SRX550M, SRX1500, SRX4100, and SRX4200 devices as next-generation firewall devices
  - Support for Firefox for accessing CSO GUI
  - Support for TLS and TCP for syslog messages
  - RMA support for provider hub devices, enterprise hub devices, and next-generation firewall devices

Software Support

IN THIS SECTION

Software Downloads

Table 1 on page 4 displays the supported versions and download links for software components associated with CSO Release 5.3.0.

NOTE:

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.
- In CSO Release 5.3.0, you can continue to manage devices running Junos OS Release 15.1X49-D172 that were onboarded in the earlier releases of CSO. However, if you are upgrading Junos OS on a device that is managed by CSO Release 5.3.0 or onboarding a device newly to CSO Release 5.3.0, the device must run Junos OS Release 19.3R2-S3.
- In addition to Junos OS Release 19.3R2-S3, CSO Release 5.3.0 also supports Junos OS Release 19.3R2-S4.

  For information about issues fixed in Junos OS Release 19.3R2-S4, see the Junos OS Release 19.3R2-S4 Release Notes.

Table 1: Software Components Associated with CSO Release 5.3.0

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

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
EX Series switches	Junos OS Release 18.4R3-S3	Junos OS Release 18.4R3-S3 • EX2300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/111100.html?pf=EX2300 • EX3400: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/111100.html?pf=EX2300 • EX4300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109631.html?pf=EX4300 • EX4600: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109681.html?pf=EX4600 • EX4650: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109689.html?pf=EX4650
NFX150 CPE device	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	Junos OS Release 19.3R2-S3 • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110795.html?pf=NFX150 • Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110724.html?pf=NFX150
		Junos OS Release 19.3R2-S4 • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114104.html?pf=NFX150 • Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114033.html?pf=NFX150
NFX250 CPE device	Junos OS Release 18.4R3-S3 with 19.3R2-S3 for vSRX3.0 Junos OS Release 15.1X53-D497 with 15.1X49-D172 for vSRX if vSRX was onboarded in an earlier version of CSO Junos OS Release 19.3R2-S4 for vSRX	Junos OS Release 18.4R3-S3 • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109826.html?pf=NFX250 • Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109672.html?pf=NFX250
		Junos OS Release 19.3R2-S4 • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114104.html?pf=NFX150 • Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114033.html?pf=NFX150

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
SRX Series CPE devices	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices): • Junos OS 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110749.html?pf=SRX300 • Junos OS 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114058.html?pf=SRX300
		SRX1500 • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110820.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114057.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114087.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114129.html?pf=SRX1500

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
		SRX4100, SRX4200: • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110821.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114057.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114087.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114129.html?pf=SRX1500

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
SRX Series next-generation firewall devices	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M: • Junos OS 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110749.html?pf=SRX300 • Junos OS 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114058.html?pf=SRX300
		SRX1500 • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110820.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114057.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114087.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114129.html?pf=SRX1500

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
		SRX4100, SRX4200: • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110821.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114059.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114088.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114130.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
SRX Series provider hub devices	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	SRX1500 • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110820.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114057.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114087.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114129.html?pf=SRX1500
		SRX4100, SRX4200: • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110821.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114059.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114088.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114130.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
SRX Series enterprise hub devices	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	SRX1500: • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110820.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114057.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114087.html?pf=SRX1500 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114129.html?pf=SRX1500
		SRX4100, SRX4200: • Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100 • Junos OS Release 19.3R2-S3 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110821.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114059.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114088.html?pf=SRX4100 • Junos OS Release 19.3R2-S4 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114130.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
vSRX for SD-WAN devices	Junos OS Release 15.1X49-D172 for devices onboarded in earlier versions of CSO Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	For hub devices (enterprise hub and provider hub) and spoke devices: vSRX (compressed tar file (TGZ) for upgrade): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110842.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114151.html?pf=vSRX
		vSRX (KVM appliance): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110851.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114160.html?pf=vSRX
		vSRX (Hyper-V image): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110850.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114159.html?pf=vSRX
		vSRX (VMware appliance with SCSI virtual disk (.ova)): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110853.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114162.html?pf=vSRX
		vSRX (VMware appliance with IDE virtual disk (.ova)): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110852.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114161.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
vSRX for next-generation firewall devices	Junos OS Release 18.4R1 Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	vSRX (compressed tar file (TGZ) for upgrade): • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86039.html?pf=vSRX • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110842.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114151.html?pf=vSRX
		vSRX (KVM appliance): • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86042.html?pf=vSRX • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110851.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114160.html?pf=vSRX
		vSRX (Hyper-V image): • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86041.html?pf=vSRX • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110850.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114159.html?pf=vSRX
		vSRX (VMware appliance with SCSI virtual disk (.ova)): • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86044.html?pf=vSRX • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110853.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86043.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.3.0 *(continued)*

Product	Supported Version	Download Link
		vSRX (VMware appliance with IDE virtual disk (.ova): • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86043.html?pf=vSRX • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110852.html?pf=vSRX • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114161.html?pf=vSRX
vSRX3.0 for SD-WAN, next-generation firewall, and hub devices	Junos OS Release 19.3R2-S3 Junos OS Release 19.3R2-S4	vSRX3.0 (compressed tar file (TGZ) for upgrade): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110843.html?pf=vSRX3.0 • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114152.html?pf=vSRX3.0
		vSRX3.0 (KVM appliance): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110855.html?pf=vSRX3.0 • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114164.html?pf=vSRX3.0
		vSRX3.0 (Hyper-V image): • Junos OS Release 19.3R2-S3: https://https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110857.html?pf=vSRX3.0 • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114166.html?pf=vSRX3.0
		vSRX3.0 (VMware appliance with SCSI virtual disk (.ova)): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110856.html?pf=vSRX3.0 • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114165.html?pf=vSRX3.0
		vSRX3.0 (VMware appliance with IDE virtual disk (.ova)): • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110854.html?pf=vSRX3.0 • Junos OS Release 19.3R2-S4: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114163.html?pf=vSRX3.0

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 .

New and Changed Features in Contrail Service Orchestration Release 5.3.0

IN THIS SECTION

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.3.0.

You can view and read the features that are available in the CSO Releases 5.1.0, 5.1.1, 5.1.2, and 5.2.0 through the following links:

- CSO 5.2.0 Release Notes
- CSO 5.1.2 Release Notes
- CSO 5.1.1 Release Notes
- CSO 5.1.0 Release Notes

SD-WAN

- **Support for adding configuration templates while creating site templates**—From CSO Release 5.3.0 onward, you can add one or more configuration templates while creating a site template. You can select the configuration templates from the Additional Configuration section of the Add Site Template page, and then set the parameters for the configuration templates that you have selected.
- **Enhancement to the edit support for site properties**—From CSO Release 5.3.0 onward:
  - A tenant administrator user can edit the general parameters and WAN parameters of an existing spoke site (with SD-WAN or next-generation firewall capabilities) or an enterprise hub site from the Site Management page (**Resources** > **Site Management**).
  - An OpCo administrator user can edit the parameters of a provider hub site with DATA_ONLY capability from the Provider Hub Devices page (**Resources** > **Provider Hub Devices**).

    NOTE: You cannot edit spoke sites with SD-LAN capability and cloud spoke sites.

- **PPPoE support on Ethernet interfaces**—From Release 5.3.0 onward, CSO supports Point-to-Point Protocol over Ethernet (PPPoE) for the Ethernet access type on SRX Series and NFX Series devices.

SD-LAN

Enhancements to the spoke site and site template workflow—From CSO Release 5.3.0 onward, you can do the following while adding an spoke site and site template to CSO:

- Add multiple EX Series switches (physical and Virtual Chassis) while adding an SD-LAN site template or an SD-LAN site.

  In releases before CSO Release 5.3.0, you can add multiple EX Series switches, one at a time, only to an existing SD-LAN site.

- Edit the parameters configured for an EX Series switch while adding the switch to a site template or a site.
- Delete EX Series switches that you added while creating a site template or manually adding a site (that is, without using a site template). In releases before CSO Release 5.3.0, you can edit the parameters of the switch that you added, but cannot delete it, while manually configuring the site.
- Assign the following while adding a site template while adding EX Series switches to a site template:
  - Access profile and configuration templates to the switch.
  - Port profiles to the switch ports.

Miscellaneous

- **Support for SRX550M, SRX1500, SRX4100, and SRX4200 devices as next-generation firewall devices—**From CSO Release 5.3.0 onward, we support the following SRX Series devices as a next-generation firewall devices: SRX550 High Memory Services Gateway (SRX550M), SRX1500, SRX4100, and SRX4200.
- **Support for Firefox for accessing CSO GUIs—**From CSO Release 5.3.0 onward, you can use Mozilla Firefox (Version 78 or later) to access the CSO GUIs.
- **Enhancements to CSO GUIs—**From CSO Release 5.3.0 onward, you can use the following GUI enhancements:
  - Improved performance of the existing workflows in GUI.
  - New icons introduced at the top-right corner of the GUI to view the policies that are due for deployment, alarms and alerts on all the devices managed by CSO, and CSO jobs that are in progress and scheduled.
  - A new menu—Favorites—introduced for quickly accessing the pages that you frequently visit. We have also added a star icon at the right corner of each page to add the page to the Favorites menu.

  - Personalized themes and navigation modes in the portal.
  - Three new widgets—Device Count by Platform, Device Count by OS, and Device Count by Status—added to the dashboard.

- **Support for TLS and TCP for syslog messages**—From CSO Release 5.3.0 onward, in a next-generation firewall deployment, the firewall devices send syslog messages to CSO by using Transport Layer Security (TLS) and Transmission Control Protocol (TCP).
- **Enhancements to configuration templates**—From CSO Release 5.3.0 onward, you can perform the following actions on configuration templates from Administration and Customer Portals:
  - Undeploy a configuration template from a device.
  - Dissociate a configuration template from a device.
  - Rename a configuration template (by using the Edit operation).
  - Export a configuration template as a ZIP file.
- **RMA support for provider hub devices, enterprise hub devices, and next-generation firewall devices**—From CSO Release 5.3.0 onward, you can initiate the Return Material Authorization (RMA) workflow for a defective SRX Series provider hub device, enterprise hub device, and next-generation firewall device. RMA is supported for the following SRX Series models:
  - SRX Series provider hub devices: SRX1500, SRX4100, SRX4200, and vSRX
  - SRX Series enterprise hub devices: SRX1500, SRX4100, SRX4200, and vSRX
  - SRX Series next-generation firewall devices: SRX300, SRX320, SRX340, SRX345, SRX550M, SRX1500, SRX4100, SRX4200, and vSRX

Deprecated Feature

- **Hybrid WAN**—From CSO Release 5.3.0 onward, CSO will not support hybrid WAN deployments.

VNFs Supported

CSO supports the VNFs listed in Table 2 on page 19.

Table 2: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX3.0	For SD-WAN deployments: vSRX KVM Appliance 15.1X49-D172 if deployed in an earlier version of CSO. vSRX3.0 19.3R2-S3	• Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM)	SD-WAN deployments supports NAT, firewall, and UTM.
Ubuntu	16.04		SD-WAN (all LAN-side functions) deployments–NFX250 and NFX150 platforms.
Fortinet	5.6.3		SD-WAN (all LAN-side functions) deployments–NFX250 and NFX150 platforms.

Licensing

For the cloud-hosted CSO solution, you need to purchase licenses to manage devices in CSO. As part of the activation process, you must provide the information required for creating your CSO account. After the account is activated, you receive an e-mail with the URL information and access credentials for logging in to the CSO portal.

For the on-premises CSO solution, you must have licenses to download and use Juniper Networks CSO. When you order licenses, you receive the information that you need to download and use CSO. If you did not order the licenses, contact your account team or Juniper Networks Customer Care for assistance.

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 *Accessing the Contrail Services Orchestration GUIs* topic in the *CSO Deployment Guide*.

Known Behavior

IN THIS SECTION

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.3.0.

Device Management

- The SRX4100 and SRX4200 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 and SRX4200 devices, and then committing the stage-1 configuration.
  - LTE and xDSL interfaces.
- In a dual SRX Series cluster, the devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX Series device, and then committing the configuration.
- 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 intall and use only an external LTE Vodafone K5160 dongle to the NFX250 device.
- NFX150 is not supported in cluster mode.
- You cannot use an NFX150 dual CPE device for deploying SD-WAN services.
- Do not zeroize EX2300 and EX3400 devices because doing so might result in unexpected behavior.
- PHC is supported for EX2300, EX3400, and EX4300 switches (except EX4300-MP) with Junos OS Release 18.4R2 and later. The CSO release is qualified for Junos OS Release 18.3R1, and the PHC capability is currently not supported for EX Series switches that are onboarded with Junos OS Release 18.3R1.

  If the PHC capability is not supported for EX Series switches, you must manually copy the stage-1 configuration from the CSO portal and paste it into the device console to commit the stage-1 configuration when you create a LAN site or activate an EX Series switch.
- UTM Web filtering is not supported in an active-active SRX Series cluster device.

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 DVPNs 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.

SD-WAN

- 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.
- ADSL and VDSL are not supported on an NFX250 device running Junos OS Release 18.4R3.3.

SD-LAN

- When a Virtual Chassis member goes down, the chassis view shows the last known status of the Virtual Chassis member ports until the member is up again.

Site and Tenant Workflow

- 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.
- 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*

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

- 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.
- VLAN IDs 4050 through 4094 are reserved for CSO configurations.

Known Issues

IN THIS SECTION

This section lists known issues in Juniper Networks CSO Release 5.3.0.

SD-WAN

- If a provider hub is used by two tenants, one with public key infrastructure (PKI) authentication enabled and other with preshared key (PSK) authentication enabled, the commit configuration operation fails. This is because only one IKE gateway can point to one policy and if you define a policy with a certificate, then the preshared key does not work.

  Workaround: Ensure that the tenants sharing a provider hub use the same type of authentication (either PKI or PSK) as the provider hub device.

  Bug Tracking Number: CXU-23107

- Sometimes, jobs to update NAT information are not getting triggered. Therefore, NAT port assigned to a DVPN IPsec configuration is incorrect.

  Workaround: Delete and create the DVPN tunnels manually by using the CSO GUI.

  Bug Tracking Number: CXU-46183

- While creating an IPsec tunnel between an Internet link that is behind NAT in a spoke to an MPLS link in an ENT hub, wrong NAT interface is configured on the IPsec tunnel. Therefore, the tunnel fails to be created.

  Workaround: You must trigger a NAT update job immediately to assign the correct NAT IP to static tunnel.

  Bug Tracking Number: CXU-46185

- 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: There is no known 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

- Upgrade of Junos OS Release 15.1X49-D172 to Junos OS Release 19.3R2-S3 fails on SRX 4100, SRX4200, and SRX300 dual CPE clusters, when functioning as enterprise hubs, due to incorrect IPsec configuration and CLI validations.

  Workaround: To upgrade the Junos OS image from Release 15.1X49-D172 to Release 19.3R2-S3:

  1. Log in to Customer Portal.

  2. Navigate to **Resources > Templates > Configuration Template**.

3. Select the **srx-rouser** template and click **Deploy to Devices**.

4. Select the device that you want to upgrade and click **Next**.

5. Select **Is Admin** for the device and click **Next**.

   The Configure Device Parameters tab is displayed.

6. Select the device that you want to upgrade and click the **Set Parameters** button above the Device table.

   The Device Configuration for the Device page appears.

7. Click the **Is Admin** toggle button to enable the **Is Admin** option.

   The rouser gets administrator privileges.

8. Click **Save** to save the configuration.

9. Click **Next**.

   The Deploy tab is displayed.

10. Select **Run now** for Choose Deployment Time.

11. Click **Finish**.

12. Access the terminal of the primary device.

    To access the device terminal:

    a. Navigate to **Resources > Devices**.

    b. Select the device and click **More > Remote Console**.

13. On the device console, access the shell and enter the following command:

```
cli -c 'show configuration | display set | grep encryption-algorithm | grep cbc
 | grep "ike proposal"' | awk -Fencryption-algorithm '{b=$1"
authentication-algorithm sha-256"; print b}'
```

14. Copy the output displayed to a text file.

15. Again, enter the following command:

```
cli -c 'show configuration | display set | grep encryption-algorithm | grep cbc
 | grep "ipsec proposal"' | awk -Fencryption-algorithm '{b=$1"
authentication-algorithm hmac-sha-256-128"; print b}'
```

16. Append the text file with the output of the command executed in Step 15.

17. Switch to edit mode on the device by typing **Edit** at the command prompt.

18. Copy the commands from the text file and paste them into the device CLI.

19. Copy the Junos OS Release 19.3R2-S3 image to the device either by using CSO or manually.

    To copy the image to the device by using CSO:

    a. Switch to Administration Portal.

    b. Navigate to **Resources > Images**.

    c. Click the **Add** icon (+) to upload the image.

    d. Wait until the upload is successful.

    e. Switch to Customer Portal.

    f. Navigate to **Resources > Images** and select the uploaded image.

    g. Click **Stage**.

    h. On the Stage Image page, select the device, ensure **Run Now** is selected for Choose Deployment time, and click **OK**.

       The device image is copied only to the primary device.

20. Copy the image to the backup device.

    To copy the image to the backup device, access the remote terminal of the backup device by referring to Step12 and enter the following command:

```
file copy <image location> nodex <new image location>

      Where, <image with location> nodex is the location of the image on node
      x, and
```

```
       <new image location> is the location to where the image should be copied
       to the backup device.
```

21. After the image is copied to both the primary and the backup devices, access the **Remote Console** option of the primary device from CSO.

22. Log in to the backup device from the primary device:

```
primary:node0}
user@node0> request routing-engine login node 1
```

23. On the backup device, issue the upgrade command **request system software add /var/tmp/*image-name* no-validate**.

```
{backup:node1}
user@node1> request system software add
/var/tmp/<junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

```
Host OS upgrade staged. Reboot the system to complete installation!


WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software delete junos'
WARNING:     command as soon as this operation completes.


WARNING:     The DHCP configuration command used will be deprecated in future
 Junos releases.
WARNING:     Please see documentation for updated commands.

Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

24. After the image on the backup device is upgraded successfully, open another remote console on the primary device and upgrade the image on the primary device.

```
{primary:node0}
user@node0> request system software add
/var/tmp/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

```
Host OS upgrade staged. Reboot the system to complete installation!


WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software delete junos'
WARNING:     command as soon as this operation completes.


WARNING:     The DHCP configuration command used will be deprecated in future
 Junos releases.
WARNING:     Please see documentation for updated commands.

Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

25. Reboot the backup device.

```
{backup:node1}
root@node1> request system reboot
Reboot the system ? [yes,no] (no)yes
```

26. Immediately open another remote console and reboot the primary device.

```
{primary:node0}
root@node0> request system reboot
Reboot the system ? [yes,no] (no)yes
```

27. After both the devices are up, redeploy the srx-rouser template on the primary device by disabling the **Admin** option.

Bug Tracking Number: CXU-50068

- When you edit an enterprise hub site by adding a WAN link, static tunnels are not established with connected spoke sites automatically.

Workaround: Reconfigure the static tunnels with connected spoke sites manually.

Bug Tracking Number: CXU-44427

SD-LAN

- CSO is unable to configure access ports on the EX4600 and EX4650 devices after you zeroize the device because a default VLAN is configured on all the ports after zeroizing.

  Workaround: Load the factory-default configuration if you zeorize the EX4600 and EX4650 devices or delete the default VLAN configuration from all the ports of the members by using commands such as **# wildcard range delete interfaces xe-0/0/[0-23]**.

  Bug Tracking Number: CXU-42865

- When adding a switch to an already provisioned site, the site state is set to Provisioned in CSO. Therefore, a link to copy the stage-1 configuration for manually activating the EX Series device does not appear. You must set the state of a site to Provisioned only when all the devices in the site are provisioned.

  Workaround: Delete the device from CSO and add the device again after rectifying the reason for provision failure.

  Bug Tracking Number: CXU-40647

- ZTP of an EX Series switch fails if you add the switch behind an enterprise hub.

  Workaround: For onboarding an EX Series switch behind an enterprise hub, manually configure the stage-1 configuration on the switch.

  Bug Tracking Number: CXU-38994

- While configuring an SD-WAN site with an EX switch, the VLAN value that you enter for a LAN segment is not saved if you enable CPE ports in the LAN segment.

  Workaround: Reenter the VLAN value after you add the CPE ports to the LAN segment.

  Bug Tracking Number: CXU-45943

- The chassis view of an EX Series Virtual Chassis may not reflect the correct status of the Virtual Chassis Ports (VCP).

  Workaround: There is no known workaround.

- When you select all VLANs for deletion and if any of the selected VLAN is connected to a CPE port, the VLANs are not deleted. An error message appears and a job to delete the VLANs is created in CSO. The jobs appears successful and the status of the VLANs appear as Delete Pending.

Workaround: When VLANS are selected for deletion and if any of the VLANS are connected to a CPE port, remove the VLAN configuration from the CPE port and then delete the VLAN.

- When you reboot an EX Series switch that is configured behind a CPE, the EX Series switch is unable to connect back to CSO as it does not get the DHCP information from the CPE.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-47062

Next-Generation Firewall

- Upgrade of a next-generation firewall from CSO Release 5.2.0 to CSO Release 5.3.0 fails when SSL policies are deployed in the firewall.

  Workaround: Deploy SSL policies after the upgrading the firewall from CSO Release 5.2.0 to CSO Release 5.3.0.

  Bug Tracking Number: CXU-50316

Security Management

- 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

General

- If you click a specific application on the Resources > Sites Management > WAN tab > Top applications widget, the Link Performance widget does not display any data.

  Workaround: You can view the data from the Monitoring >Application Visibility page or Monitoring >Traffic Logs page.

  Bug Tracking Number: CXU-39167

- After Network Address Translation (NAT), only one DVPN tunnel is created between two spoke sites if the WAN interfaces (with link type as Internet) of one of the spoke site have the same public IP address.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-41210

- 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

- The Users page continues to display the name of the user that you deleted. This is because the Users page is not automatically refreshed.

  Workaround: Manually refresh the page.

  Bug Tracking Number: CXU-41793

- After ZTP of an NFX Series device, the status of some tunnels are displayed as down. This issue occurs if you are using the subnet IP address192.168.2.0 on WAN links, which causes an internal IP address conflict.

  Workaround: Avoid using the 192.168.2.0 subnet on WAN links.

  Bug Tracking Number: CXU-41511

- In the CSO GUI, in the LAN tab of a next-generation firewall site with a LAN switch, when you click the arrow icon next to a LAN segment, the ports displayed in the Switch Ports field disappear.

  Workaround: Hover over the ***+number of ports*** link in the Switch Ports column to view the list of ports on the LAN.

  Bug Tracking Number: CXU-42608

- Installation of licenses on SRX1500 and SRX4200 dual CPE clusters by using CSO is failing.

  Workaround: Install the licenses manually. To install the licenses manually:

  1. Copy the license files for both the devices to the primary node of the cluster.

  2. Install the license on the primary device.

     ```
     root@node0>request system license add /var/tmp/<node0-license-file.txt>
     ```

  3. Copy the license file of the backup node to the backup node.

     ```
     root@node0>file copy /var/tmp/<node1-license-file.txt>
     ```

  4. Log in to the backup node and install the license.

     ```
     root@node1>request system license add /var/tmp/<node1-license-file.txt>
     ```

  Bug Tracking Number: CXU-40522

- Image upgrade on an SRX4*X*00 Series cluster fails as the ISSU upgrade command throws an error due to real-time performance monitoring (RPM) configuration.

  Workaround: To upgrade an SRX4*X*00 Series cluster:

  1. Log in to CSO Customer Portal and apply the *srx-rouser* configuration template on the primary device in the cluster.

  2. Deploy the configuration template on the primary device by enabling the **Admin** option for the device.

  3. Copy the image to be upgraded on to both the primary and the backup devices by using CSO or manually.

  4. After the image is copied on both the primary and the backup devices, access the **Remote Console** option for the device from CSO.

  5. Log in to the backup device from the primary device:

     ```
     primary:node0}
     user@node0> request routing-engine login node 1
     ```

  6. On the backup device, issue the upgrade command **request system software add /var/tmp/<*image-name*> no-validate**.

     ```
     {backup:node1}
     user@node1> request system software add
     /var/tmp/<junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
     ```

     ```
     Host OS upgrade staged. Reboot the system to complete installation!


     WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
     WARNING:     'request system reboot' command when software installation is
     WARNING:     complete. To abort the installation, do not reboot your system,
     WARNING:     instead use the 'request system software delete junos'
     WARNING:     command as soon as this operation completes.


     WARNING:     The DHCP configuration command used will be deprecated in future
      Junos releases.
     WARNING:     Please see documentation for updated commands.
     ```

```
Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

7. After the image on the backup device is upgraded successfully, open another remote console on the primary device and upgrade the image on the primary device.

```
{primary:node0}
user@node0> request system software add
/var/tmp/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

```
Host OS upgrade staged. Reboot the system to complete installation!


WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software delete junos'
WARNING:     command as soon as this operation completes.


WARNING:     The DHCP configuration command used will be deprecated in future
 Junos releases.
WARNING:     Please see documentation for updated commands.

Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

8. Reboot the backup device.

```
{backup:node1}
root@node1> request system reboot
Reboot the system ? [yes,no] (no)yes
```

9. Immediately open another remote console and reboot the primary device.

```
{primary:node0}
root@node0> request system reboot
Reboot the system ? [yes,no] (no)yes
```

10. After both the devices are up, redeploy the srx-rouser template on the primary device by disabling the **Admin** option.

The image is now upgraded on both the devices of the cluster.

Bug Tracking Number: CXU-39491

- Link metric widgets do not show data as expected when an analytics node is down.

  Workaround: Bring up the analytics node to view link metric widgets correctly.

  Bug Tracking Number: CXU-30813

- When you install the license on the backup node of an SRX dual CPE cluster, the installation fails.

  Workaround: To install license on the backup node of an SRX dual CPE cluster by using CSO:

  1. Install license on the primary node by using CSO
  2. Reboot the primary node to switch the backup node to function as the primary node.
  3. After the backup node becomes the primary node, install license for the backup node (currently working as the primary node) by using CSO.

  Bug Tracking Number: CXU-43085

- While you deploy the VRRP configuration templates on a SRX Series or EX Series devices, the template does not render as expected on the Devices page of the CSO GUI.

  Workaround: Edit and save the VRRP configuration template without making any changes for the VRRP template to render correctly on the CSO GUI for SRX Series and EX Series devices.

- CSO does not support cluster-level Return Material Authorization (RMA) for SRX Series dual CPE devices. Only cluster node-level RMA is supported.

  Workaround: There is no known workaround.

  Bug Tracking Number: CXU-32157

- ZTP with phone-home client does not work if PPPoE is enabled on the OAM link with xDSL or Ethernet interfaces.

  Workaround: Copy the Stage-1 configuration to the device to connect the device to CSO and provision the device.

Bug Tracking Number: CXU-50427

- Deleting an SRX345 dual CPE is failing. However, the site related to the SRX345 device is deleted from the CSO GUI.

  Workaround: There is no known workaround.

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.3.0:

- You cannot filter the ports for SRX Series devices while adding an on-premises spoke site or while adding a switch.

  Bug Tracking Number: CXU-32826

- The Install Signature page does not reflect the correct OS version for a spoke site after the image on the device is upgraded.

  Bug Tracking Number: CXU-36373

- The deployment of a port profile fails if the values you have configured for the firewall filter are not supported on the device running Junos OS.

  Bug Tracking Number: CXU-39629

- When DVPN tunnels (GRE_IPSEC tunnels) are established between a pair of SRX300 Line devices that have Internet WAN links behind NAT, the GRE OAM status of the tunnels is displayed as DOWN and hence the tunnels are marked as DOWN and not usable for traffic.

  Bug Tracking Number: CXU-41281

- While you are using a remote console for a tenant device, if you press the Up arrow or the Down arrow on the keyboard, then instead of the command history, irrelevant text (that includes the device name and the tenant name) appears on the console.

  Bug Tracking Number: CXU-41666

- The chassis view for an EX2300 Virtual Chassis appears blank when the device resources are used up and the request for getting a response from the device times out.

  Bug Tracking Number: CXU-42866

- Provisioning an SRX340 device as a next-generation firewall by using CSO is failing when Junos OS Release 19.3R2 is installed on the device.

  Bug Tracking Number: CXU-43362

- On devices running Junos Release OS 19.3R2-S2, the SLA reason field (Actual Delay, Expected Delay, Jitter, Loss) for a Link Switch event is missing in the WAN tab of the Site Management page.

  Bug Tracking Number: CXU-43653

- RFC-1918 subnets cannot be used in LAN subnets and LAN segments.

  Bug Tracking Number: CXU-44158

- The chassis view of an EX Series Virtual Chassis may not reflect the correct status of the Virtual Chassis ports (VCPs).

  Bug Tracking Number: CXU-44880

- When you select all VLANs for deletion and if one or more of the selected VLANs is connected to a CPE port, the VLANs are not deleted. An error message appears and a job to delete the VLANs is created in CSO. The jobs appear to be successful and the status of the VLANs appear as Delete Pending.

  Bug Tracking Number: CXU-44966

- When CSO is upgraded to Release 5.2.0, there are 15 LAN ports in the SRX1500 dual CPE device template, when the actual number of LAN ports should be four.

  Bug Tracking Number: CXU-45889

- ZTP fails on SRX345 and vSRX due to issues with loading default certificates.

  Bug Tracking Number: CXU-45904

- You cannot edit a standalone SD-LAN site although the Edit Site button is enabled.

  Bug Tracking Number: CXU-45918

- When you clone a site template containing a next-generation firewall and a switch, you may not be able to edit some of the fields in the cloned template.

  Bug Tracking Number: CXU-45919

- On the Site Management page for an OpCo, the operational status of a provider hub is displayed as N/A when the status is actually up.

  Bug Tracking Number: CXU-45924

- While you deploy the VRRP configuration template on an SRX Series or EX Series device, the template does not render as expected on the Devices page of the CSO GUI.

  Bug Tracking Number: CXU-46049

- The infotip for the ADSL_ENCAP parameter in the SRX as SDWAN CPE device profile incorrectly indicates the encapsulation used to connect to the ADSL service provider through PPPoE. The ADSL_ENCAP parameter does not apply to PPPoE, but to PPPoA.

  Bug Tracking Number: CXU-46189

- CSO may not detect an EX Series switch connected behind an SRX Series device running Junos OS Release 19.3R2-S1 or Release 19.3R2-S2. This is because the port connecting the EX Series switch and

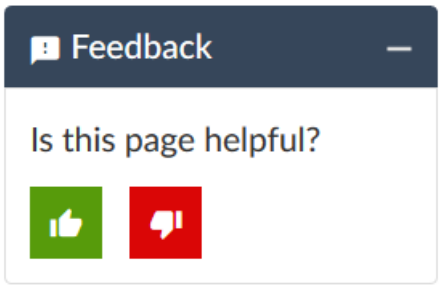
the CPE is blocked by RSTP running on the SRX Series device and hence no IP address is assigned by DHCP to the port.

Bug Tracking Number: CXU-46760

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

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit 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/
- 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/.

Revision History

Oct 8, 2020—Revision 5, Added support for Junos OS Release 19.3R2-S4.

Sept 22, 2020—Revision 4, Updated the description for CXU-40522 to include SRX1500

Sept 9, 2020—Revision 3, Incorporated editorial feedback.

August 4, 2020—Revision 2, Added SRX1500 and SRX4000 line of devices supported for spoke and provider hub. Also, addded CXU-50068, CXU-50427, CXU-50316, and CXU-50112 to the list of known issues and known behavior.

July 24, 2020—Revision 1, CSO Release 5.3.0