

# Contrail Service Orchestration Release Notes

Release 4.0.0  
28 January 2019  
Revision 7

These Release Notes accompany Release 4.0.0 of Juniper Networks® Contrail Service Orchestration (CSO). They contain installation and upgrade information, and they describe new and changed features, limitations, and known and resolved issues in the software.

## Contents

Introduction .....	3
Installation and Upgrade .....	5
Software Downloads .....	6
Installation Instructions .....	7
Software Installation Requirements for NFX Series Network Services	
Platform .....	7
Upgrade Instructions .....	8
Installation and Upgrade Limitations .....	8
Post-Installation and Post-Upgrade Instructions .....	8
New and Changed Features in Contrail Service Orchestration Release 4.0.0 .....	9
Installation and Upgrade .....	9
Device Management .....	9
SD-WAN .....	11
Miscellaneous .....	12
Unified Portal .....	14
Unsupported Features .....	14
Servers, Software, and Network Devices Tested .....	15
Hardware, Software, and Virtual Machine Requirements for CSO .....	15
VNFs Supported .....	15
Licensing .....	16
Accessing the CSO GUIs .....	16
Known Behavior .....	16
AWS Spoke .....	17
Policy Deployment .....	17
SD-WAN .....	18
Security Management .....	18
Site and Tenant Workflow .....	18

Topology .....	20
User Interface .....	20
General .....	20
Known Issues .....	23
AWS Spoke .....	24
CSO HA .....	24
SD-WAN .....	28
Security Management .....	29
Site and Tenant Workflow .....	30
General .....	33
Resolved Issues .....	45
Documentation Updates .....	47
Documentation Feedback .....	47
Requesting Technical Support .....	47
Self-Help Online Tools and Resources .....	48
Creating a Service Request with JTAC .....	48
Revision History .....	48

## Introduction

---

Juniper Networks Contrail Service Orchestration (CSO) transforms traditional branch networks, offering opportunities for high flexibility of the network, rapid introduction of new services, automation of network administration, and cost savings. The solution supports both Juniper Networks and third-party virtualized network functions (VNFs) that network providers use to create network services.

CSO Release 4.0.0 is a secure software-defined WAN (SD-WAN) solution that builds on the capabilities of CSO Release 3.3 and the Cloud CPE solution. The following are the highlights of the features available in Release 4.0.0:

- SD-WAN
  - Secure OAM network
  - ADSL and VDSL access types
  - Service chaining in SD-WAN deployments
  - Enhanced LTE support
  - Real-time-optimized SD-WAN on NFX250 dual CPE devices
  - Multihoming in real-time-optimized SD-WAN
  - Cost-based link switching
  - vSRX as SD-WAN hub gateway
- Infrastructure
  - Optimized memory footprint
  - GUI-based downloader and installer
  - Support for applying security patches for microservices without reboot
  - Upgrade from CSO Release 3.3.1 or Release 3.3.0 to Release 4.0.0

You can also upgrade from CSO Release 3.2.1 to Release 4.0.0 by first upgrading to CSO Release 3.3.1.

- Devices
  - Support for NFX150 as a CPE device
  - Descriptive device template names
  - Support for bootstrap logs
- Miscellaneous
  - Object-based custom roles
  - Support for operating companies
  - Audit logs
  - Option to enable stage-2 configuration templates

- Site upgrade
- Additional portal customization options
- Hybrid WAN and SD-WAN sites for the same tenant

CSO can be implemented by service providers to offer network services to their customers or by Enterprise IT departments in a campus and branch environment. In these release notes, service providers and Enterprise IT departments are called *service providers*, and the consumers of their services are called *customers*.

The solution offers the following deployment models:

- Cloud CPE distributed deployment Model (*distributed deployment*)

In the distributed deployment, customers access network services on a CPE device, located at a customer's site. These sites are called *on-premise sites* in these release notes.

Sites can be configured as one of the following types:

- Hybrid WAN
- SD-WAN

In a distributed deployment:

- Network Service Orchestrator, together with Network Service Controller, provides ETSI-compliant management of the life cycle of network service instances.
- Network Service Controller provides the VIM.
- The CPE device provides the NFV infrastructure.

- Cloud CPE centralized deployment Model (*centralized deployment*)

In a centralized deployment, customers access network services in a service provider's cloud. Sites that access network services in this way are called *cloud sites* in these release notes.

In this deployment, CSO uses the following components for the NFV environment:

- Network Service Orchestrator provides ETSI-compliant management of the life cycle of network service instances.
- Contrail Cloud Platform provides the underlying software-defined networking (SDN), NFV infrastructure (NFVI), and the virtualized infrastructure manager (VIM).

CSO can be deployed in three deployment types—small, medium, or large.

[Table 1 on page 5](#) shows the number of sites and VNFs supported for each environment.

Table 1: Number of Sites and VNFs Supported

Deployment Type	Number of VNFs Supported for a Centralized Deployment	Number of Sites and VNFs Supported for a Distributed Deployment	Number of Sites Supported for an SD-WAN Deployment	
			Hub and Spoke Sites	Full Mesh Sites
Small	10 VNFs	Up to 450, 2 VNFs per site	Up to 450	Up to 100
Medium	100 VNFs, 20 VNFs per Contrail compute node	Up to 3500, 2 VNFs per site	Up to 3500	Up to 200
Large	500 VNFs, 20 VNFs per Contrail compute node	Up to 5000, 2 VNFs per site	Up to 5000	Up to 200

## Installation and Upgrade

From CSO Release 4.0.0 onward, you can install CSO using a new GUI-based installer as well as through the existing CLI installer.



### NOTE:

- When you install or upgrade CSO by using the CLI, ensure that you save the passwords for each infrastructure component when they are displayed on the console because these passwords are encrypted and are not displayed again.

In addition, during the installation, ensure that you save the Administration Portal password that is displayed on the console. For the upgrade, you must log in using the password configured for the previously installed version of CSO.

- If you are using the GUI installer, after the installation is successful, click the [View all IP addresses and passwords](#) link to view all the IP addresses used by CSO and the passwords for various CSO components.

Ensure that you save the passwords for each CSO component (the *cspadmin* password, used for the Administration Portal login, is the most important) because these passwords are not displayed again.

- [Software Downloads](#)
- [Installation Instructions](#)
- [Software Installation Requirements for NFX Series Network Services Platform](#)
- [Upgrade Instructions](#)
- [Installation and Upgrade Limitations](#)
- [Post-Installation and Post-Upgrade Instructions](#)

## Software Downloads

Table 2 on page 6 displays the supported versions and download links for CSO Release 4.0.0 and associated software components. We recommend that you use the CSO Downloader to download and install CSO.

**Table 2: CSO and Associated Software Components**

Product	Supported Version	Download Link
CSO Downloader (available for Windows, MacOS, and Linux Desktop versions)	4.0.0	<a href="https://www.juniper.net/support/downloads/?p=cso">https://www.juniper.net/support/downloads/?p=cso</a>
Contrail Service Orchestration	4.0.0	<a href="https://www.juniper.net/support/downloads/?p=cso">https://www.juniper.net/support/downloads/?p=cso</a>
Juniper Identity Management Service (JIMS)	1.1.1R1	Pre-bundled with CSO and also available here: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/75619.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/75619.html</a>
Contrail Analytics	4.1.1.0-130	Pre-bundled with CSO
Contrail Cloud Platform	3.2.5	<a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/69888.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/69888.html</a>
NFX150 CPE device	Junos OS Release 18.2R1	<a href="https://www.juniper.net/support/downloads/?p=nfx150">https://www.juniper.net/support/downloads/?p=nfx150</a>
NFX250 CPE device	Junos OS Release 15.1X53-D490	<a href="https://www.juniper.net/support/downloads/?p=nfx250">https://www.juniper.net/support/downloads/?p=nfx250</a>
SRX Series CPE device	Junos OS Release 15.1X49-D143	<ul style="list-style-type: none"> <li>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77057.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77057.html</a></li> <li>SRX1500: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77056.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77056.html</a></li> <li>SRX1500 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77100.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77100.html</a></li> <li>SRX1500 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77125.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77125.html</a></li> <li>SRX4100, SRX4200: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77058.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77058.html</a></li> <li>SRX4100, SRX4200 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77099.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77099.html</a></li> <li>SRX4100, SRX4200 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77124.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77124.html</a></li> </ul>

Table 2: CSO and Associated Software Components (continued)

Product	Supported Version	Download Link
vSRX	Junos OS Release 15.1X49-D143	<ul style="list-style-type: none"> <li>vSRX (Compressed tar file (TGZ) for upgrade): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77138.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77138.html</a></li> <li>vSRX (KVM appliance): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77148.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77148.html</a></li> <li>vSRX (Hyper-V image): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77146.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77146.html</a></li> <li>vSRX (VMware appliance with SCSI virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77149.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77149.html</a></li> <li>vSRX (VMware appliance with IDE virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77147.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/77147.html</a></li> </ul>
MX Series (hub device)	Junos OS Release 16.1R5	<a href="https://www.juniper.net/support/downloads/">https://www.juniper.net/support/downloads/</a>

## Installation Instructions

A full-version installer is available for CSO Release 4.0.0, which can be used for small, medium, and large deployments. For more information, follow the instructions in the [Installation and Upgrade Guide](#) or the README file that is included with the software installation package.



**NOTE:** The physical servers on which you install CSO must have Internet access to download the libvirt packages. After the packages are downloaded, you do not need Internet access for the rest of the CSO installation.

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

For more information, see [https://www.juniper.net/documentation/en\\_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/](https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/).

## Upgrade Instructions



**NOTE:** You can upgrade to CSO Release 4.0.0 from CSO Release 3.3.1 or Release 3.3.0.

You can also upgrade from CSO Release 3.2.1 to Release 4.0.0 by first upgrading to CSO Release 3.3.1.

If your installed version of CSO is not Release 3.3.1, 3.3.0, or 3.2.1, then you must perform a fresh installation of CSO Release 4.0.0.

If your installed version is CSO Release 3.3.1 or Release 3.3.0, you can use a script (**upgrade.sh**) to directly upgrade to CSO Release 4.0.0. If the upgrade is unsuccessful, you can roll back to CSO Release 3.3.1 or Release 3.3.0, respectively.

For more information, see *Upgrading Contrail Service Orchestration Overview* in the [Installation and Upgrade Guide](#).

## Installation and Upgrade Limitations

- For SD-WAN deployments, CPE devices behind NAT are supported only for Internet links.
- If the Kubernetes minion node in the central or regional microservices virtual machine (VM) goes down, the pods on the minion node are moved to another Kubernetes minion node. When you bring the minion node back up, the pods do not automatically rebalance across the nodes.
- The VM on which the virtual route reflector (VRR) is installed supports only one management interface.
- Before upgrading vSRX by using CSO, execute the **request system storage cleanup** command on the vSRX by using Junos OS CLI.

## Post-Installation and Post-Upgrade Instructions

- After you successfully install or upgrade CSO, you must do the following:
  - Configure SMTP settings—After you log in for the first time to the CSO GUI, you must configure the SMTP settings for your deployment on the SMTP Settings page (**Administration > SMTP**).
  - Configure name servers on CPE devices—Use custom properties to provide the name server details when you are adding a tenant.
- Accessing GUIs—We recommend that you use Google Chrome version 60 or later to access the CSO GUIs. For more information, see *Accessing the Contrail Services Orchestration GUIs* in the Deployment Guide.



## New and Changed Features in Contrail Service Orchestration Release 4.0.0

---

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 4.0.0.

- [Installation and Upgrade](#)
- [Device Management](#)
- [SD-WAN](#)
- [Miscellaneous](#)
- [Unified Portal](#)
- [Unsupported Features](#)

### Installation and Upgrade

- **Optimized resource footprint for CSO**—From Release 4.0.0 onward, CSO offers additional deployment modes (small and medium) where regional and central components are colocated, thus reducing the required server resources.
- **CSO installation using GUI**—From CSO Release 4.0.0 onward, you can install CSO by using a new GUI installer as well as through the traditional CLI. This feature simplifies the CSO installation process and automatically provisions the VMs. It consists of two components—the downloader and the CSO installer.

Currently, upgrades are not supported through the GUI.

- **New nomenclature for CSO environments**—From CSO Release 4.0.0 onward, the deployment types are referred to as small, medium, and large.
  - A small deployment is not configured for high availability and is recommended if you need to manage up to 450 sites.
  - A medium deployment is configured with high availability and is recommended if you need to manage up to 3500 sites.
  - A large deployment is configured with high availability and is recommended if you need to manage up to 5000 sites.
- **Support for applying security patches for microservices without needing to reboot**—From CSO Release 4.0.0 onward, you can apply in-service patches to CSO microservices without needing to reboot. This feature is applicable to only microservices and is not supported for infrastructure components.

### Device Management

- **Support for NFX150 as a CPE device**—From CSO Release 4.0.0 onward, you can add the following NFX150 device models as CPE devices in SD-WAN and Hybrid WAN deployments:
  - NFX150-C-S1
  - NFX150-C-S1-AE/AA

- NFX150-C-S1E-AE/AA
- NFX150-S1
- NFX150-S1E

The following display names (device templates) are supported:

- NFX150 as Managed Internet CPE
- NFX150 as Hybrid WAN CPE
- NFX150 as Secure Internet CPE
- NFX150 as SD-WAN CPE
- **Software features supported on the NFX150 device**—From CSO Release 4.0.0 onward, the NFX150 device supports the following features:
  - Hybrid WAN deployment
    - NFX150 device as managed Internet CPE device, secured Internet CPE device, and hybrid WAN CPE device.
    - Stage-2 configuration templates.
    - Service chaining with third-party VNFs such as Riverbed and Ubuntu.
  - SD-WAN deployment
    - NFX150 device as SD-WAN CPE.
    - Multihoming to MX Series and SRX Series hub devices with Application Quality of Experience (AppQoE), advanced policy-based routing (APBR), application visibility, and real-time performance monitoring (RPM).
    - Service chaining with third-party VNFs such as Fortinet (VNF in Layer 2 virtual-wire-pair mode), and Ubuntu (single-legged VNF).
    - Service chaining support without WAN optimization, AppQoE, and APBR.
    - NFX150 device as a CPE device in hub-and-spoke, and full mesh topologies.
    - LTE, ADSL, and VDSL access link types for WAN connectivity.
    - LTE support with RPM and AppQoE.
    - SD-WAN, firewall, SSL proxy, network address translation (NAT), and unified threat management (UTM) policies.
    - Application path selection with dynamic service-level agreement (SLA) profile, RPM, and APBR.
    - Secure Operation, Administration, and Maintenance (OAM) network.



**NOTE:** The NFX150 device is not supported in device redundancy mode.

- **Support for pushing licenses to NFX150 devices**—From CSO Release 4.0.0 onward, you can push licenses to NFX150 devices.
- **Support for monitoring threats on NFX150 devices**—From CSO Release 4.0.0 onward, on NFX150 devices, you can monitor incoming and outgoing threats between geographic regions on the threats map.
- **Support for enabling stage-2 configuration templates**—From CSO Release 4.0.0 onward, you can enable the stage-2 configuration template for all tenants, specific tenants, an SP administrator, or an OpCo administrator.
- **Change in device template names**—From CSO Release 4.0.0 onward, the device template names and descriptions are modified to provide information about the device family and the deployment model.

To view the changed device template names and descriptions, log in to Administration Portal and select **Resources > Device Templates**.

- **Support for bootstrap logs**—From CSO Release 4.0.0 onward, bootstrap logs (stage-1 configuration and device availability) are included in Zero Touch Provisioning (ZTP) job logs. You can use the bootstrap logs to monitor the progress of device activation during stage-1 configuration.

## SD-WAN

- **Support for secure OAM network**—From CSO Release 4.0.0 onward, you can configure a secure Operation, Administration, and Maintenance (OAM) network between SD-WAN sites and CSO. The secure OAM network is built using dedicated IPsec tunnels that are established between each CPE device associated with the SD-WAN site and a cloud hub with OAM capability.

You specify the capability of the cloud hub device as either data, OAM, or data and OAM while adding the cloud hub device.

- **Support for ADSL and VDSL access types on NFX Series devices**—CSO Release 4.0.0 supports asymmetric digital subscriber line (ADSL) and very-high-bit-rate digital subscriber line (VDSL) access links on NFX150 and NX250 devices. You configure ADSL or VDSL access types while creating an on-premise spoke site in an SD-WAN deployment.
- **Support for service chaining**—CSO Release 4.0.0 supports service chaining in SD-WAN deployments for the following third-party VNFs:
  - Fortinet VNF in Layer 2 virtual wire-pair mode
  - Ubuntu single-legged VNF
- **Enhanced support for LTE interface**—From CSO Release 4.0.0 onward, you can configure the LTE interface on NFX250 devices as a backup link, a default link, an OAM link, or exclusively for breakout traffic. In CSO Release 3.3.x, the LTE link is selected as the backup link by default.



**NOTE:** The LTE link is supported only in the hub-and-spoke topology and in the full-mesh topology with a hub.

- **Support for real-time-optimized SD-WAN on NFX250 dual CPE devices**—From Release 4.0.0 onward, CSO supports NFX250 dual CPE devices for real-time-optimized SD-WAN deployments. You can select dual CPE connection plans for sites of tenants that have the SD-WAN mode set to real time-optimized.

Support for dual CPE devices ensures high availability for SD-WAN in real-time-optimized mode.

- **Support for multihoming in real-time-optimized SD-WAN**—From Release 4.0.0 onward, CSO supports multihoming in real-time-optimized SD-WAN deployments; support for multihoming in real-time-optimized SD-WAN enhances the redundancy for AppQoE.
- **Enhancements to SLA profile-based link switching**—From Release 4.0.0 onward, when two or more links meet the SLA profile parameters, CSO chooses the least-expensive link to route the traffic. CSO uses the cost per month (**Cost/month**) parameter specified for the WAN link to identify the most cost-effective link to route traffic. If a less expensive link comes online and meets the specified SLA parameters, the traffic is switched to the less expensive link.



**NOTE:** In real-time-optimized SD-WAN deployments, CSO does not consider the cost per month parameter while switching links.

- **Support for vSRX as SD-WAN hub gateway**—From Release 4.0 onward, CSO supports the use of vSRX as an SD-WAN hub gateway in two modes. The first mode is fully orchestrated, where CSO manages the entire life cycle of the vSRX VM. The second mode is partially orchestrated, where a third-party orchestrator starts the vSRX VM, and then hands over the ZTP and service definition tasks to CSO.



**NOTE:** CSO does not start the vSRX VM in either mode.

## Miscellaneous

- **Object-based custom roles**—From Release 4.0.0 onward, CSO enables you to create object-based custom roles. When you create custom roles, you can select objects (for example, devices, device templates, and images) in the CSO application and assign access privileges (read, create, update, delete, and other actions) for those objects. You can assign one or more roles (both predefined and custom) to a user when you create or edit a user account. If you assign more than one role to a user, then the user will have combined capabilities of those roles.
- **Support for operating companies**—CSO Release 4.0.0 supports operating companies in a service provider environment. A global service provider can create one or more operating companies and share resources (cloud hub devices, device templates, and so on) with operating companies. An operating company (OpCo) is a region-specific service provider that can manage its tenants and provide services to them. Tenants managed by one OpCo are isolated from tenants of another OpCo.

- **Mapping between CSO-defined and SSO-defined roles**—From CSO Release 4.0.0 onward, for the SSO authentication and authorization method, a list of permitted roles (both predefined and custom) must be provided to the SSO server. Only users with permitted roles in the Security Assertion Markup Language (SAML) attribute of the SSO server are allowed to log in to CSO. Roles used in the SSO server (Identity Provider) are different from the roles used in CSO. Therefore, you must map the roles that are defined in CSO with the roles defined in the SSO server.
- **Support for audit logs**—From Release 4.0.0 onward, CSO supports audit logs that contain information about tasks initiated by using the CSO GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries include details about user-initiated tasks, such as the name, role, and IP address of the user who initiated a task, the status of the task, and the date and time of execution. You can export audit logs (up to 30 days) in comma-separated values (CSV) format. Log in to Administration Portal or Customer Portal and select **Administration > Audit Logs** to view the logs.
- **Enhancements in license management**—From CSO Release 4.0.0 onward, you can push licenses to multiple devices from the Devices page. You can also view the number of devices to which a license is pushed on the License Files page.
- **Additional options to customize the unified portal**—From CSO Release 4.0.0 onward, you have more options to customize the unified Administration and Customer Portal. Customization options include background color of UI elements, change in background color of UI elements, custom color palette for login page, and so on.
- **Support for SD-WAN and Hybrid WAN sites for the same tenant**—From CSO Release 4.0.0 onward, a single tenant can have both SD-WAN and Hybrid WAN sites. While creating a tenant, an SP administrator can specify whether a tenant can create:
  - Only SD-WAN sites
  - Only Hybrid WAN sites
  - Both SD-WAN and Hybrid WAN sites

## Unified Portal

- **Support for site upgrade**—From CSO Release 4.0.0 onward, you can upgrade one or more sites from the Sites page. The Sites page provides information about sites that must be upgraded and sites for which the upgrade is optional.

Upgrading sites that are created in Release 3.3.0 and Release 3.3.1 is optional. You must upgrade sites that are created in releases earlier than Release 3.3.0.

## Unsupported Features

The CSO Release 4.0.0 documentation describes some features that are present in the application but that have not yet been fully qualified by Juniper Networks. If you use any of these features before they have been fully qualified, it is your responsibility to ensure that the feature operates correctly in your targeted configuration.

The following features are present but unsupported in this release:

- **IPsec tunnel encryption**—From CSO Release 4.0.0 onward, the following IPsec tunnel encryption types are supported for SD-WAN deployments:
  - 3DES-CBC
  - AES-128-CBC
  - AES-128-GCM
  - AES-256-CBC
  - AES-256-GCM

The default encryption type is AES-256-GCM.

- **PKI certificates**—From CSO Release 4.0.0 onward, CSO supports public key infrastructure (PKI) certificates for IPsec tunneling on NFX250, NFX150, and SRX Series devices for SD-WAN deployments.
- OAM-only hub
- Data-only hub
- ZTP over ADSL or VDSL links
- PPPoE over ADSL or VDSL links (because of limitations on NFX150 and NFX250 devices).



**NOTE:** You can use static IP addresses or DHCP-based IP addresses for link configuration.

---

## Servers, Software, and Network Devices Tested

From CSO Release 4.0.0 onward, the information in this section is moved to the *Hardware and Software Required for Contrail Service Orchestration* topic in the *Contrail Service Orchestration Installation and Upgrade Guide*.

## Hardware, Software, and Virtual Machine Requirements for CSO

From CSO Release 4.0.0 onward, the information in this section is moved to the *Minimum Requirements for Servers and VMs* topic in the *Contrail Service Orchestration Installation and Upgrade Guide*.

## VNFs Supported

CSO supports the Juniper Networks and third-party VNFs listed in [Table 3 on page 15](#).

**Table 3: VNFs Supported by Contrail Service Orchestration**

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	vSRX KVM Appliance 15.1X49-D143	<ul style="list-style-type: none"> <li>Network Address Translation (NAT)</li> <li>Demonstration version of Deep Packet Inspection (DPI)</li> <li>Firewall</li> <li>Unified threat management (UTM)</li> </ul>	<ul style="list-style-type: none"> <li>Centralized deployment</li> <li>Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.</li> </ul>	Element Management System (EMS) microservice, which is included with CSO
LxCIPtable (a free, third party VNF based on Linux IP tables)	14.04	<ul style="list-style-type: none"> <li>NAT</li> <li>Firewall</li> </ul>	Centralized deployment	EMS microservice
Cisco Cloud Services Router 1000V Series (CSR-1000V)	3.15.0	Firewall	Centralized deployment	Junos Space Network Management Platform
Riverbed SteelHead	9.2.0	WAN optimization	Hybrid WAN deployment—NFX250 and NFX150 platforms.	EMS microservice
Fortinet	5.6.3	Firewall	Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms.	EMS microservice
Single-legged Ubuntu	16.04	Firewall	Hybrid WAN and SD-WAN deployments—NFX250 and NFX150 platforms.	EMS microservice

## Licensing

---

You must have licenses to download and use the 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.

The CSO licensing model depends on whether you use a centralized or distributed deployment:

- For a centralized deployment, you need licenses for Network Service Orchestrator and for Contrail Cloud Platform. You can either purchase both types of licenses in one Cloud CPE MANO package or you can purchase each type of license individually.

You also need licenses for:

- Junos OS software for the MX Series router, EX Series switch, and QFX Series switch in the Contrail Cloud Platform.
  - VNFs that you deploy.
  - (Optional) Licenses for Junos Space Network Management Platform, if you deploy VNFs that require this EMS.
- For a distributed deployment, Juniper Networks has introduced bundled licenses in addition to the a la carte (existing) licenses. The SD-WAN bundle license, which includes hardware and software licenses, can be purchased as subscription or perpetual licenses.

An SD-WAN bundle includes licenses for hardware (SRX Series and NFX Series), Junos OS, SD-WAN features, and CSO for orchestration and management.

The licenses for Junos OS software and hardware for the MX Series router is not included as part of the SD-WAN bundle and must be purchased separately.

## Accessing the CSO GUIs

---



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

From CSO Release 4.0.0 onward, the information in this section is moved to *Accessing the Contrail Services Orchestration GUIs* topic in the *CSO Deployment Guide*.

## Known Behavior

---

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 4.0.0.

- [AWS Spoke](#)
- [Policy Deployment](#)
- [SD-WAN](#)



- [Security Management](#)
- [Site and Tenant Workflow](#)
- [Topology](#)
- [User Interface](#)
- [General](#)

## AWS Spoke

- When an AWS spoke site is being provisioned and the vSRX instance is coming up, all traffic from the LAN and WAN subnets (configured during site creation) is stopped for 16–30 minutes. After the device is activated and if intent-based policies are configured, the traffic flows as configured.
- The cloud formation template includes a new route table to forward traffic to the vSRX device. If you have configured manual routing between your subnets and VMs, then the new route table replaces the manual routing with only one route forwarding the traffic to the vSRX device.
- The current supported Junos OS release for the AWS spoke is Junos OS Release 15.1X49.D143. When a new qualified image is posted in AWS marketplace, the procedure to update the Amazon Machine Image (AMI) ID is as follows:
  1. Log in Administration Portal.
  2. Select **Resources > Device Templates**.  
The Device Template page appears.
  3. Select **vSRX\_AWS\_SDWAN\_Endpoint\_option\_1**.
  4. Select **Edit Device Template > Template Settings**.  
The Template Settings page appears.
  5. Modify the image ID to the AMI ID for your region.
  6. Click **Save**.
  7. Proceed with the workflow for the cloud formation template in AWS.
- When you create a cloud spoke site, the default link fields and backup link fields are not applicable.

## 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 is done so 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

- 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.
- If the SD-WAN mode is **Real-Time Optimized** and a path switch is triggered because a link goes down, sometimes the link switch event displayed in the CSO GUI does not contain the SLA violation metric details.
- On the SD-WAN Events page, when you 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. However, even though an SLA violation is reported, the traffic does not switch to a different link.

## Security Management

- Intrusion prevention system (IPS) is not supported. Therefore, in the IPS report, the attack name from the IPS signatures is displayed as UNKNOWN.
- SSL Proxy is not supported on SRX300 and SRX320 series devices.

## Site and Tenant Workflow

- In the Configure Site workflow, use IP addresses instead of hostnames for the NTP server configuration.
- CSO uses hostname-based certificates for device activation. The regional microservices VM hostname must be resolvable from the CPE device.
- 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.
  - Tenant Administrator users cannot delete sites.
  - 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 UI. There is no impact on the functionality.
  - CSO does not push the default class-of-service configuration on the hub device. You must configure this configuration manually to ensure that the hub configuration is synchronized with the spoke configuration.
  - On a cloud hub shared by multiple tenants, by default, CSO does not add a default route and no security policies are configured for the traffic to reach the Internet. You must add the default route and the required security policies for the site traffic to reach the Internet through the cloud hub.
  - If you do not use the redirect service from Juniper Networks (redirect.juniper.net), after you upgrade an NFX Series device to Junos OS Release 15.1X53-D473, the device is unable to connect to the regional server because the phone home server certificate (**phd-ca.crt**) is reverted to the factory default.

Workaround: Manually copy the regional certificate to the NFX Series device.

- On the Sites page, when you trigger the **Upgrade** action, the site upgrade analysis report might not list the impact of parent device profile on the upgrade. However, there is no impact on the upgrade because the upgrade workflow takes into account the impact of the parent device profile and pushes the correct upgrade workflows to the device.
- If an NFX250 CPE device is pre-staged to use CSO as the phone-home server, bypassing the redirect service from Juniper Networks, you must add the following configuration to prevent the CSO certificate from being overwritten during a reboot:

```
set system phone-home ca-certification-file /root/phcd-ca.crt
```

## Topology

- DHCP configuration on WAN links on a SD-WAN hub is not supported.
- Automatic hub-meshing is not supported. Hub-meshing must be performed manually in order for traffic to flow between the hubs.
- On-premise hubs are not supported.
- An MX Series router configured as a cloud hub device 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.

## General

- When you edit a tenant, changing the deployment plan from Hybrid WAN to SD-WAN or vice versa is not supported, although the field is displayed as editable.
- For a centralized deployment, use the following procedure to check that the JSM Heat resource is available in Contrail OpenStack on the Contrail Controller node.



**NOTE:** This procedure must be performed on all the Contrail Controller nodes in your CSO installation.

1. Log in to the Contrail Controller node as root.
2. To check whether the JSM Heat resource is available, execute the **heat resource-type-list | grep JSM** command.

If the search returns the text **OS::JSM::Get Flavor**, the file is available in Contrail OpenStack.

3. If the file is missing, do the following:
  - a. Use Secure Copy Protocol (SCP) to copy the `jsm_contrail_3.py` file to the following directory:
    - For Heat V1 APIs, the `/usr/lib/python2.7/dist-packages/contrail_heat/resources` directory on the Contrail Controller node.
    - For Heat V2 APIs, the `/usr/lib/python2.7/dist-packages/vnc_api/gen/heat/resources` directory on the Contrail Controller node.



**NOTE:** The `jsm_contrail_3.py` file is located in the `/root/Contrail_Service_Orchestration_4.0.0/scripts` directory on the VM or server on which you installed CSO.

- b. Rename the file to `jsm.py` in the Heat resource directory to which you copied the file.
  - c. Restart the Heat services by executing the `service heat-api restart && service heat-api-cfn restart && service heat-engine restart` command.
  - d. After the services restart successfully, verify that the JSM Heat resource is available as explained in Step 2. If it is not available, repeat Step 3.
- In vCPE deployments, when a tenant object is created through Administration Portal or the API for a centralized deployment, Contrail OpenStack adds a default security group for the new tenant. This default security group denies inbound traffic and you must manually update the security group in Contrail OpenStack to allow ingress traffic from different networks. Otherwise, Contrail OpenStack might drop traffic.
- In vCPE deployments, CSO does not provide a remote procedure call (RPC) to get the device identifier for a specific site. You can use multiple API calls or the license installation tool to obtain the device identifier for a specific site.
- 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.

- The Ubuntu VNF interface toward the LAN segment of the vSRX gateway router is not automatically provisioned by CSO. You must manually provision the interface as follows:

- On a LAN segment that does not use a VLAN, execute the **ifconfig ens5 ip-prefix** command, where **ip-prefix** is the IP prefix of the LAN subnet.
- On a LAN segment that uses a VLAN, execute the following commands:

```
vconfig add ens5 vlan-id  
ifconfig ens5.vlan-id ip-prefix
```

where **vlan-id** is the VLAN ID of the LAN and **ip-prefix** is the IP prefix of the LAN subnet.

- Class-of-service (CoS) configuration on Layer 2 interfaces (ge-0/0/\*) is not supported on NFX150 CPE devices.
- Image upgrade of a vSRX gateway router on NFX Series devices by using the CSO GUI is not supported.

Workaround: Upgrade the image by using the CLI of the NFX Series device.

- In CSO Release 4.0.0, the collection of service metrics is disabled by default for SRX Series and NFX150 devices, so the **get\_service\_metrics** API does not return any data.

To enable the collection of service metrics:

1. On the infrastructure VM or, if regions are present, the regional infrastructure VM, log in as root and execute the **etcdctl set /telemetry-agent/metric\_collection ENABLE** command.
2. To restart the telemetry agent microservice:
  - If no regions are present, log in to the microservices VM as root and execute the **kubectrl delete pods csp.csp-telemetry-agent -n regional** command.
  - If regions are present, log in to the regional microservices VM as root and execute the **kubectrl delete pods csp.csp-telemetry-agent** command.

The collection of service metrics data is enabled, and you can use the **get\_service\_metrics** API to obtain the data.

- The RMA workflow is not supported on NFX150 CPE devices.

## Known Issues

---

This section lists known issues in Juniper Networks CSO Release 4.0.0.

- [AWS Spoke](#)
- [CSO HA](#)
- [SD-WAN](#)
- [Security Management](#)
- [Site and Tenant Workflow](#)
- [General](#)

## AWS Spoke

- The AWS device activation process takes up to 30 minutes. If the process does not complete in 30 minutes, a timeout might occur and you must retry the process. You do not need to download the cloud formation template again.

To retry the process:

1. Log in to Customer Portal.
2. Access the Activate Device page, enter the activation code, and click **Next**.
3. After the **CREATE\_COMPLETE** message is displayed on the AWS server, click **Next** on the Activate Device page to proceed with device activation.

Bug Tracking Number: CXU-19102.

## CSO HA

- In a CSO HA environment, two RabbitMQ nodes are clustered together, but the third RabbitMQ node does not join the cluster. This might occur just after the initial installation, if a virtual machine reboots, or if a virtual machine is powered off and then powered on.

Workaround: Do the following:

1. Log in to the installer VM.
2. Navigate to the current deployment directory for CSO—for example, `/root/Contrail_Service_Orchestration_4.0.0/`.
3. Execute the `./recovery.sh` command.
4. Specify the option to recover RabbitMQ, and press Enter.
5. In the RabbitMQ dashboards for the central and regional microservices VMs, confirm that all the available infrastructure nodes are present in the cluster.

Bug Tracking Number: CXU-12107

- In an HA setup, the time configured for the CAN VMs might not be synchronized with the time configured for the other VMs in the setup. This can cause issues in the throughput graphs.

Workaround:

1. Log in to can-vm1 as the root user.



2. Modify the `/etc/ntp.conf` file to point to the desired NTP server.
3. Restart the NTP process.

After the NTP process restarts successfully, can-vm2 and can-vm3 automatically resynchronize their times with can-vm1.

Bug Tracking Number: CXU-15681.

- When a high availability (HA) setup comes back up after a power outage, MariaDB instances do not come back up on the VMs.

Workaround:

Perform the following steps to recover the MariaDB instances:

1. Log in to the installer VM.
2. Navigate to the current deployment directory for CSO—for example, `/root/Contrail_Service_Orchestration_4.0.0/`.
3. Execute the `sed -i`  
`"s@/var/lib/mysql/grastate.dat@/mnt/data/mysql/grastate.dat@g"`  
`recovery/components/recover_mariadb.py` command.
4. Execute the `./recovery.sh` command.
5. Specify the option to recover MariaDB, and press Enter.

Bug Tracking Number: CXU-20260.

- In some cases, when power fails, the ArangoDB cluster does not form.

Workaround:

1. Log in to the centralinfravm3 VM.
2. Execute the following commands:  
  

```
service arangodb3.cluster stop
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```
3. Log in to the centralinfravm2 VM.
4. Execute the following commands:  
  

```
service arangodb3.cluster stop
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```
5. Log in to the centralinfravm1 VM.

6. Execute the following commands:

```
service arangodb3.cluster stop
cd /var/lib/arangodb3 && mv setup.json setup.json.old
```

7. On the centralinfravm1 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.
8. On the centralinfravm2 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.
9. On the centralinfravm3 VM, execute the **service arangodb3.cluster start** command and wait for 20 seconds for the command to finish executing.

Bug Tracking Number: CXU-20346.

- In a HA setup, if you shut down all the CSO servers, after the servers are restarted successfully, MariaDB and ArangoDB fail to form their respective clusters.

Workaround:

1. Perform a clean reboot of the central infrastructure VMs.
2. After the VMs have rebooted successfully, check the cluster health on the HAproxy page (<http://central-ip-address:1936>, where *central-IP-address* is the IP address of the VM that hosts the microservices for the central POP).
3. If the MariaDB and ArangoDB clusters are still down, you can recover the clusters by performing the following procedures:
  - To recover the MariaDB cluster, perform the following steps:
    - a. On the centralinfravm1 VM, execute the **service mysql stop** command.
    - b. On the centralinfravm2 VM, execute the **service mysql stop** command.
    - c. On the centralinfravm3 VM, execute the **service mysql stop** command.
    - d. On all three central infrastructure VMs, verify that the service has stopped executing the **service mysql status** command.
    - e. On the centralinfravm1 VM, start the service by executing the **service mysql start** command.
    - f. On the centralinfravm2 VM, start the service by executing the **service mysql start** command.

- g. On the centralinfravm3 VM, start the service by executing the **service mysql start** command.
- h. On all three central infrastructure VMs, verify that the service has started executing the **service mysql status** command.
- To recover the ArangoDB cluster, perform the following steps:
  - a. On the centralinfravm1 VM, execute the **service arangodb3.cluster stop** command.
  - b. On the centralinfravm2 VM, execute the **service arangodb3.cluster stop** command.
  - c. On the centralinfravm3 VM, execute the **service arangodb3.cluster stop** command.
  - d. On all three central infrastructure VMs, verify that the service has stopped executing the **ps -aef|grep arangodb** command.
  - e. On the centralinfravm1 VM, start the service by executing the **service arangodb3.cluster start** command.
  - f. On the centralinfravm2 VM, start the service by executing the **service arangodb3.cluster start** command.
  - g. On the centralinfravm3 VM, start the service by executing the **service arangodb3.cluster start** command.
  - h. On all three central infrastructure VMs, verify that the service has started executing the **ps -aef|grep arangodb** command.

Bug Tracking Number: CXU-21819.

- In a HA setup, if you onboard devices and deploy policies on the devices and if one of the policy deployments is in progress when a microservices or infrastructure node goes down, the deployment job is stuck in the **In Progress** state for about 90 minutes (the default timeout value), and you cannot perform deploy operations for the tenant for about 90 minutes.

Workaround: Wait for the job to fail and then redeploy the policy.

Bug Tracking Number: CXU-21922.

- If an infrastructure node goes down in a HA setup in which all nodes were previously up, and you create a firewall policy and try to deploy the policy, the deployment job is stuck in the in-progress state and a Redis timeout error is displayed in the job log.

Workaround:

1. Wait for approximately 90 minutes for the job to fail.
2. Bring up the infrastructure node that was down.
3. Redeploy the firewall policy.

Bug Tracking Number: CXU-24559.

- When you execute the **upgrade.sh** script to upgrade a setup running CSO Release 3.3.1 to CSO 4.0.0, the load service data operation fails and a **401, Authentication required** error is displayed in the upgrade log.

Workaround: On the installer VM, execute the **upgrade.sh** script again. The upgrade completes successfully.

Bug Tracking Number: CXU-24574.

## SD-WAN

- On the Site SLA Performance page, applications with different SLA scores are plotted at the same coordinate on the x-axis.

Workaround: None.

Bug Tracking Number: CXU-19768.

- When all local breakout links are down, site to Internet traffic fails even though there is an active overlay to the hub.

Workaround: None.

Bug Tracking Number: CXU-19807

- If the Internet breakout WAN link of the cloud 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.
- On the SD-WAN Events page, for link switch events, if you mouse over the **Reason** field, the values displayed for the SLA metrics are the ones that are recorded when the system logs are sent from the device and not the values for which the SLA violation was detected.

Workaround: None.

Bug Tracking Number: CXU-21461.

- In a hub-and-spoke topology with multi-tenancy enabled, when a spoke site is configured with two MPLS and two Internet links with MPLS selected as the default,

the traffic from the hub to the spoke site takes the same path instead of taking the path (link) on which the traffic was received by the hub (incoming WAN link). However, there is no traffic loss.

Workaround: Remove the static route with the next hop and replace it with a static route with the qualified next hop.

Bug Tracking Number: CXU-23197.

- If a WAN link on a CPE device goes down, the WAN tab of the *Site-Name* page (in Administration Portal) displays the corresponding link metrics as **N/A**.

Workaround: None.

Bug Tracking Number: CXU-23996.

- If a tenant has a real-time-optimized site, link switch events (on the Monitor page) might display the same WAN link for both source and destination tunnels.

Workaround: None.

Bug Tracking Number: CXU-24154.

## Security Management

- On the Active Database page in Customer Portal, the wrong installed device count is displayed. The count displayed is for all tenants and not for a specific tenant.

Workaround: None.

Bug Tracking Number: CXU-20531.

- If a cloud 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 cloud hub use the same type of authentication (either PKI or PSK) as the cloud 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.

- In the JIMS-to-CSO Configuration panel of the Identity Management page, if you try set a password for the Juniper Identity Management Service (JIMS) user and then save the password, an error message is displayed and the password is not saved.

Workaround: None.

Bug Tracking Number: CXU-24419.

- Even though SD-WAN, firewall, or SSL proxy policies are deployed successfully on the device, the CSO GUI incorrectly indicates that policies need to be deployed.

Workaround: None.

Bug Tracking Number: CXU-24628.

## Site and Tenant Workflow

- The tenant delete operation fails when CSO is installed with an external Keystone.

Workaround: You must manually delete the tenant from the Contrail OpenStack user interface.

Bug Tracking Number: CXU-9070

- If you try to activate a branch SRX Series device with the factory-default configuration, the stage-1 configuration commit might fail when there are active DHCP server bindings on the device. This is because of the default DHCP server settings present in factory-default configuration.

Workaround: When you are pre-staging the CPE device for activation, remove the DHCP server-related configuration from the device by executing the following commands on the Junos OS CLI:

```
set system services dhcp-local-server group jdhcp-group interface fxp0.0
set system services dhcp-local-server group jdhcp-group interface irb.0
```

Bug Tracking Number: CXU-13446

- In some cases, if automatic license installation is enabled in the device profile, after ZTP is complete, the license might not be installed on the CPE device even though license key is configured successfully.

Workaround: Reinstall the license on the CPE device by using the Licenses page on the Administration Portal.

Bug Tracking Number: PR1350302.

- For a tenant, LAN segments with overlapping IP prefixes across sites are not supported.

Workaround: Create LAN segments with unique IP prefixes across sites for the tenant.

Bug Tracking Number: CXU-20494.

- When the primary and backup interfaces of the CPE device uses the same WAN interface of the hub, the backup underlay might be used for Internet or site-to-site traffic even though the primary links are available.

Workaround: Ensure that you connect the WAN links of each CPE device to unique WAN links of the hub.

Bug Tracking Number: CXU-20564.

- After you configure a site, you cannot modify the configuration either before or after activation.

Workaround: None.

Bug Tracking Number: CXU-21165

- If you initiate the RMA workflow on an NFX Series device that was successfully onboarded and provisioned with stage-2 templates, the device RMA operation might get stuck in the device activation stage if the stage-2 configuration templates have interdependencies.

Workaround: Ensure that the stage-2 templates that are deployed on the device do not have interdependencies before initiating the device RMA workflow.

Bug Tracking Number: CXU-21464.

- On the **Monitor > Overview** page, if you click a site indicating that a major alarm was triggered (site icon color turns orange), and in the subsequent popup, click the link for major alarms in the **Alerts & Alarms** section, you are taken to the Alarms page. However, no alarm for the device is displayed.

Workaround: None.

Bug Tracking Number: CXU-21828.

- If a tenant is deleted and a different tenant is added with the same name as the previously deleted tenant, ZTP of the NFX Series spoke device fails during the VRR reconfiguration.

Workaround:

1. Delete the tenant.
2. Add the tenant with a name that is different from that of the deleted tenant.
3. Retry the ZTP workflow.

Bug Tracking Number: CXU-24260.

- On an NFX250 device, if you disable (detach) a failed service successfully and then try to delete the site, the delete site operation fails.

Workaround: None.

Bug Tracking Number: CXU-24355.

- When you try to activate a site with an SRX Series device, ZTP might fail with an error during the installation of the default trusted certificates.

Workaround: Retry the failed job after some time.

Bug Tracking Number: CXU-24487.

- If you try to delete a tenant that has custom roles defined, the delete tenant operation fails and an error message is displayed in the job log. In addition, though the job fails, the tenant might not be displayed in scope switcher or on the Tenants page.

Workaround: Delete the custom roles associated with the tenant and then trigger the tenant delete operation.

Bug Tracking Number: CXU-24655.

- If you try to activate a site with an MPLS link by using DHCP, the default route pointing to the MPLS gateway is added to the hub device, which results in Internet traffic from the hub taking the MPLS link.

Workaround: None.

Bug Tracking Number: CXU-24666.

- On the Import Sites page, the operation to import multiple sites by using a JSON file fails.

Workaround: Use the Sites page to create sites.

Bug Tracking Number: CXU-24730.

- For an NFX150 device in a hub-and-spoke topology, if you configure the LTE link for OAM traffic, ZTP might fail during the site activation task.

Workaround: Retry the failed job from the Jobs page, and the ZTP operation is successful.

Bug Tracking Number: CXU-24762.

- If you trigger the tenant creation workflow, the tenant might be displayed in the CSO GUI even before the job is completed. If you then try to trigger workflows for that tenant, the subsequent jobs fail because the tenant creation job is not completed.

Workaround: Wait for the tenant creation job to complete successfully before triggering any workflows for the tenant.

Bug Tracking Number: CXU-24783.

- If you provision a device, push a license on the device (by using CSO), and then try to delete the site (associated with the device), the operation to delete the site fails.

Workaround: Delete the license from the device (by using CSO) and then delete the site.

Bug Tracking Number: CXU-24790.

- The Configure Site operation for a cloud spoke site fails.

Workaround: None.

Bug Tracking Number: CXU-24795.

- If you try to delete an operating company that has custom roles defined, the delete operation fails. In addition, the operating company might not be displayed in scope switcher or on the Operating Companies (OpCos) page.

Workaround: Delete the custom roles associated with the operating company and then trigger the deletion of the operating company.

Bug Tracking Number: CXU-25062.



## General

- If you create VNF instances in the Contrail cloud by using Heat Version 2.0 APIs, a timeout error occurs after 120 instances are created.

Workaround: Contact Juniper Networks Technical Support.

Bug Tracking Number: CXU-15033

- When you upgrade the gateway router by using the CSO GUI, after the upgrade completes and the gateway router reboots, the gateway router configuration reverts to the base configuration and loses the IPsec configuration added during Zero Touch Provisioning (ZTP).

Workaround: Before you upgrade the gateway router by using the CSO GUI, ensure that you do the following:

1. Log in to the Juniper Device Manager (JDM) CLI of the NFX Series device.
2. Execute the **virsh list** command to obtain the name of the gateway router (*GWR\_NAME*).
3. Execute the **request virtual-network-functions *GWR\_NAME* restart** command, where *GWR\_NAME* is the name of the gateway router obtained in the preceding step.
4. Wait a few minutes for the gateway router to come back up.
5. Log out of the JDM CLI.
6. Proceed with the upgrade of the gateway router by using the CSO GUI.

Bug Tracking Number: CXU-11823.

- CSO might not come up after a power failure.

Workaround:

1. Log in to the installer VM.
2. Navigate to the **/root/Contrail\_Service\_Orchestration\_4.0.0/** directory.
3. Run the **reinitialize\_pods.py** script as follows:

```
./python.sh recovery/components/reinitialize_pods.py
```

4. SSH to the VRR by using the VRR IP address to check if you are able to access the VRR.

If there is an error in connecting (**port 22: Connection refused**), then you must recover the VRR by following step 5 through 21.

5. Log in to physical server hosting the VRR.

6. Execute the **virsh destroy vrr** command to destroy the VRR.



**WARNING:** Do not execute the **virsh undefine vrr** command because doing so will cause the VRR configuration to be lost and the configuration cannot be recovered.

7. Delete the VRR image that is located in the `/root/ubuntu_vm/vrr/vrr-15.1R6.7.qcow2` directory.

8. Copy the fresh VRR image from the `/root/disks/vrr-15.1R6.7.qcow2` directory to the `/root/ubuntu_vm/vrr/vrr-15.1R6.7.qcow2` directory.

9. Execute the **virsh start vrr** command and wait for approximately 5 minutes for the command to finish executing.

10. Execute the **virsh list --all** command to check if the VRR is running or not.

If the VRR is not running, check that the image that was copied was the uncorrupted image and re-try the steps from step 7.

11. If the VRR is running, navigate to the `/root/ubuntu_vm/vrr/` directory.

12. Run the **./vrr.exp** command to push the base configuration to the VRR.

13. Check if the VRR is reachable from the regional microservices VM. If the VRR is reachable, proceed to step 14. If the VRR is not reachable:

- a. Log in to the VRR.
- b. Check if the base configuration was pushed properly:
  - If the base configuration was pushed properly, re-check if the VRR is reachable from the regional microservices VM. If the VRR is reachable, proceed to step 14.
  - If the base configuration was not pushed properly:
    - i. Add the necessary routes to reach CSO.
    - ii. Re-check if the VRR is reachable from the regional microservices VM. If the VRR is reachable, proceed to 14.

14. Import the POP by using the URL `https://central-ms-ip:443/tssm/import-pop`, where *central-ms-ip* is the IP address of the central microservices VM.

15. Use POSTMAN to import the VRR.



**NOTE:** *Do not* import the VRR until the VRR is reachable from the regional microservices VM.

The following is the JSON format for the VRR. (In the JSON below, *<vrr-ip-address>* is the IP address of the VRR and *<vrr-password>* is the password that was configured for the VRR.

```
{
  "input": {
    "job_name_prefix":
    "ImportPop",
    "pop": [{
      "dc_name": "regional",
      "device": [{
        "name": "vrr-<vrr-ip-address>",
        "family": "VRR",
        "device_ip":
        "<vrr-ip-address>",
        "assigned_device_profile": "VRR_Advanced_SDWAN_option_1",
        "authentication": {
          "password_based": {
            "username": "root",
            "password": "<vrr-password>"
          },
          "management_state": "managed",
          "pnf_package": "null"
        },
        "name": "regional"
      }
    ]
  }
}
```

16. Verify whether the VRR is imported properly:
- Log in to the CSO Administration Portal.
  - Click **Resources > POPs > Import POPs > Import History** and confirm that the **ImportPop** job is running and that it has completed successfully.
17. On the Tenants page, add a tenant named **recovery**.
18. After the tenant is successfully created, log in to the VRR and access the Junos OS CLI.
19. Execute the **show configuration|display set** and verify that the tenant configuration (for the previously-configured tenants) is recovered.

20. Execute the **show bgp summary** and check that the BGP status to the hub and spokes are **Established**.

21. If the status is **Not Established**, add the routes for the OAM traffic of the hub and spokes to the VRR and recheck the status.

Bug Tracking Number: CXU-16530

- The provisioning of CPE devices fails if all VRRs within a redundancy group are unavailable.

Workaround: Recover the VRR that is down and retry the provisioning job.

Bug Tracking Number: CXU-19063

- The CSO health check displays the following error message: **ERROR: ONE OR MORE KUBE-SYSTEM PODS ARE NOT RUNNING**

Workaround:

1. Log in to the central microservices VM.
2. Execute the **kubectrl get pods --namespace=kube-system** command.
3. If the kube-proxy process is not in the Running state, execute the **kubectrl apply -f /etc/kubernetes/manifests/kube-proxy.yaml** command.

Bug Tracking Number: CXU-20275.

- After the upgrade, the health check on the standalone Contrail Analytics Node (CAN) fails.

Workaround:

1. Log in to the CAN VM.
2. Execute the **docker exec analyticsdb service contrail-database-nodemgr restart** command.
3. Execute the **docker exec analyticsdb service cassandra restart** command.

Bug Tracking Number: CXU-20470.

- The class-of-service scheduler configuration does not take effect on the CPE device.

Workaround:

1. Log in to the CPE device and access the Junos OS CLI.
2. Enable the scheduler map on each physical interface manually by executing the following commands:

```
set class-of-service interfaces interface-name unit * scheduler-map scheduler-map-name
set interfaces interface-name per-unit-scheduler
```

Where *interface-name* is the name of the physical interface (for example, ge-0/0/4), and *scheduler-map-name* is the name of the scheduler map.

3. Commit the configuration on the CPE device.

Bug Tracking Number: CXU-20708.

- The load services data operation or health check of the infrastructure components might fail if the data in the Salt server cache is lost because of an error.

Workaround: If you encounter a Salt server-related error, do the following:

1. Log in to the installer VM.
2. Execute the `salt '*' deployutils.get_role_ips 'cassandra'` command to confirm whether one or more Salt minions have lost the cache.
  - If the output returns the IP address for all the Salt minions, this means that the Salt server cache is fine; proceed to step 7.
  - If the IP address for some minions is not present in the output, this means that the Salt server has lost its cache for those minions and must be rebuilt as explained from step 3.
3. Navigate to the current deployment directory for CSO; for example, `/root/Contrail_Service_Orchestration_4.0.0/`.
4. Redeploy the central infrastructure services (up to the NTP step):
  - a. Execute the `DEPLOYMENT_ENV=central ./deploy_infra_services.sh` command.
  - b. Press Ctrl+c when you see the following message on the console:

```
2018-04-10 17:17:03 INFO utils.core Deploying roles set(['ntp']) to servers
['csp-central-msvm', 'csp-contrailanalytics-1', 'csp-central-k8mastervm',
'csp-central-infravm']
```

5. Redeploy the regional infrastructure services (up to the NTP step):
  - a. Execute the `DEPLOYMENT_ENV=regional ./deploy_infra_services.sh` command.

- b. Press Ctrl+c when you see a message similar to the one for the central infrastructure services.
6. Execute the **salt '\*' deployutils.get\_role\_ips 'cassandra'** command and confirm that the output displays the IP addresses of all the Salt minions.
7. Re-run the load services data operation or the health component check that had previously failed.

Bug Tracking Number: CXU-20815.

- In some cases, high values of round-trip time (RTT) and jitter are displayed in the CSO GUI because of high values reported in the device system log.

Workaround: None.

Bug Tracking Number: CXU-21434.

- On an NFX Series CPE device, if you try to upgrade a vSRX gateway router, the upgrade might fail due to a lack of storage space on the VM.

Workaround:

Before triggering the upgrade of the vSRX gateway router on an NFX Series device, perform the following steps:

1. Access the vSRX CLI on the NFX Series device.
2. Execute the **request system storage cleanup** command.
3. Access the JDM CLI on the NFX Series device.
4. Execute the **show virtual-network-function** command and note down the name of the vSRX gateway router VM.
5. Execute the **request virtual-network-function gwr-vm-name restart** command to reboot the VM, where *gwr-vm-name* is the name of the vSRX gateway router VM that was obtained in the preceding step.
6. Wait for the vSRX gateway router VM to successfully reboot.

Trigger the upgrade of the vSRX gateway router by using the CSO GUI.

Bug Tracking Number: CXU-21440.

- In some cases, when the infrastructure VMs in the CSO setup are unhealthy and you initiate the upgrade, the upgrade process fails to perform a health check before starting the upgrade.

Workaround: Recover the infrastructure VMs manually before proceeding with the upgrade.

Bug Tracking Number: CXU-21536.

- For an MX Series cloud hub device, if you have configured the Internet link type as OAM\_and\_DATA, the reverse traffic fails to reach the spoke device if you do not configure additional parameters by using the Junos OS CLI on the MX Series device.

Workaround:

- Log in to the MX Series device and access the Junos OS CLI.
- Find the **next-hop-service outside-service-interface** multiservices interface as follows:
  - Execute the **show configuration | display set | grep outside-service-interface** command.
  - In the output of the command, look for the multiservices (ms-) interface corresponding to the service set that CSO created on the device.

The name of the service set is in the format `ssettenant-name_DefaultVPN-tenant-name`, where *tenant-name* is the name of the tenant.

The following is an example of the command and output:

```
show configuration | display set | grep outside-service-interface
set groups mx-hub-Acme-Acme_DefaultVPN-vpn-routing-config services
service-set ssetAcme_DefaultVPN-Acme next-hop-service
outside-service-interface ms-1/0/0.4008
```

In this example, the tenant name is Acme and the multiservices interface used is ms-1/0/0.4008.

- After you determine the correct interface, add the following configuration on the device: **set routing-instances WAN\_0 interface *ms-interface*** where *ms-interface* is the name of the multiservices interface obtained in the preceding step.
- Commit the configuration.

Bug Tracking Number: CXU-21818.

- In Resource Designer, if you add a VNF that does not require a password and trigger the Add VNF Manager workflow, you are asked to enter a password even though the VNF does not require it.

Workaround: Even for VNFs that do not require a password, enter a dummy password in Resource Designer when you are creating a VNF package.

Bug Tracking Number: CXU-21845.

- In a full mesh topology, the simultaneous deletion of LAN segments on all sites is not supported.

Workaround: Delete LAN segments on one site at a time.

Bug Tracking Number: CXU-21936.

- When an SRX Series device with factory configuration is activated by using ZTP with a redirect server, the device activation fails because the learned phone home server is deleted during the activation process.

Workaround: Configure the phone home server IP address on the SRX Series device and retry the ZTP workflow.

Bug Tracking Number: CXU-22154.

- When you install the CSO Downloader app on MacOS, you might receive an error message indicating that the application cannot be opened because it is from an unidentified developer.

Workaround: Access the MacOS **Security & Privacy** settings and allow the CSO Downloader app to be opened and continue with the installation.

Bug Tracking Number: CXU-22661.

- In small deployments, in rare cases, the DNS lookup fails between microservices, which leads to job failures.

Workaround:

1. Access Kibana and check whether the following log is present: **Timeout while contacting DNS servers.**
2.
  - If the log is present:
    - a. Log in to the installer VM as root.
    - b. Run the `./python.sh recovery/components/reinitialize_pods.py` script from the same directory where the CSO package was extracted (untarred).
  - If the log is not present, contact Juniper Networks Technical Support.

Bug Tracking Number: CXU-23201.

- If you run the script to revert an upgraded CSO Release 4.0.0 setup to CSO Release 3.3.1, the revert operation fails because of an ArangoDB cluster error.

Workaround: Use the same workaround as CXU-20346.

Bug Tracking Number: CXU-23338.

- On a CSO setup with secure OAM configured, if you bring up the FortiGate VNF and then apply the license on the VNF, the VNF reboots. However, after rebooting, sometimes the VNF does not come back up.

Workaround: To ensure that the VNF comes back up, deactivate the VNF and then reactivate it by performing the following steps:



1. Log in to the JDM CLI of the NFX Series device and access configuration mode.
2. Deactivate the VNF by executing the **deactivate virtual-network-functions Fortinet-oob-2-Firewall** command.
3. Commit the changes by executing the **commit** command.
4. Rollback the changes by executing the **rollback 1** command
5. Commit the changes by executing the **commit** command.
6. Exit the configuration mode by executing the **quit** command.
7. Execute the **show virtual-network-functions** command and confirm that the status is **Running alive**, which means that the VNF is up.

Bug Tracking Number: CXU-23371.

- If one or more VRRs are down, jobs might take a long time to complete, or, in some cases, fail.

Workaround: Ensure that all VRRs are up before trying the Add Tenant or Add Site workflows.

Bug Tracking Number: CXU-23710.

- The image upgrade of the vSRX gateway router on NFX Series devices by using the CSO GUI is not supported.

Workaround: Upgrade the image by using the CLI of the NFX Series device.

Bug Tracking Number: CXU-23804.

- On an NFX Series device with a Ubuntu VNF instantiated, if you use SSH to log in to the VNF by using the loopback IP address (configured for secure OAM) with port 49154, the connection does not work.

Workaround:

1. Use SSH to log in to the vSRX gateway router by using the loopback IP address.
2. Use SSH to log in to the OAM IP address of the Ubuntu VNF with username **root** and password **passwOrd**.
3. In the Ubuntu VNF, add a route to the IP address of the machine from where you want to log in by using SSH.

You can now use SSH to log in from the configured machine by using the loopback IP address with port 49154.

Bug Tracking Number: CXU-23953.

- If all the infrastructure VMs are not up, then the downloading of generated reports fails.

Workaround: Ensure that all the infrastructure VMs are up and then download the generated reports.

Bug Tracking Number: CXU-24400.

- On an Ubuntu VNF spawned on an NFX150 device, the ping command to a website address (fully qualified domain name) does not work.

Workaround:

1. In Resource Designer, clone the existing ubuntu-fw-NFX150 template for the NFX150 device.
2. Edit the template and ensure that offloads are disabled for the **Left Interface**.
3. Click **Next** and complete the edit operation.

Bug Tracking Number: CXU-24441.

- If you are using the GUI installer to install CSO, sometimes the installation page freezes (percentage completion on the VMs does not change) during the installation because of a Rest API timeout.

Workaround: Reload the CSO installation page in the browser, which will update the status of the installation.

Bug Tracking Number: CXU-24471.

- When you reboot a device from the Tenant Devices or Devices page, the reboot job fails because connectivity is lost during the reboot.

Workaround: Check the operational status of the device on the Tenant Devices or Devices page. During the reboot phase, the operational status of the device is **Down**. After the device is successfully rebooted and connectivity is restored, the operational status of the device changes to **Up**. You can now trigger operations on the device by using the CSO GUI.

Bug Tracking Number: CXU-24512.

- If you try to modify a stage-2 configuration template that contains a password configuration, you are asked to reenter the password every time even if you do not want to set the password.

Workaround: In the Stage-2 Configuration Templates page (**Device Template > Stage-2 Config Templates**), ensure that the password configuration is moved to the bottom, and do not click the tab corresponding to the password configuration.

Bug Tracking Number: CXU-24531.

- If you are using the GUI installer to install CSO, sometimes the UI freezes during the installation and no installation progress is seen. However, the installation continues in the backend.

Workaround: Perform the following tasks:

1. Reload the installation UI page in the browser.  
If the UI page loads successfully, no further action is needed. If the UI page does not load, proceed to step 2.
2. Log in to the installer VM as root.
3. Kill the existing processes triggered by the GUI installer by executing the **kill \$(sudo lsof -t -i:8080)** command.
4. Navigate to the **/root/cso\_dl/Contrail\_Service\_Orchestration\_4.0.0/** directory.
5. Restart the Flask server by executing the **bash run\_ui.sh** command.
6. After you see the **==== INFO Installer App initialized =====** message on the console, reload the installation UI page in the browser.

Bug Tracking Number: CXU-24552.

- If all the infrastructure VMs are not up, reports cannot be generated.

Workaround: Restart the security management monitoring microservice:

1. Log in to the microservices VM as root.
2. Run the **kubectrl get pods | grep csp-secmgt-monitoring** command to determine the name of the pod for the security management monitoring microservice.
3. Restart the pod by executing the **kubectrl delete pod *pod-name*** command, where *pod-name* is the name of the microservices pod obtained in the preceding step.
4. Wait until the pod is in the **1/1 running** state.

You can now retry the report generation.

Bug Tracking Number: CXU-24560.

- If you try to onboard an NFX150 device with the Hybrid WAN CPE device template, the activation fails after the stage-1 configuration is deployed because connectivity to the device is lost.

Workaround: You must update the NAT rule configuration to re-enable connectivity between the device and CSO by performing the following steps:

1. After the stage-1 configuration is deployed, log in to the device.
2. Log in to the Junos OS CLI and access configuration mode.
3. Update the source NAT rule configuration on the device to add interface NAT. A sample configuration is shown below.

```
set security nat source rule-set deop1-1-lan-wan-ruleset from routing-instance trust
set security nat source rule-set deop1-1-lan-wan-ruleset to interface ge-1/0/1.0
set security nat source rule-set deop1-1-lan-wan-ruleset to interface ge-1/0/2.0
set security nat source rule-set deop1-1-lan-wan-ruleset to interface ge-1/0/9.0
set security nat source rule-set deop1-1-lan-wan-ruleset rule rule-WAN_0 match
source-address 0.0.0.0/0
set security nat source rule-set deop1-1-lan-wan-ruleset rule rule-WAN_0 then source-nat
interface
set security nat source rule-set deop1-1-lan-wan-ruleset rule rule-WAN_1 match
source-address 0.0.0.0/0
set security nat source rule-set deop1-1-lan-wan-ruleset rule rule-WAN_1 then source-nat
interface
```

Bug Tracking Number: CXU-24606.

- On a site with network segmentation enabled, if you add a new LAN segment and deploy it, the job is successful. However, the LAN segment's state remains **Configured** instead of **VPN Attached**.

Workaround: Redeploy the LAN segment and the state changes to **VPN Attached**.

Bug Tracking Number: CXU-24691.

- The CSO Downloader might not add the default route on the installer VM, if the installer VM is launched in a subnet that is different from the subnet in which the CSO servers are located.

Workaround: After the installer VM is spawned, add the default route on the installer VM by executing the **route add default gw ip-address adapter** CLI command, where *ip-address* is the address of the default gateway and *adapter* is the name of the network adapter. For example, **route add default gw 192.0.2.1 eth0**.

Bug Tracking Number: CXU-24697.

- When you use the CSO GUI installer, VRR behind NAT is not supported for small deployments. However, VRR behind NAT is supported for medium and large deployments using the CSO GUI, or for small, medium, or large deployments using the CLI installer.

Workaround: If you want to use the VRR behind NAT feature in a small deployment, use the CLI-based installer and not the GUI installer.

Bug Tracking Number: CXU-24699.

- If a user with an OpCo Admin role clones a device template and a tenant of that OpCo creates a site using the cloned device template, the site creation operation fails.

Workaround: Ensure that device templates are cloned or modified only by users with the SP Admin role.

Bug Tracking Number: CXU-24799.

- If the CSO GUI installer is used in the **custom install** mode and after CSO is successfully installed, you click the **Launch CSO Admin Portal** button, the installer tries to invoke Administration Portal by using the VRR IP address instead of the IP address of the central microservices VM.

Workaround: Use the IP address of the central microservices VM to launch Administration Portal in your browser.

Bug Tracking Number: CXU-24907.

- The Help (?) menu for the Administration Portal and Customer Portal is empty and does not display any links.

Workaround: Use the following links to access the Administration Portal and Customer Portal Help Centers:

- Administration Portal: [https://www.juniper.net/documentation/en\\_US/cso4.0/help/information-products/pathway-pages/admin-portal-index.html](https://www.juniper.net/documentation/en_US/cso4.0/help/information-products/pathway-pages/admin-portal-index.html)
- Customer Portal: [https://www.juniper.net/documentation/en\\_US/cso4.0/help/information-products/pathway-pages/customer-portal/cp-index.html](https://www.juniper.net/documentation/en_US/cso4.0/help/information-products/pathway-pages/customer-portal/cp-index.html)

You can also use the **More...** hyperlink on a page to access the online help content for that page.

Bug Tracking Number: CXU-24941.

## Resolved Issues

---

The following issues are resolved in Juniper Networks CSO Release 4.0.0.

- After an SD-WAN CPE device is activated by using ZTP, you must install APBR licenses and application signatures before deploying SD-WAN policies through the Administration Portal GUI.

Bug Tracking Number: CXU-14799.

- Hybrid-WAN and SD-WAN deployments using the same MX as a hub is not supported.

Bug Tracking Number: CXU-16547.

- When you are creating an SLA Profile and want to specify the advanced configuration, then you must specify maximum upstream rate, maximum upstream burst size, maximum downstream rate and maximum downstream burst size.

Bug Tracking Number: CXU-17735.

- For an AWS spoke, during the activation process, the device status on the Activate Device page is displayed as **Detected** even though the device is down.

Bug Tracking Number: CXU-19779.

- On the **Monitor > Overview** page, if you select a cloud hub site and access the **WAN** tab, an error message is displayed.

Bug Tracking Number: CXU-20353.

- In the bandwidth-optimized SD-WAN mode, when the same SLA is used in the SD-WAN policy for different departments and an SLA violation occurs, two link switch events that appear identical, because the department name is missing from the event details, are displayed.

Bug Tracking Number: CXU-20529.

- On the SD-WAN Policy page, if you click the up or down arrow to reorder a policy intent, then the policy intent moves to the top of the list instead of moving one intent above or below respectively. In addition, when you click **Deploy**, the changes are not deployed to the device.

Bug Tracking Number: CXU-20861.

- If you restart a central microservices VM or the **csp.secmgt-sm** Kubernetes pod on a central microservices VM when the deployment of a firewall policy or NAT policy is in progress, the deployment job fails.

In addition, after the restart is completed, if you modify the firewall or NAT policy, the changes fail to deploy.

Bug Tracking Number: CXU-21106.

- In a tenant with real-time-optimized SD-WAN, the duration of the link switch violation (on the **WAN** tab of the *Site-Name* page) might be displayed incorrectly.

Bug Tracking Number: CXU-21590.

- The connection of the Celery worker to RabbitMQ might be lost in some cases, such as the shutdown of the infrastructure VM, pool network, or high load on the infrastructure VMs. After the broken connection is detected, Celery is restarted. However, if an exception takes place during the restart, then the Celery worker loses the connection to RabbitMQ.

Bug Tracking Number: CXU-21823.

- In a full mesh topology, if a site uses the same underlay to connect to a site and a hub, the link score of the overlay between the site and the hub is displayed as poor instead of N/A (not applicable).

Bug Tracking Number: CXU-21824.

- A user with the Tenant Administrator role cannot install application signatures on the devices belonging to a tenant.

Bug Tracking Number: CXU-22064.

- If you try to delete the SLA profile associated with the SD-WAN policy immediately after deleting the SD-WAN policy, then an error message might be displayed and the SLA profile is not deleted.

Bug Tracking Number: CXU-22168.

- The rollback operation on a CSO setup configured on an ESXi server fails.

Bug Tracking Number: CXU-22288.

- The upgrade of Network Service Controller fails.

Bug Tracking Number: CXU-22345.

## Documentation Updates

---

This section lists the errata and changes in the CSO Release 4.0.0 documentation:

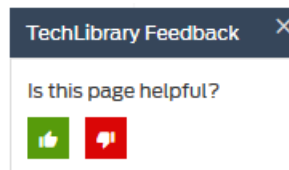
- From CSO Release 4.0.0, the following new guides are available:
  - *CSO Installation and Upgrade Guide*
  - *CSO Monitoring and Troubleshooting Guide*
- The installation and upgrade information, which was previously a part of the *CSO Deployment Guide*, is moved to the *CSO Installation and Upgrade Guide*.

## 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](mailto: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

---

28 January 2019—Revision 7, CSO Release 4.0.0

24 October 2018—Revision 6, CSO Release 4.0.0

27 July 2018—Revision 5, CSO Release 4.0.0

20 July 2018—Revision 4, CSO Release 4.0.0

6 July 2018—Revision 3, CSO Release 4.0.0



6 July 2018—Revision 2, CSO Release 4.0.0

30 June 2018—Revision 1, CSO Release 4.0.0

Copyright © 2019 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.