

Contrail Service Orchestration Release Notes

Release 5.1.1
April 7, 2020
Revision 4

These Release Notes accompany Release 5.1.1 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 | 3

Software Support | 4

Software Downloads | 4

Software Installation Requirements for NFX Series Network Services Platform | 11

New and Changed Features in Contrail Service Orchestration Release 5.1.1 | 12

Install and Upgrade | 12

SD-WAN | 13

SD-LAN | 14

Miscellaneous | 14

Deprecated Features | 15

VNFs Supported | 15

Licensing | 16

Accessing the CSO GUIs | 17

Known Behavior | 17

Install and Upgrade | 18

Device Management | 19

Dynamic VPN (DVPN) | 20

Policy Deployment | 20

SD-WAN | 21

SD-LAN | 21

Security Management | 22

Site and Tenant Workflow	22
Topology	23
User Interface	23
General	24
Known Issues	25
SD-WAN	25
SD-LAN	26
CSO High Availability	27
Security Management	28
Site and Tenant Workflow	29
General	29
Resolved Issues	35
Documentation Feedback	35
Requesting Technical Support	36
Self-Help Online Tools and Resources	36
Creating a Service Request with JTAC	37
Revision History	37

Introduction

You can deploy CSO Release 5.1.1 on-premises or use it as a cloud-based service.

CSO Release 5.1.1 supports the following types of accounts:

- Service provider accounts—Service provider administrators can add tenants to and enable services such as SD-WAN, LAN, and next-generation firewall for the service provider network. They can also manage profiles and policies for traffic, configure service-level agreement (SLA) policies, breakout policies, and firewall management.

NOTE: When offered as a cloud-based service, CSO does not support the Service Provider administrator role.

- 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 5.1.1:

- **Install and Upgrade**

- Support for ESXi hypervisors
- Supported path for upgrade from CSO Release 4.1.1 to CSO Release 5.1.1

- **SD-WAN features**

- Support for full mesh on all WAN links of enterprise hubs
- Support for full mesh on all WAN links of dual CPE spoke sites
- Support for advertising LAN prefix
- Support for multiple WAN links on the same physical interface for enterprise hub sites
- Support for SRX1500 as a spoke, a provider hub, or an enterprise hub

- **SD-LAN features**

- Support for adding multiple EX Series switches

- Support for preprovisioning an EX Series Virtual Chassis
- Assigning port profiles to an EX Series Switch while onboarding
- **Miscellaneous**
 - Support for ZTP on copper ports
 - Support for autogenerating e-mails for SD-LAN and SD-WAN alarms
 - Support for LAG templates

Software Support

IN THIS SECTION

- [Software Downloads | 4](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 11](#)

Software Downloads

[Table 1 on page 4](#) displays the supported versions and download links for software components associated with CSO Release 5.1.1.

NOTE:

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.
- CSO Release 5.1.1 extends Beta support for Junos OS Release 19.3R2-S1.

Table 1: Software Components Associated with CSO Release 5.1.1

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 5.1.1 (continued)

Product	Supported Version	Download Link
EX Series switches	Junos OS Release 18.4R2	Junos OS Release 18.4R2
	Junos OS Release 18.4R3	<ul style="list-style-type: none"> • EX2300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300 • EX3400: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300 • EX4300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93859.html?pf=EX4300 • EX4600: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93861.html?pf=EX4600 • EX4650: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93900.html?pf=EX4650 <p>Junos OS Release 18.4R3</p> <ul style="list-style-type: none"> • EX2300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101422.html?pf=EX2300 • EX3400: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101422.html?pf=EX3400 • EX4300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101391.html?pf=EX4300 • EX4600: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101393.html?pf=EX4600 • EX4650: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101432.html?pf=EX4650

Table 1: Software Components Associated with CSO Release 5.1.1 (continued)

Product	Supported Version	Download Link
NFX150 CPE device	Junos OS Release 18.2X85-D12 Junos OS Release 19.3R2-S1	<ul style="list-style-type: none"> Junos OS 18.2X85-D12 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94797.html Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94794.html Junos OS 19.3R2-S1 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103935.html?pf=NFX150 Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103865.html?pf=NFX150
NFX250 CPE device	Junos OS Release 15.1X53-D497 Junos OS Release 18.4R3	<ul style="list-style-type: none"> Junos OS Release 15.1X53-D497 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92335.html Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92333.html Junos OS Release 18.4R3 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101464.html?pf=NFX250 Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101399.html?pf=NFX250
SRX Series CPE devices	Junos OS Release 15.1X49-D172 Junos OS Release 19.3R2-S1	SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices): <ul style="list-style-type: none"> Junos OS 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92321.html Junos OS 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103890.html?pf=SRX300

Table 1: Software Components Associated with CSO Release 5.1.1 (continued)

Product	Supported Version	Download Link
SRX Series Next-Generation Firewall devices	Junos OS Release 18.4R1	SRX300, SRX320, SRX340, SRX345, and SRX550:
	Junos OS Release 19.3R2-S1	<ul style="list-style-type: none"> Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/85904.html?pf=SRX300 Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103890.html?pf=SRX300
SRX Series Provider Hub device	Junos OS Release 15.1X49-D172	SRX1500 <ul style="list-style-type: none"> Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html Junos OS Release 15.1X49-D172 (USB) : https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html Junos OS Release 15.1X49-D172 (PXE): : https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html SRX4100, SRX4200: <ul style="list-style-type: none"> Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html Junos OS Release 15.1X49-D172 (USB): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html Junos OS Release 15.1X49-D172 (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html

Table 1: Software Components Associated with CSO Release 5.1.1 (continued)

Product	Supported Version	Download Link
SRX Series Enterprise Hub devices	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> SRX4100, SRX4200: <ul style="list-style-type: none"> Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html Junos OS Release 15.1X49-D172 (USB): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html Junos OS Release 15.1X49-D172 (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html Junos OS Release 19.3R2-S1 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103891.html?pf=SRX4100 Junos OS Release 19.3R2-S1 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103919.html?pf=SRX4100 SRX1500: <ul style="list-style-type: none"> Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html Junos OS Release 15.1X49-D172 (USB): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html Junos OS Release 15.1X49-D172 (PXE): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html Junos OS Release 19.3R2-S1 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103889.html?pf=SRX1500 Junos OS Release 19.3R2-S1 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103918.html?pf=SRX1500
	Junos OS Release 19.3R2-S1	

Table 1: Software Components Associated with CSO Release 5.1.1 (continued)

Product	Supported Version	Download Link
vSRX for SD-WAN devices	<p>Junos OS Release 15.1X49-D172</p> <p>Junos OS Release 19.3R2-S1</p>	<p>For hub devices and spoke devices:</p> <ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92328.html • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103996.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92331.html • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104008.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92332.html • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104007.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92330.html • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104010.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 15.1X49-D172: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92329.html • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104009.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.1.1 (continued)

Product	Supported Version	Download Link
vSRX for next-generation firewall devices	Junos OS Release 18.4R1 Junos OS Release 19.3R2-S1	<ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86039.html?pf=vSRX • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/103996.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86042.html?pf=vSRX • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104008.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86041.html?pf=vSRX • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104007.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86044.html?pf=vSRX • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104010.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 18.4R1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86043.html?pf=vSRX • Junos OS Release 19.3R2-S1: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/104009.html?pf=vSRX

We recommend that you use Junos OS Release 15.1X49-D172 in your production environment instead of Junos OS Release 19.3R2-S1 because of the following known limitations in Junos OS Release 19.3R2-S1:

- Connection fails when traffic is sent through an NFX250 device on which vSRX is installed. [PR 1483425]
- In an SRX3xx dual CPE cluster, ZTP does not progress if the secure OAM tunnel from the primary node is down. [PR 1484382, PR 1484389]
- Sometimes, vSRX when running on an NFX250 device does not show the ge- interfaces after you upgrade the image from Junos OS Release 15.1X49-D172.1 to Junos OS Release 19.3R2-S1. [PR 1482360]
- In an SRX1500 dual-CPE cluster, you cannot add a license to the backup node by using the **request system license add** command. [PR 1485128]
- GRE interface in an NFX150 device may appear as down, even though it is actually up. [PR 1456184]
- Zero-touch provisioning (ZTP) of a device running Junos OS Release 19.3R2-S1 may fail due to failure in installing the default-trusted certificate authority (CA). [PR 1472607]
- Full mesh dynamic VPN tunnel formed through a device running Junos OS 19.3R2-S1 may not come up. [PR 1482984]
- LAN traffic may be interrupted while configuring a full mesh DVPN tunnel on a device running Junos OS Release 19.3R2-S1. [PR 1484083]
- During ZTP of an SRX1500 dual CPE cluster, the devices in the cluster reboot automatically. [PR 1484257]

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: Only an SP administrator can upload the software image to CSO. 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 5.1.1

IN THIS SECTION

- [Install and Upgrade | 12](#)
- [SD-WAN | 13](#)
- [SD-LAN | 14](#)
- [Miscellaneous | 14](#)

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.1.1.

You can view and read the features that are available in the CSO Release 5.1.0 through the following link:

- [CSO 5.1.0 Release Notes](#)

Install and Upgrade

- **Support for ESXi**—CSO Release 5.1.0 supports only the KVM hypervisor, whereas CSO Release 5.1.1 supports KVM and ESXi version 6.7 hypervisors.
- **Supported path for upgrade from CSO Release 4.1.1 to CSO Release 5.1.1**—The only supported upgrade path is from CSO Release 4.1.1 with *medium* deployment to CSO Release 5.1.1 with *HA* deployment. For details, see the *Install and Upgrade guide*.
- **Disk space required for upgrade from CSO Release 5.1.0 to CSO Release 5.1.1**—You must have at least 40 GB disk space on the *startupserver* VM to run the `upgrade.sh` script. For details, see the *Install and Upgrade guide*.

SD-WAN

- **Support for full mesh on all WAN links of enterprise hubs and dual CPE Spoke sites**—From CSO Release 5.1.1 onward, you can enable full mesh and configure mesh tags on up to four WAN links of an enterprise hub and dual CPE spoke sites. In releases before CSO Release 5.1.1, you can configure a maximum of three WAN links for meshing.
- **Support for advertising LAN prefixes**—From CSO Release 5.1.1 onward, you can advertise the LAN prefixes of SD-WAN spoke sites to the data center through the data center department associated with the enterprise hub. This feature is applicable to dynamically routed LAN segments on the data center department and is disabled by default.

If you disable advertising LAN prefixes of SD-WAN spoke sites, LAN routes are not advertised to the neighbor. In such cases, you must configure source NAT on the enterprise hub from the CSO UI or configure reverse routes on the routing device.

NOTE: You must avoid overlapping IP addresses between the SD-WAN LAN network and the data center network.

- **Support for multiple WAN links on the same physical interface for enterprise hub sites**—From CSO Release 5.1.1 onward, for enterprise hub sites, you can configure more than one WAN link on the same physical interface. The WAN links are connected from the same physical interface to the provider edge (PE) nodes through logical subinterfaces with VLAN separation.
- **Support for SRX1500 as a spoke, a provider hub, or an enterprise hub**—From CSO Release 5.1.1 onward, you can configure an SRX1500 device as a spoke, a provider hub, or an enterprise hub in SD-WAN deployments. You can use the SRX1500 device as a single CPE or dual CPE cluster in the SD-WAN deployments.

NOTE:

- SRX1500 devices must run Junos OS Release 19.3R2-S1 (Beta version) to be configured as a spoke or enterprise hub.
- In CSO Release 5.1.1, LTE and DSL links are not supported for SRX1500 devices.

SD-LAN

- **Support for adding multiple EX Series switches**—From CSO Release 5.1.1 onward, you can add one or more EX Series switches to an existing SD-LAN site. Both physical, standalone EX Series switches and EX Series Virtual Chassis are supported.

NOTE: To configure more than one switch with an SD-WAN CPE or a next-generation firewall, add an SD-LAN logical site and add multiple switches to the site. You can manage the connectivity and configuration between the switches and the CPE or next-generation firewall either by using configuration templates or manually.

- **Support for preprovisioning an EX Series Virtual Chassis**—From CSO Release 5.1.1 onward, you can preprovision an EX2300, EX3400, EX4300, EX4600, and EX4650 Virtual Chassis. This means that while adding an SD-LAN site, you can configure a Virtual Chassis by specifying the primary, backup, and linecard members of the Virtual Chassis in the site creation workflow.

The members of the Virtual Chassis must be of the same device type, with the same device models or different device models.

NOTE: Mixed-mode Virtual Chassis, that is, members of different device types, is not supported in this release. For example, the members of the Virtual Chassis cannot be a combination of EX4300 and EX4600 or EX4650 devices.

- **Assigning port profiles to an EX Series Switch while onboarding**—From CSO Release 5.1.1 onward, you can assign port profiles to a switch while onboarding the switch to CSO. By assigning port profiles while onboarding the switch, you can provision the switch and configure the switch ports in a single operation.

Miscellaneous

- **Support for ZTP on copper ports**—From CSO Release 5.1.1 onward, the factory-default settings on NFX Series devices enable you to use cost-effective copper ports (10/100/1000BASE-T) as WAN ports and to perform zero-touch provisioning (ZTP) of the devices.

In CSO releases before Release 5.1.1, you can use only SFP ports as the factory-default WAN ports and to perform ZTP.

- For NFX150 devices (with platform image 19.3R2 and later), the factory-default WAN ports are the first copper port and last SFP port. You can use these ports to perform ZTP.

- For NFX250 devices, you can use any of the ports on the front panel to perform ZTP.
- **Support for autogenerating e-mails for SD-LAN and SD-WAN alarms**—From CSO Release 5.1.1 onward, SP administrators, OpCo administrators, and tenant administrators can enable e-mail notifications and specify the recipients to be notified if there are SD-LAN and SD-WAN alarms.
- **Support for LAG templates**—From CSO Release 5.1.1 onward, you can configure a link aggregation group (LAG) on an EX Series switch by using the following configuration templates:
 - MC-LAG: Template for configuring a multichassis link aggregation group (MC-LAG) on an MC-LAG peer device.
 - LAG-EX-Trunk: Template for configuring a link aggregation group (LAG) on a switch when the switch is operating in trunk mode.

Deprecated Features

This section describes the features that are deprecated or for which support is withdrawn from CSO Release 5.1.1.

- Starting from CSO Release 5.1.1 onward, you cannot use CSO to configure an MX Series device as a provider hub.

VNFs Supported

CSO supports the VNFs listed in [Table 2 on page 16](#).

Table 2: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX	For Hybrid WAN and SD-WAN deployments: vSRX KVM Appliance 15.1X49-D172	<ul style="list-style-type: none"> • Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM) 	Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.
Ubuntu	16.04		Hybrid WAN and SD-WAN (all LAN-side functions) deployments–NFX250 and NFX150 platforms.
Fortinet	5.6.3		Hybrid WAN and 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 to access the CSO GUIs.

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

Known Behavior

IN THIS SECTION

- [Install and Upgrade | 18](#)
- [Device Management | 19](#)
- [Dynamic VPN \(DVPN\) | 20](#)
- [Policy Deployment | 20](#)
- [SD-WAN | 21](#)
- [SD-LAN | 21](#)
- [Security Management | 22](#)
- [Site and Tenant Workflow | 22](#)
- [Topology | 23](#)
- [User Interface | 23](#)
- [General | 24](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.1.1.

Install and Upgrade

- After upgrading from CSO Release 4.1.1 to CSO Release 5.1.1, you must modify the IP address of the virtual route reflector (VRR) configuration.

To modify the IP address of the VRR, connect to VRR-1 VM and change the public IP address of VRR-1 to 192.168.10.29/32. Similarly, connect to VRR-2 VM and change the IP address of VRR-1 to 192.168.10.30/32.

- While upgrading from CSO Release 5.0.x to CSO Release 5.1.1, the upgrade of a site with NFX250 device may fail due to connectivity issues.

NOTE: To use the CPE behind NAT and multi-service shared bearer (MSSB) features, you must upgrade sites configured in the earlier releases of CSO as follows:

- When upgrading from CSO Release 5.0.x to CSO Release 5.1.1, any site with OAM or OAM-DATA hub must also be upgraded to CSO Release 5.1.1. Upgrade of enterprise hubs, data hubs, and spoke sites to CSO Release 5.1.1 is optional.
- When upgrading from CSO Release 5.1.0 to CSO Release 5.1.1, upgrade of sites (both hub and spoke) to CSO Release 5.1.1 is optional.
- When upgrading from CSO Release 4.1.1 to CSO Release 5.1.1, any site with OAM or OAM-DATA hub must also be upgraded to CSO Release 5.1.1. Upgrade of enterprise hubs, data hubs, and spoke sites to CSO Release 5.1.1 is optional.

- While upgrading from CSO Release 4.1.1 to CSO Release 5.1.1, to avoid issues because of user or group permissions, you must run the following commands on all the infrastructure nodes to back up Elasticsearch data:

```
service elasticsearch stop
usermod -u 2001 elasticsearch
groupmod -g 2001 elasticsearch
chown -R elasticsearch:elasticsearch /var/log/elasticsearch
chown -R elasticsearch:elasticsearch /usr/share/elasticsearch/
chown -R elasticsearch:elasticsearch /var/lib/elasticsearch
chown -R elasticsearch:elasticsearch /mnt/data/elasticsearch
chown -R elasticsearch:elasticsearch /home/elasticsearch
chown -R root:elasticsearch /etc/elasticsearch
service elasticsearch restart
```

- After you upgrade to CSO Release 5.1.1, you must change the **etcd** values of the hostname and IP address of the south-bound load balancer (SBLB) host to match the values in CSO Release 4.1.1 to maintain the same connections between the nodes as in CSO Release 4.1.1.

To update the **etcd** values, execute the following commands in the startup server:

1. **kubectl exec -it etcd-etcd-0 bash -n infra**
 2. **etcdctl set /csp/infra/fmpmlb/host <virtual IP address of SBLB in CSO Release 4.1.1>**
 3. **etcdctl set /telemetryconverter/virtualhostname ""{"regional": "SBLB hostname in CSO Release 4.1.1", "central": ""}"**
- While you upgrade from CSO Release 4.1.1 to CSO Release 5.1.1, MariaDB might fail to restore at the first attempt. MariaDB is restored successfully in the next attempt.

Device Management

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

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.
- DVPN is not supported for cloud spoke sites.

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.
- You must not start the Custom Application Signature name or Custom Application Signature Group name with the keyword Junos. This keyword is reserved for only predefined applications.

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 WAN tab of the *Site-Name* page, the link metrics graph displays aggregated data. Therefore, in cases where the aggregation interval overlaps between source and destination link data, the link metrics graph displays incorrect data.
- 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).
- When an SD-WAN policy is deployed and a high rate of traffic flows through the CPE device, this might lead to network congestion and introduce delays or cause traffic loss. However, even though an SLA violation is reported, the traffic does not switch to a different link.
- In device redundancy mode, when you reboot a node, the device fails to generate a few system logs. Because a few system logs are not generated, the link switch event in CSO displays the same interface as the source interface and the destination interface.
- Sometimes duplicate link switch events are displayed on the Link Switch Events page.
- You cannot use an NFX150 dual CPE device for deploying SD-WAN services.

SD-LAN

- Overlapping LAN segments are not supported within a tenant network.
- PHC is supported for EX2300, EX3400, and EX4300 Series switches (except EX4300-MP) with only Junos OS Release 18.4R2 and later. CSO Release is qualified for Junos OS Release 18.3R1, and the PHC capability is currently not supported for EX switches that are onboarded with Junos OS release 18.3R1.

If the PHC capability is not supported for EX switches, you must manually copy the stage-1 configuration from the CSO portal and paste it to the device console to commit the stage-1 configuration when you create a LAN site or activate an EX series switch.

- Do not zeroize EX2300 and EX3400 devices as doing so might result in unexpected behavior.
- 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.

Security Management

- UTM Web filtering is not supported in an active-active SRX Series cluster device.
- Performance of SSL proxy may not be as expected on SRX300 and SRX320 devices.

Site and Tenant Workflow

- When tenants are created, ensure that the tenant name is unique across the CSO instance; that is, the same tenant name should not be there in any of the OpCo networks on the CSO instance.
- 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*

Topology

- DHCP configuration on WAN links on a SD-WAN hub is not supported.

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
11oOYS6n9l0WDZcxXYWWeINlu6zOSilZYVIdwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

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

General

- While deploying CSO, only one Redis server will be running on a pod. The Redis server automatically restarts if you restart or terminate the pod.
- If you choose to purge the audit log with the **Archive and Store in Local Location** option selected, you need to contact Juniper Networks for accessing the locally archived audit logs. We recommend that you use the **Archive and Store in Remote Location** option for easy access to archived logs. When you run an audit log purge with the **Archive and Store in a Remote Location** option selected, ensure that the remote server where you want to archive the purged audit logs is reachable from CSO.
- A LAN segment deploy job is handled in two parts in the following sequence:
 1. LAN segment-related policies are deployed.
 2. Firewall policies are deployed.

However, the deploy job status is updated as soon as the first part is completed. Because of this, a deploy job for a LAN segment is shown as a success even though the associated firewall policy deployment is still in progress.

- 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.
- Class-of-service (CoS) configuration on Layer 2 interfaces (*ge-0/0/port number*) is not supported on NFX150 CPE devices.
- Enterprise hub is not supported for cloud spoke sites.

Known Issues

IN THIS SECTION

- [SD-WAN | 25](#)
- [SD-LAN | 26](#)
- [CSO High Availability | 27](#)
- [Security Management | 28](#)
- [Site and Tenant Workflow | 29](#)
- [General | 29](#)

This section lists known issues in Juniper Networks CSO Release 5.1.1.

SD-WAN

- On an enterprise hub, when there are no non-data center departments, the SD-WAN policy deploy job may return the following message and fail:

No update of SD-WAN policy configuration on device due to missing required information.

Workaround: There is no functional impact; the deploy job completes successfully when a non-data center department with a LAN segment is deployed on an enterprise hub.

Bug Tracking Number: CXU-31365

- If the Internet breakout WAN link of the provider hub is not used for provisioning the overlay tunnel by at least one spoke site in a tenant, then traffic from sites to the Internet is dropped.

Workaround: Ensure that you configure a firewall policy to allow traffic from security zone *trust-tenant-name* to zone *untrust-wan-link*, where *tenant-name* is the name of the tenant and *wan-link* is the name of the Internet breakout WAN link.

- Bug Tracking Number: CXU-21291
- While provisioning a dual CPE SRX Series cluster as an enterprise hub with the multi-access shared bearer (MASB) configuration, the stage-1 configuration fails to commit because untagged logical interfaces are not supported on the device interface when MASB is configured.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-42201

SD-LAN

- The phone-home process might not be triggered if you zeroize an EX Series switch and commit the configuration manually on the switch.

Workaround: To trigger the phone-home process, run the **delete chassis auto-image-upgrade** command and commit the delete operation.

Bug Tracking Number: CXU-39129

- 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.

Workaround:

- Edit the firewall filter.
- Update the values according to the supported configuration specified for a firewall filter, in this [link](#).
- Redeploy the port profile.

Bug Tracking Number: CXU-39629

- 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 zeroize 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

- 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.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-42866

- In an on-premises installation, when deploying a port profile configuration fails on an EX4650 switch, CSO displays the management status of the site with EX4650 switch as provisioned even though the ZTP job fails on the switch.

Workaround: Ensure that no port profile is deployed on an EX4650 switch during ZTP.

Bug Tracking Number: CXU-42181

- 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

CSO High Availability

- In an HA setup, deployment of NAT and firewall policies fail if secmgt-sm pods fail to initialize after a snapshot process and remain in 0/1 Running state.

Workaround: Run the following curl command from the microservices VM and make sure scemgt-sm pods comes to 1/1 Running state:

curl -XPOST "https://<central-vip>/api/juniper/sd/csp-web/database-initialize" -H 'Content-Type: application/json' -H 'Accept: application/json' -H "X-Auth-Token: token"

Bug Tracking Number: CXU-31446

- In an HA installation, during infrastructure deployment, sometimes services inside the Contrail Analytics Node remain in the initializing state. Because of this, the Contrail Analytics Node cannot be configured and the infrastructure deployment fails.

Workaround: There is no known workaround. You must delete all the virtual machines spawned and start the deployment again from scratch.

Bug Tracking Number: CXU-42965

- In an HA setup, in case of power failure scenarios, certain workflows, such as onboard tenant or configure site, may fail randomly with ReadTimeout Error.

Workaround: Contact JTAC for the recovery procedure.

Bug Tracking Number: CXU-43001

- 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

- After you restart all the three infrastructure nodes, MariaDB is not restored properly.

Workaround: Execute the **recovery.sh** on the startup server and select the **MariaDB** option to restore MariaDB completely.

```
root@startupserver:/opt/cso/Contrail_Service_Orchestration_5.1.1# ./recovery.sh
```

Bug Tracking Number: CXU-42125

- In an high availability installation of CSO, when a server is restarted, the node on which RabbitMQ is running does not join the cluster.

Workaround: Execute the **recovery.sh** script on the startup server and select the **RabbitMQ** option to recover the RabbitMQ cluster and restart microservices.

Bug Tracking Number: CXU-43726

- After restarting the etcd pod, the pod does not return to the running state. Instead the pod is in the crashloopbackoff state.

Workaround: Contact JTAC for getting the etcd pod to the running state.

Bug Tracking Number: CXU-38345

Security Management

- 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

- 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

- If SSL proxy is configured on a dual CPE device and if the traffic path is changed from one node to another node, the following issue occurs:

- For cacheable applications, if there is no cache entry the first session might fail to establish.
- For non-cacheable applications, the traffic flow is impacted.

Workaround: None.

Bug Tracking Number: CXU-25526

Site and Tenant Workflow

- On a site with an NFX250 device and EX Series switch, the EX Series switch is not detected if there are no LAN segments.

Workaround: Onboard the site with at least one LAN segment.

Bug Tracking Number: CXU-38960

- When you perform ZTP on more than one enterprise hub at the same time, ZTP for one or the other enterprise hub may fail.

Workaround: Perform ZTP on enterprise hubs one after the other; that is, after the ZTP of the first enterprise hub completes successfully. You can also retry executing the failed ZTP job.

Bug Tracking Number: CXU-42985

- When onboarding a next-generation firewall and switch, the CSO GUI may temporarily show that provisioning the firewall has failed when a license is not present, although the ZTP task completes and the site is provisioned.

Workaround: Refresh the page to view the final status of onboarding the next-generation firewall.

Bug Tracking Number: CXU-43024

General

- In next-generation firewall sites with LAN, the recall of EX2300 and EX3400 devices with the zeroize option does not work. This issue occurs because EX2300 and EX3400 do not support the zeroize option.

Workaround: Manually clean up the EX2300 and EX3400 devices.

Bug Tracking Number: CXU-35208

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32826

- UTM Web filtering fails at times even though the Enhanced Web Filtering (EWF) server is up and online.

Workaround: From the device, configure the EWF Server with the IP address 116.50.57.140 as shown in the following example:

```
root@SRX-1# set security utm feature-profile web-filtering juniper-enhanced server host 116.50.57.140
```

Bug Tracking Number: CXU-32731

- If you create or delete a DVPN tunnel, you cannot reach the LAN interface on the SRX Series device.

Workaround: Reboot the spoke or execute the following commands and then roll back the changes.

- **set groups dept-configuration interfaces ge-0/0/4 vlan-tagging**
- **set groups dept-configuration interfaces ge-0/0/5 vlan-tagging**

Bug Tracking Number: CXU-35379

- 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

- While adding a spoke site if you add and associate one or more departments with one or more LAN segments, sometimes the department's VRF tables might not be created at the enterprise hub. This causes the enterprise hub's 0/0 (default) route to be missing in the spoke site department's VRF tables.

Workaround: Delete and redeploy the LAN segments.

Bug Tracking Number: CXU-37770

- When DVPN tunnels (GRE_IPSEC tunnels) are established between a pair of SRX3XX 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.

Workaround : Disable the GRE OAM keepalive configuration to make the tunnel usable for traffic.

Bug Tracking Number: CXU-41281

- The health check in the CAN node fails while you run the **deploy.sh** script on the startup server during the HA deployment. This is because the Kafka process is inactive in one of the CAN nodes.

Workaround:

1. Log in to the CAN node.
2. Run the **docker restart analyticsdb analytics controller** command and wait for around 10 minutes.

3. Rerun the **components_health_check.sh** script on the startup server.

4. If the CAN node components are still unhealthy, repeat 2 and 3.

If all the components are healthy, then proceed with the installation.

Bug Tracking Number: CXU-41232

- Alarms are not getting generated if the date and time is not in sync with the NTP server.

Workaround: CSO and devices must be NTP-enabled. Make sure CSO and device time are in sync.

Bug Tracking Number: CXU-40815

- The firewall policy deployment fails if the system has more than 10,000 addresses.

Workaround: In the **elasticsearch.yml** file, update the **index.max_result_window** parameter to **20000**.

Bug Tracking Number: CXU-41678

- The bootstrap job for a device remains in the In Progress state for a considerable time. This is because CSO fails to receive the bootstrap completion notification from the device.

Workaround: If the bootstrap job is in the In Progress state for more than 10 minutes, add the following configuration to the device:

set system phone-home server https://redirect.juniper.net

Bug Tracking Number: CXU-35450

- 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

- In case of an AppQoE event (packet drop or latency), the application may not switch to the best available path among the available links.

Workaround: Reboot the device.

Bug Tracking Number: CXU-41922

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

Workaround. To clear the irrelevant text, press the down arrow key a few times and then press Enter.

Bug Tracking Number: CXU-41666

- While you are editing a tenant, if you modify **Tenant-owned Public IP Pool** under Advanced Settings (optional), then the changes that you made to the **Tenant-owned Public IP pool** field are not reflected after the completion of the edit tenant operation job.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41139

- The TAR file installation of a distributed deployment fails. This issue occurs if the version of the bare-metal server that you are using is later than the recommended version.

Workaround: You must install the **python-dev** script before running the **deploy-sh** script.

After you extract the CSO TAR file on the bare-metal server:

1. Navigate to the **/etc/apt** directory and execute the following commands:
 - **cp sources.list sources.list.cso**
 - **cp orig-sources.list sources.list**
2. Install the **python2.7-dev** script by running the following commands:
 - **apt-get update && apt-get install python2.7-dev**
 - **cp sources.list.cso sources.list**
3. Navigate to the **/root/Contrail_Service_Orchestration_5.1.0** folder and then run the **deploy.sh** script.

Bug Tracking Number: CXU-41845

- 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 address 192.168.2.0 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

- If you have installed CSO Release 5.1 on a single node and if there is a power failure, the UI is not accessible even if the power resumes.

Workaround:

1. On the infraservices virtual machine (VM),
 - a. Stop the kubernetes and dockers on both infra service and microservice by running the **service kubelet stop** and **service docker stop** commands.
 - b. Navigate to the **/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt** folder and take a backup of the **meta.db** file.

```
root@k8-infra1-vm:~# cd
/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt/
root@k8-infra1:/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt#
mv meta.db meta.db.bak
```

- c. Navigate to the **/var/lib/docker** folder and take a backup of the **network** file.

```
root@k8-infra1-vm:/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt#
cd /var/lib/docker
root@k8-infra1:/var/lib/docker# mv network network_bkp
```

2. On the microservice VM,
 - a. Stop the kubernetes and dockers on both infra service and microservice by running the **service kubelet stop** and **service docker stop** commands.
 - b. Navigate to the **/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt** folder and take a backup of the **meta.db** file.

```
root@k8-microservices_1:~# cd
/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt/
root@k8-microservices_1:/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt#
mv meta.db meta.db.bak
```

- c. Navigate to the **/var/lib/docker** folder and take a backup of the **network** file.

```
root@k8-microservices_1:/var/lib/docker/containerd/daemon/io.containerd.metadata.v1.bolt#
cd /var/lib/docker
root@k8-microservices_1:/var/lib/docker# mv network network_bkp
```

3. Restart the kubernetes and dockers on both infra service and microservice by running the **service docker start** and **service kubelet start** commands.
4. Navigate to the **Contrail_Service_Orchestration_** folder and run the **setup_NAT_rule.sh** script on the bare-metal server to enable traffic flow from outside the network.

```
root@ccra-68:~/Contrail_Service_Orchestration_/ci_cd# ./setup_NAT_rule.sh
```

5. On the Startup server, run the **kubectrl delete pods -all -n central && kubectrl delete pods -all -n regional** command to restart CS0 microservices.

Bug Tracking Number: CXU-41460

- 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 an SRX4200 dual CPE cluster 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

- When you back up an SD-WAN report generated in CSO Release 4.1.1 and restore it in CSO Release 5.1.1, an error appears when you try to download the report, and the report is not downloaded.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-42395

- When you configure a CPE behind NAT, DVPN tunnels stay between an Internet link that is behind NAT and an Internet link that is not behind NAT due to a wrong external interface in the IPsec configuration.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-43217

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.1.1:

- The parameter, `NO_LOCAL_FAVOR_ECMP`, is added to the configuration templates for an SRX dual CPE cluster, such as dual SRX as SD-WAN CPEs, to load balance equal-cost multi path (ECMP) traffic across active-active links on the nodes of an SRX dual CPE cluster. This parameter is available only when the devices in the cluster are running Junos OS Release 19.3R2-S1 or later.

Bug Tracking Number: CXU-42357

- When you configure and deploy IPS on the firewall rule, IDP does not detect the attacks and processes the traffic on an NFX150 device with Junos OS Release 18.2X85-D12 when a dynamic application is configured.

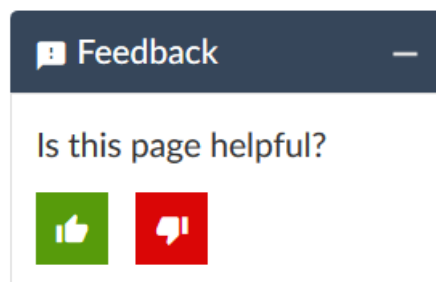
NOTE: This issue is resolved when you use Junos OS Release 18.3R1 or later on the NFX150 device.

Bug Tracking Number: CXU-38388

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

12 February, 2020—Revision 1, CSO Release 5.1.1

2 March, 2020—Revision 2, CSO Release 5.1.1

5 March, 2020—Revision 3, Added note that SP admin role is not applicable when CSO is offered as a cloud-based service.

7 April, 2020—Revision 4, Incorporated editorial comments.

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.