

# Contrail Service Orchestration Release Notes

Release 4.1.1  
22 August 2019  
Revision 3

These Release Notes accompany Release 4.1.1 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes contain installation and upgrade information, and describe new and changed features, limitations, and known and resolved issues in the software.

<b>Contents</b>	<b>Introduction   3</b>
	<b>Installation and Upgrade   5</b>
	Software Downloads   6
	Installation Instructions   8
	Software Installation Requirements for NFX Series Network Services Platform   9
	Upgrade Instructions   9
	Installation and Upgrade Limitations   9
	Post-Installation, Post-Upgrade Instructions and Notes   10
	<b>New and Changed Features in Contrail Service Orchestration Release 4.1.1   10</b>
	<b>Servers, Software, and Network Devices Tested   10</b>
	<b>Hardware, Software, and Virtual Machine Requirements for CSO   11</b>
	<b>VNFs Supported   11</b>
	<b>Licensing   12</b>
	<b>Accessing the CSO GUIs   13</b>
	<b>Known Behavior   13</b>
	Device Management   13
	AWS Spoke   14
	Dynamic VPN (DVPN)   15
	Policy Deployment   15
	SD-WAN   16
	Security Management   17

Site and Tenant Workflow	17
Topology	18
User Interface	19
General	19
Known Issues	22
Audit Logs	23
AWS Spoke	24
CSO High Availability	24
SD-WAN	28
Security Management	30
Site and Tenant Workflow	31
General	34
Resolved Issues	41
Documentation Updates	43
Documentation Feedback	43
Requesting Technical Support	44
Self-Help Online Tools and Resources	44
Creating a Service Request with JTAC	45
Revision History	45

# 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 4.1.1 is a secure software-defined WAN (SD-WAN) solution that builds on the existing capabilities of CSO and the Cloud CPE solution.

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 4](#) 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 a Hub and Spoke SD-WAN Deployment
Small	10 VNFs	Up to 500, 2 VNFs per site	Up to 500
Medium	100 VNFs, 20 VNFs per Contrail compute node	Up to 3500, 2 VNFs per site	Up to 3500
Large	500 VNFs, 20 VNFs per Contrail compute node	Up to 6000, 2 VNFs per site	Up to 6000

The following table provides the number of sites and tunnels supported by full-mesh deployments:

**Table 2: Number of Sites, Tenants, and Tunnels Supported for a Full-Mesh SD-WAN Deployment**

Description	Scale
Number of full-mesh DVPN tunnels supported per tenant	50000
Number of full-mesh DVPN tunnels supported across a CSO installation	125000
Number of full-mesh tenants qualified across a CSO installation	200 tenants with 10 sites per tenant
Number of full-mesh sites qualified for a given tenant	250 sites

Table 2: Number of Sites, Tenants, and Tunnels Supported for a Full-Mesh SD-WAN Deployment (*continued*)

Description	Scale
Maximum number of events per second that can be processed by SD-WAN log processing	90000
Number of tunnels supported on NFX250	600 tunnels
Number of tunnels supported on SRX4100 and SRX 4200	1500 tunnels

## Installation and Upgrade

### IN THIS SECTION

- [Software Downloads | 6](#)
- [Installation Instructions | 8](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 9](#)
- [Upgrade Instructions | 9](#)
- [Installation and Upgrade Limitations | 9](#)
- [Post-Installation, Post-Upgrade Instructions and Notes | 10](#)

You can install CSO by using a GUI-based installer as well as through the 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

Table 3 on page 6 displays the supported versions and download links for CSO Release 4.1.1 and associated software components. We recommend that you use the CSO Downloader to download and install CSO.

**Table 3: CSO and Associated Software Components**

Product	Supported Version	Download Link
CSO Downloader (available for Windows, MacOS, and Linux Desktop versions)	4.1.1	<a href="https://www.juniper.net/support/downloads/?p=cso">https://www.juniper.net/support/downloads/?p=cso</a>
Contrail Service Orchestration	4.1.1	<a href="https://www.juniper.net/support/downloads/?p=cso">https://www.juniper.net/support/downloads/?p=cso</a>
Juniper Identity Management Service (JIMS)	1.1.1.R1	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	4.1.2.0-171	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>

Table 3: CSO and Associated Software Components (*continued*)

Product	Supported Version	Download Link
NFX150 CPE device	Junos OS Release 18.2X85D11	<ul style="list-style-type: none"> <li>• Install Media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88051.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88051.html</a></li> <li>• Install Package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87999.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87999.html</a></li> </ul>
NFX250 CPE device	Junos OS Release 15.1X53-D497	<ul style="list-style-type: none"> <li>• Install Media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88050.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88050.html</a></li> <li>• Install Package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87998.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87998.html</a></li> </ul>
SRX Series devices	Junos OS Release 15.X49-D172	<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/92321.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92321.html</a></li> <li>• SRX1500: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html</a></li> <li>• SRX1500 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html</a></li> <li>• SRX1500 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html</a></li> <li>• SRX4100, SRX4200: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html</a></li> <li>• SRX4100, SRX4200 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html</a></li> <li>• SRX4100, SRX4200 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html</a></li> </ul>

Table 3: CSO and Associated Software Components (*continued*)

Product	Supported Version	Download Link
vSRX	Junos OS Release 15.1X49-D172	<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/92328.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92328.html</a></li> <li>• vSRX (KVM appliance): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92331.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92331.html</a></li> <li>• vSRX (Hyper-V image): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92332.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92332.html</a></li> <li>• vSRX (VMware appliance with SCSI virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92330.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92330.html</a></li> <li>• vSRX (VMware appliance with IDE virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92329.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92329.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 4.1.1, 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 4.1.1 only from CSO Release 4.0.2.

If your installed version of CSO is not Release 4.0.2, then you must perform a fresh installation of CSO Release 4.1.1.

If your installed version is CSO Release 4.0.2, you can use a script (**upgrade.sh**) to directly upgrade to CSO Release 4.1.1. If the upgrade is unsuccessful, you can roll back to CSO Release 4.0.2.

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.
- The VM on which the virtual route reflector (VRR) is installed supports only one management interface.

## Post-Installation, Post-Upgrade Instructions and Notes

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.
- To use full capabilities of CSO Release 4.1.1, we recommend that you upgrade the sites by using the site upgrade workflow, to Release 4.1.1.
- After you upgrade a site, delete and recreate the SD-WAN policies other the ones that use local breakout. For local breakout policies, create a local breakout profile.
- After you upgrade CSO to Release 4.1.1, existing SD-WAN policies are shown as undeployed in the CSO UI even though the policies are still active and deployed.

## New and Changed Features in Contrail Service Orchestration Release 4.1.1

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 4.1.1. For new and changed features in CSO Release 4.1.0, see the CSO 4.1.0 Release Notes at [https://www.juniper.net/documentation/en\\_US/cso4.1/information-products/topic-collections/release-notes/4.1.0/index.html](https://www.juniper.net/documentation/en_US/cso4.1/information-products/topic-collections/release-notes/4.1.0/index.html).

- **Ability to attach Zscaler with any interface of a site that has local breakout enabled**—Starting from CSO Release 4.1.1 onward, for tenants that use PKI authentication, Zscaler can be attached to any interface that has local breakout enabled. Previously, if the tenants were using PKI authentication, Zscaler could be attached only to an interface that was configured for exclusive local breakout.

## Servers, Software, and Network Devices Tested

For information about servers, software, and network devices tested, see the *Hardware and Software Tested for Contrail Service Orchestration* topic in the [Installation and Upgrade Guide](#)

# Hardware, Software, and Virtual Machine Requirements for CSO

For information about hardware, software, and virtual machine requirements, see the *Minimum Requirements for Servers and VMs* topic in the [Installation and Upgrade Guide](#).

## VNFs Supported

CSO supports the Juniper Networks and third-party VNFs listed in [Table 4 on page 11](#).

**Table 4: VNFs Supported by Contrail Service Orchestration**

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	For Hybrid WAN and SD-WAN deployments:  vSRX KVM Appliance 15.1X49-D172	<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>• Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.</li> <li>• Centralized deployment</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

Table 4: VNFs Supported by Contrail Service Orchestration (*continued*)

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
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 *Contrail Services Orchestration (CSO) GUIs* topic in the [CSO Deployment Guide](#).

## Known Behavior

### IN THIS SECTION

- [Device Management | 13](#)
- [AWS Spoke | 14](#)
- [Dynamic VPN \(DVPN\) | 15](#)
- [Policy Deployment | 15](#)
- [SD-WAN | 16](#)
- [Security Management | 17](#)
- [Site and Tenant Workflow | 17](#)
- [Topology | 18](#)
- [User Interface | 19](#)
- [General | 19](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 4.1.1.

## Device Management

- The SRX4100 and SRX4200 devices supports all existing SD-WAN features, except the following:

- Phone home client—The CPE devices must be manually activated by copying the stage-1 configuration from the Administration Portal, pasting it to the console of the SRX4100 and SRX4200 devices, and then committing the stage-1 configuration.
- LTE and xDSL interfaces.
- Service chaining.

## 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.D170. 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.

## Dynamic VPN (DVPN)

- The 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 taken into account 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.
- The 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 expire because of inactivity in 60 seconds and that causes CSO to close the corresponding sessions and trigger **APPTRACK\_SESSION\_CLOSE** messages. The **APPTRACK\_SESSION\_CLOSE** messages are tracked by Contrail Analytics Node (CAN), and are added to the number of sessions closed. The sessions closed count is used to calculate the DVPN delete threshold.
- Site-to-Site DVPN tunnels fail to establish if the CPE is behind a NAT device.
- DVPN tunnels between spoke sites and indirect gateway sites cause asymmetric traffic.

## 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

- 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 intents 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.
- Between spoke 1 (attached to the cloud hub) and spoke 2 (attached to the cloud hub and the gateway site), traffic occurs in the following paths:
  - From spoke 1 to spoke 2, forward traffic goes through the cloud hub (to spoke 2) and reverse traffic goes through the gateway site (to spoke 1).
  - From spoke 2 to spoke 1, forward traffic goes through the gateway site (to spoke 1) and the reverse traffic goes through the cloud hub to spoke 2.
- Default application traffic profile parameters will get modified during CSO upgrade.
- 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.
- Use breakout profiles to define all types of static SD-WAN policies.
- In a CSO Release 4.1.1 setup that has been upgraded from a CSO Release 4.0.2 setup, you cannot use a static SLA defined from the **SD-WAN > Application SLA Profiles** page when you create an SD-WAN policy that has application set to ANY. In such cases, use breakout profile of type Backhaul, which can be defined from the **SD-WAN > Breakout Profiles** page.
- 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.
- 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 source interface same as the destination interface.
- Sometimes duplicate link switch events are displayed on the Link Switch Events page.



## 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.
- Ensure that tenants use unique site names so that no two tenants have sites with the same name.
- Though the tenant creation workflow UI supports negative values for the Max Tunnels per Tenant parameter, always ensure that you use a positive value for the Max Tunnels per Tenant parameter.
- 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 or later, 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.

- 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
```

- 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*
- Before you onboard a cloud hub with PKI as the VPN authentication method, ensure that the NTP server is configured on the device. After the device is onboarded, add the NTP server details manually on the cloud hub or in the stage-2 configuration.

Before you upgrade a site, ensure that you configure NTP server details on the device manually or in the stage-2 configuration.

## 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.

## 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
1loOYS6n9l0WDZcxXYWWeINlu6zOSilZYVIIdwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

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

## General

- Installer VM needs to be rebooted after you upgrade CSO to Release 4.1.0.
- 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.

- Ensure that you enable port number 443, which is required for phone home services and device activation. In previous releases, port number 444 was supported for phone home services and device activation.
- The following are the limitations of doing image upgrade from the Image Landing page:

- JDM images cannot be upgraded parallelly. The upgrade have to be done in a sequence because the connection to CSO gets reestablished when the primary JDM reboots and that affects the upgrade operation of the other JDM.
- GWR cluster nodes should not be upgraded (neither parallelly nor sequentially) from the Image Landing page because the cluster nodes should always run the same version.

We recommend that you use the Site Upgrade workflow which handles the image upgrade of both JDM and GWR cluster appropriately

- 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\_4.1.1/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 from the Image Landing page is not supported.

Workaround: Upgrade the image by using the Site Upgrade workflow from the Site Landing Page.

- LAN routes are not advertised to the neighbor in case of a data center deployment on a gateway site that uses routing protocols such as BGP or OSPF. In such cases, configure source NAT on the gateway site from the CSO UI or configure reverse routes on the routing device.
- Overlapping LAN segments are not supported across a CSO installation.

## Known Issues

### IN THIS SECTION

- [Audit Logs | 23](#)
- [AWS Spoke | 24](#)
- [CSO High Availability | 24](#)
- [SD-WAN | 28](#)
- [Security Management | 30](#)
- [Site and Tenant Workflow | 31](#)
- [General | 34](#)

This section lists known issues in Juniper Networks CSO Release 4.1.1.

## Audit Logs

- For purge audit log job, the recurrence is not working as expected.

Workaround: Schedule separate jobs for each of the recurring instances.

Bug Tracking Number: CXU-32608

- Run Now option does not work when you try to select the option while editing a scheduled purge audit log to run immediately.

Workaround:

- Create a new job and select the Run Now option.

or

- While editing a scheduled job to run immediately, instead of using the Run Now option, modify the schedule to use the current time.

Bug Tracking Number: CXU-32604

- The audit log does not contain job IDs for the following tasks:

- Reboot
- License push

You can view the job details from the Jobs page.

Workaround: For license push jobs, you can use the license name and the timestamp from the audit logs to view the corresponding job details from the Jobs page.

Bug Tracking Numbers: CXU-29488

- Addition and deletion of mesh tags are not captured in the DVPN audit logs.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32252

## 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 High Availability

- In an HA setup, when one of the CAN nodes is down, some of the widgets do not show link metrics.

Workaround: Restart the CAN node to view link metrics for all widgets.

Bug Tracking Number: CXU-30813

- In an HA setup, if CAN has gone down because of a power outage, the contrail-database-nodemgr in Analyticsdb remains in down state even after CAN comes back online. In such cases, you see the following status:

```
root@canvm2:~# docker exec -it analyticsdb contrail-status
== Contrail Database ==
contrail-database: active

contrail-database-nodemgr initializing (Cassandra state detected DOWN. )
kafka active

cassandra is detected down in database-nodemgr so please recover Casandra in it
and start the workflows
```

Workaround: Run the nodetool repair and make sure that Cassandra is up and running.

Bug Tracking Number: CXU-32214



- In an HA setup, some of the virtual route reflectors (VRRs) are incorrectly reported as down even though those VRRs are up and running. This problem occurs because some of the alarms that are generated when VRRs are down after a power failure fail to be cleared even after the VRRs come back online.

Workaround: Though this issue does not have any functional impact, we recommend that you restart the VRR to clear the alarms.

Bug Tracking Number: CXU-31448

- In an HA setup, with three load-balancer VMs, if the primary load balancer goes down, one of the remaining load-balancer VMs is switched over as the primary. However, after the original load-balancer VM comes up, it is switched over as the primary again.

Workaround: There is no functional impact and no known workaround.

Bug Tracking Number: CXU-15441

- After a power failure, CAN installed on a physical server does not come up online correctly.

Workaround:

Follow these steps to restore CAN installed on a physical server:

1. Log in to the CAN server and **scp** the **/root/can\_bkp** folder to installer VM.
2. Reimage the server.
3. Navigate to the **Contrail\_Service\_Orchestration\_4.1.1** folder.
4. Execute **DEPLOYMENT\_ENV=central ./deploy\_infra\_services.sh** on installer VM until it starts deploying NTP.
5. Execute **salt '\*'contrail\*' network.hw\_addr eth0**.
 

```
csp-contrailanalytics-3.4D5UTX.central: 52:54:00:2c:a6:4d
csp-contrailanalytics-1.4D5UTX.central: 52:54:00:2b:4f:da
csp-contrailanalytics-2.4D5UTX.central: 52:54:00:ea:ee:67
```
6. Open **deployments/central/roles.conf**. Search for can1, can2 and can3. Make sure that the MAC addresses listed in (4) matches the field **hardware\_address** for each of can1, can2 and can3.
7. Open **deployment/central/topology.conf**, and edit servers under **[TARGETS] servers =**

```
csp-contrailanalytics-1, csp-contrailanalytics-2, csp-contrailanalytics-3.
```
8. Execute **DEPLOYMENT\_ENV=central ./deploy\_infra\_services.sh**.
9. Check health of CAN by executing **./components\_health.sh**.

10. To restore the data back, copy the backed up **can\_bkp** folder from installer VM to the respective CAN servers under **root/**.

11. Execute the following steps on all three CAN servers:

- a. `root@sspt-ubuntu5-vm7:~# docker exec controller service cassandra stop`
- b. `root@sspt-ubuntu5-vm7:~# docker exec analyticsdb service cassandra stop`
- c. `root@sspt-ubuntu5-vm7:~# docker exec -it controller bash`
- d. `root@sspt-ubuntu5-vm7(controller):/var/lib/cassandra# rm -rf *`
- e. `root@sspt-ubuntu5-vm7(controller): exit`
- f. `root@sspt-ubuntu5-vm7:~# docker exec -it analyticsdb bash`
- g. `root@sspt-ubuntu5-vm7(analyticsdb):/var/lib/cassandra# rm -rf *`
- h. `root@sspt-ubuntu5-vm7(analyticsdb): exit`
- i. `root@sspt-ubuntu5-vm7:~# cd can_bkp/analyticsdb_old/`
- j. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp commitlog/analyticsdb:/var/lib/cassandra`
- k. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp data/analyticsdb:/var/lib/cassandra`
- l. `root@sspt-ubuntu5-vm7:~/can_bkp/analyticsdb_old/cassandra# docker cp saved_caches/analyticsdb:/var/lib/cassandra`
- m. `root@sspt-ubuntu5-vm7:~# cd can_bkp/controller_old/`
- n. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp commitlog/controller:/var/lib/cassandra`
- o. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp data/controller:/var/lib/cassandra`

- p. `root@sspt-ubuntu5-vm7:~/can_bkp/controller_old/cassandra# docker cp saved_caches/controller:/var/lib/cassandra`
- q. `root@sspt-ubuntu5-vm7:~# docker exec controller chown -R cassandra:cassandra /var/lib/cassandra/`
- r. `root@sspt-ubuntu5-vm7:~# docker exec analyticsdb chown -R cassandra:cassandra /var/lib/cassandra/`
- s. `root@sspt-ubuntu5-vm7:~# docker exec analyticsdb service cassandra start`
- t. `root@sspt-ubuntu5-vm7:~# docker exec controller service cassandra start`

12. Check health of CAN by executing `./components_health.sh`.

- 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_4.1.1/`.
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

## SD-WAN

- SD-WAN policies that use the Cloud-Zscaler profile fails to deploy if the traffic type traffic profile Internet is not enabled.

Workaround: Create a custom cloud breakout profile and use it instead of the default cloud breakout profile in the SD-WAN policy.

Bug Tracking Number: CXU-35901

- Traffic from a spoke site that has a dynamic SLA policy enabled and is connected to an MX Series device functioning as a cloud hub device takes asymmetric paths, that is different paths for upstream and downstream.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32506

- The firewall policy status changes to undeployed after the create DVPN and certificate renewal events even though the policy remains active on devices.

Workaround: No workaround required as the functionality is not affected.

Bug Tracking Number: CXU-32464

- Class-of-service configuration is not deployed if the gateway site has only a data center department.

Workaround: Deploy at least one department other than the data center department on the gateway site and apply SD-WAN policies for the department.

Bug Tracking Number: CXU-30365

- The tenant name appears as default project when you generate a report based on the predefined template, SD-WAN Performance Report.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-31653

- On gateway site, when there are no non-datacenter departments, 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-datacenter department with a LAN segment is deployed on Gateway site.

Bug Tracking Number: CXU-31365

- SD-WAN deployment policy job may fail if policy intent involves datacenter department or department without any LAN segment. This does not impact SD-WAN policy deployment for other sites.

Workaround: Use more specific SD-WAN intents, with department or department with site, to exclude datacenter departments and departments without LAN segments.

Bug Tracking Number: CXU-31313

- In a bandwidth-optimized, hub-and-spoke topology where network segmentation is enabled, a new LAN segment that has an existing department added to it might cause a deploy job to fail.

Workaround: Delete the LAN segment and retry the deploy job. If there are policy dependencies, remove the dependencies before you delete the LAN segment.

Bug Tracking Number: CXU-25968

- OAM configurations remain on an MX Series device that you have deactivated as cloud hub from CSO.

Workaround: Manually remove the configuration from the device.

Bug Tracking Number: CXU-25412

- When the WAN link endpoints are of different types and if overlay tunnels are created based on matching mesh tags, the static policy for site-to-site or central Internet breakout traffic might give preference to the remote link type instead of the local link type.

Bug Tracking Number: CXU-28358

- 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
- 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 you delete a cloud hub that is created in Release 3.3.1, CSO does not delete the stage-2 configuration.

Workaround: You must manually delete the stage-2 configuration from the device.

Bug Tracking Number: CXU-25764

## Security Management

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

Workaround: From the device, configure the EWF Server with the 116.50.57.140 IP address 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

- 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

- 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

- The UTM policy configuration is not deployed on an SD-WAN site with the SRX device model SRX345-DUAL-AC.

Workaround:

1. Add the SRX345-DUAL-AC device model to the schema file.

**NOTE:** In the schema-svc docker, the schema file is available at /opt/csp-schema-data/\*configuration.json.

2. Restart the pod.

Bug Tracking Number: CXU-25706

## Site and Tenant Workflow

- After you do an RMA for a site, alarms for Zscaler tunnels may not work.

Workaround: Recreate the Zscaler tunnels from **Configuration > SD-WAN > Breakout Profiles > Cloud Breakout** settings.

Bug Tracking Number: CXU-36000

- If the PKI server used by a tenant fails, you cannot renew or revoke the certificates that are used by the sites or create new sites for the tenant.

Workaround: Delete the tenant and create a new tenant with the new PKI server credentials.

Bug Tracking Number: CXU-35644

- After you upgrade CSO from Release 4.0.2 to Release 4.1.1, RMA does not work for sites that are not upgraded to Release 4.1.1.

Workaround: Delete the device from the site and add that back to the site.

Bug Tracking Number: CXU-35049

- After you upgrade CSO to Release 4.1.1, hybrid WAN CPEs show a major alarm.

Workaround: Upgrade the sites that show the alarm to CSO Release 4.1.1.

Bug Tracking Number: CXU-34162

- For centralized deployments, site status is shown as down. However, there is no impact to the traffic and the VNF is operational.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32663

- After a revert action following an upgrade failure or backup restore, the user is unable to onboard tenants. This problem occurs because sometimes after the revert action, the csp-service-lookup fails as flannel is unable to provide subnet lease.

Workaround: Run **service flanneld restart** on all microservices VMs.

Bug Tracking Number: CXU-32110

- On a site deployed with only application-specific breakout policies (that is, no breakout policy is configured for ANY application), traffic fails when all overlay tunnels are down.

Workaround: Deploy a breakout policy for "ANY" application.

Bug Tracking Number: CXU-28436

- During site activation, activation of NFX250 dual CPE connected to MX series cloud hub device may fail with the following error message: **No existing device\_initiated device connection.**

Workaround: Retry the failed ZTP job from the administration portal.

Bug Tracking Number: CXU-27902

- After a site upgrade, status of policies that are associated with the site appears as pending deployment even though they are already deployed.

Workaround: Trigger a policy deployment job to deploy the policies. CSO does not deploy the policies unless there are updates to the policy, but the status of policies are appropriately updated after you run a deployment job.

Bug Tracking Number: CXU-27528

- If you create a new tenant with the name of a tenant that was deleted, certain inconsistencies such as policy deployment failure are noticed.

Workaround: When you create a tenant, ensure that you do not use the same name as that of a deleted tenant.

Bug Tracking Number: CXU-26886

- Site upgrade for hub sites that were created using custom device profile or cloned device profile is incomplete.

Workaround:

- After the upgrade, go to tssm core docker by entering the following command: **docker exec -it *docker name* bash**
- In the docker run the following command: **root@csp:/# cd /opt/meta\_data/**
- From /opt/meta\_data, run **cp SRX\_Advanced\_SDWAN\_HUB\_option\_1\_upgrade.yaml custom\_device\_profile\_upgrade.yaml**

Bug Tracking Number: CXU-26532

- 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

- On an NFX250 device, if you disable (detach) a failed service successfully and then try to delete the site, the site is not deleted.

Workaround: None.

Bug Tracking Number: CXU-24355

- 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

- 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

- The Configure Site operation fails if you import a cloud hub with a name that is different from that of other tenants.

Workaround: While you are importing a cloud hub, specify the same name that is used while onboarding a cloud hub for a global service provider.

Bug Tracking Number: CXU-25740

- You cannot configure a site with dual CPE devices if WAN links are used exclusively for local breakout traffic.

Workaround: While you are creating a site and enabling the link for local breakout, instead of selecting the **Use only for breakout traffic** option, select **Use for breakout & WAN** traffic. Also, while you are configuring a site ensure that the WAN link is connected to a hub.

Bug Tracking Number: CXU-25776

## General

- You cannot reboot a single node in an SRX cluster device.

Workaround: Wait for 10 minutes and retry the operation.

Bug Tracking Number: CXU-36844

- SRX cluster deletion fails and returns the following error message:  
**/var/db/scripts/event/load-recovery.slax: Permission denied.** This problem occurs if **load-recovery.slax** is present on the device.

Workaround: Before you delete an SRX cluster, rename the **load-recovery.slax** file on both the devices on the cluster.

To rename the file:

1. Log in to the SRX cluster device.
2. To go to **/var/db/scripts/event**, enter the following command:  
**cd /var/db/scripts/event**
3. Rename **load-recovery.slax**. For example:

**mv load-recovery.slax load-recovery.slax.old**

4. Repeat these steps on both the nodes.

Bug Tracking Number: CXU-36384

- CSO UI navigation becomes slow or unresponsive for 8 to 10 minutes when a server fails.

Workaround: Wait for 10 minutes and retry the operation.

Bug Tracking Number: CXU-35769

- Unable to deploy new VRR after CSO is upgraded to 4.1.1.

Workaround: Copy **vrr,baseMs** and **Baseinfra** images from the **CSO/artifacts** directory to **/var/www/html/csp\_components** before you try to deploy the new VRR..

Bug Tracking Number: CXU-33967

- Status of the pods appear as Unknown or Pending instead of Running.

Workaround: Run the **reinitialize\_pods.py** script. The script calculates the pod count per node and if the pod count is not properly distributed across the nodes, deletes and redeploys services, pods, and deployments.

Bug Tracking Number: CXU-32574

- ZTP for SRX 3xx devices may fail during the default trust certificate installation.

Workaround: Because default trust certificates are used for application firewall, which is not a supported feature on SRX300 and SRX320 devices, disable installation of default trust certificates in the device template for SRX300 and SRX320 devices.

For SRX 340 and 345 devices, retry the failed ZTP job. If application firewall is not required, you can consider disabling the installation of default trust certificates for SRX340 and SRX345 as well.

Bug Tracking number: CXU-32627

- LAN segments added after a site is activated are not monitored for alarm events. Because of this, link down events for the LAN port are not reported by CSO.

Workaround: Add LAN segments while you create a site.

Bug Tracking Number: CXU-32508

- Information related to deleted VMs remains on an ESXi server.

Workaround: Before you install CSO on an ESXi server, manually delete any VM folder that is available under **/vmfs/volumes/datastore/vm\_folder**.

Bug Tracking Number: CXU-32337

- When you delete a tenant in CSO without deleting the corresponding virtual user account in the JIMS server, JIMS keeps attempting CSO authorization for the deleted tenant. Authorization failures are recorded in the CSO audit logs. This causes spamming of the CSO audit logs and might cause deterioration of database performance.

Workaround: Before you delete a tenant from CSO, delete information specific to that tenant from JIMS.

Bug Tracking Number: CXU-32315

- If a restore operation fails, even subsequent attempts from a healthy backup fail and return the following error message:

```
BNR: ERROR : RESTORE FAILED. DISCONTINUED FURTHER PROCESSING.
BNR: ERROR: RUN HEALTHCHECK USING 'cso_backuprestore -b health check'
FIX ALL ISSUES AND RETRY RESTORE.
```

Workaround:

1. Run a health check: **cso\_backuprestore -b health check**.
2. Fix any components that are in stopped or failing state.
3. When CSO is in healthy state, run the restore operation again.

Bug Tracking Number: CXU-32064

- When you configure a site for SRX Series devices, the stage-1 configuration might fail if you use the fully qualified domain name (FQDN) for NTP server configuration.

Workaround: Use the IP address of the NTP server instead of its FQDN.

Bug Tracking Number: CXU-31415

- The LAN segment state is changed to *VPN attached* if the LAN segment deployment failed because of network connectivity issues.

Workaround: Delete and redeploy the LAN segment after you resolve the network connectivity issue.

Bug Tracking Number: CXU-31039

- Signature installation fails on some sites when you attempt to install signatures on more than a hundred sites in a single deploy job.

Workaround: Install signatures separately on the site where the installation failed.

Bug Tracking Number: CXU-28923

- The Revert to Default function does not restore default APN settings if the SIM is already connected to a network with a custom APN.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-28724

- MySQL fails to come back online after an abnormal shutdown or restart of an infrastructure VM.

Workaround: Run the following script:

`root@installervm:~/Contrail_Service_Orchestration_4.1.1# ./recovery.sh` and select **1** from the options.

Bug Tracking Number: CXU-32046

- Images and licenses that customers uploaded are lost during a disaster recovery.

Workaround: Upload the images and licenses again.

Bug Tracking Number: CXU-31533

- Reverting from CSO Release 4.1.0 to Release 4.0.2 fails because the controller container on the `contrail_analytics` node is in Exited mode.

Workaround:

1. Log in to the CAN VM.
2. Run `docker ps-a`.
3. If the status of the controller container is Exited, run `docker restart controller`.

Bug Tracking Number: CXU-31469

- Importing POP or onboarding tenants remain In Progress state for long and fail.

Workaround: Clear data files in `/var/lib/zookeeper/version-2` and restart zookeeper.

Bug Tracking Number: CXU-29856

- If multiple sites are using the same MX series cloud hub, IPSec overlay tunnels for some of the WAN links may fail to come up and show the following error: **Negotiation failed with error code NO\_PROPOSAL\_CHOSEN received from peer (5 times)**.

Workaround: Clear the IPSec session from the connected MX series cloud hub by executing the `clear services ipsec-vpn ipsec security-associations` command.

Bug Tracking Number: CXU-27638

- ZTP for SRX devices fails. This problem occurs if the SRX device was connected to clients on the LAN side before ZTP and has bindings that are not cleared during ZTP.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-27376

- On an Ubuntu VNF spawned on an NFX250 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-NFX250` template for the NFX250 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-24985

- 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

- 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

- 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 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_4.1.1/`**.
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

- 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:

1. Log in to the MX Series device and access the Junos OS CLI.
2. Find the **next-hop-service outside-service-interface** multiservices interface as follows:
  - a. Execute the **show configuration | display set | grep outside-service-interface** command.
  - b. 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.

3. 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.

4. 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

- 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

- When you reboot a device from the Tenant Devices or Devices pages, the reboot job fails because the 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

- For an NFX250 device, the Ubuntu VNF service chain configuration is incorrect if you set `SINGLE_SSH_TO_NFX` to False and then instantiate a service.

Workaround: None.

Bug Tracking Number: CXU-25018

- An error occurs while EEPROM contents for copper ports are being read.

Workaround: None.

Bug Tracking Number: PR1372217

- Because of insufficient buffer size, vSRX performs queue scheduling incorrectly and drop packets.

Workaround: Set the buffer size to 3000 microseconds by executing the **set class-of-service schedulers scheduler-name buffer-size temporal 3000** command.

Bug Tracking Number: PR1361720.

## Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 4.1.1:

- Status of an overlay link is not always updated in the WAN tab of the Site page.

Bug Tracking Number: CXU-32812

- For sites that were provisioned in Release 4.0.2 and upgraded to 4.1.0, the Create and Delete threshold values for DVPN tunnels are shown as undefined in the WAN tab of the Site page

Bug Tracking Number: CXU-32753

- Post site upgrade on NFX150-S1E, ge-1/0/8 fails to initialize.

Bug Tracking Number: CXU-32747

- Site upgrade job remains in the In Progress state.

Bug Tracking Number: CXU-32643

- Sometimes, sites created with PKI may fail to activate.

Bug Tracking Number CXU-32350

- For dual CPE sites activated in 4.1.0 and for older sites that were activated in 4.0.2, sites column in the alarms page does not provide the site name. The site name, however, is shown in the description column and also in the detailed alarm view.

Bug Tracking Number: CXU-32681

- During CSO installation from the installer UI, infrastructure services deployment returns the following error message and fails:

```
Hostname not pingable locally in server csp-installer-vm.  
Please setup hostname correctly.
```

Bug Tracking number: CXU-32721

- SLA and DVPN reports do not contain data for tenants that have bandwidth-optimized SD-WAN deployments.

Bug Tracking Number: CXU-32496

- The job log does not state why remote archiving of logs failed if the log archiving failed because of an incorrect path. This issue occurs while doing audit log purge with remote archiving.

Bug Tracking Number: CXU-32454

- WAN links for an NFX250 site that is upgraded to Release 4.1.0 and has local breakout enabled, appear in red in the WAN tab of the Site page.

Bug Tracking Number: CXU-32450

- When there are multiple breakout rules that apply to any application (when the ANY option is selected), even if you delete one of the rules, the corresponding configuration is not removed from the device.

Bug Tracking Number: CXU-32380

- SD-WAN policies fail to deploy if a site is not upgraded from CSO Release 4.0.2 to CSO Release 4.1.0.

Bug Tracking Number: CXU-32289

- After power shutdown of servers, SD-WAN site configuraton fails because of issues with arangodb.

Bug tracking number: CXU-32169

- Dual CPE site is shown as down after site upgrade.

Bug Tracking Number: CXU-31941

- Source tunnel information is missing for SD-WAN link switch events when traffic switches:
  - From the overlay tunnel toward the gateway or hub to site-to-site DVPN tunnels.

- From site-to-site DVPN tunnels to the overlay tunnel toward the gateway or hub.

Bug Tracking Number: CXU-31714

- Stage-1 configuration on an NFX Series device might fail if no OAM-and-data link is configured during site configuration.

Bug Tracking Number: CXU-31304

- On the Audit Logs page, the Username and Role columns do not display the actual name and the role of the user, respectively. Instead, the name of the user is displayed as Admin and role of the user is displayed as \_member\_admin.

Bug Tracking Number: CXU-25189

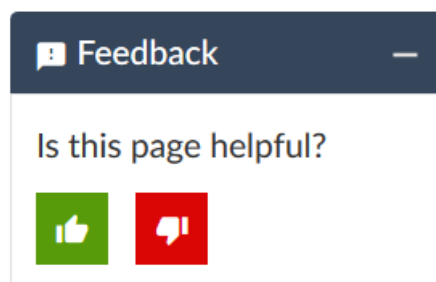
## Documentation Updates

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

## 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

15 July 2019—Revision 1, CSO Release 4.1.1

8 August 2019—Revision 2, CSO Release 4.1.1

22 August 2019—Revision 3, CSO Release 4.1.1

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.