

Contrail Service Orchestration Release Notes

Release 5.1.2
21 August, 2020
Revision 3

These Release Notes accompany Release 5.1.2 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction | 3

Software Support | 3

Software Downloads | 3

Software Installation Requirements for NFX Series Network Services Platform | 8

Installation and Upgrade Instructions | 9

New and Changed Features in Contrail Service Orchestration Release 5.1.2 | 9

VNFs Supported | 9

Licensing | 10

Accessing the CSO GUIs | 10

Known Behavior | 11

Install and Upgrade | 11

Device Management | 11

Dynamic VPN (DVPN) | 12

Policy Deployment | 13

SD-WAN | 13

SD-LAN | 14

Security Management | 14

Site and Tenant Workflow | 14

Topology | 15

User Interface | 15

General | 15

Known Issues | 16

SD-WAN | 17

SD-LAN | 18

CSO High Availability | 19

Security Management | 25

Site and Tenant Workflow | 26

General | 26

Resolved Issues | 30

Documentation Feedback | 31

Requesting Technical Support | 32

Self-Help Online Tools and Resources | 32

Creating a Service Request with JTAC | 33

Revision History | 33

Introduction

You can deploy CSO Release 5.1.2 on-premises only.

CSO Release 5.1.2 supports the following types of accounts:

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

There are no new features in CSO Release 5.1.2.

Software Support

IN THIS SECTION

- [Software Downloads | 3](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 8](#)
- [Installation and Upgrade Instructions | 9](#)

Software Downloads

[Table 1 on page 4](#) displays the supported versions and download links for software components associated with CSO Release 5.1.2.

NOTE:

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.

Table 1: Software Components Associated with CSO Release 5.1.2

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.5R1	Pre-bundled with CSO.
EX Series switches	Junos OS Release 18.4R2 Junos OS Release 18.4R3	Junos OS Release 18.4R2 <ul style="list-style-type: none"> • EX2300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300 • EX3400: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300 • EX4300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93859.html?pf=EX4300 • EX4600: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93861.html?pf=EX4600 • EX4650: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93900.html?pf=EX4650 Junos OS Release 18.4R3 <ul style="list-style-type: none"> • EX2300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101422.html?pf=EX2300 • EX3400: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101422.html?pf=EX3400 • EX4300: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101391.html?pf=EX4300 • EX4600: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101393.html?pf=EX4600 • EX4650: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/101432.html?pf=EX4650

Table 1: Software Components Associated with CSO Release 5.1.2 (continued)

Product	Supported Version	Download Link
NFX150 CPE device	Junos OS Release 19.3R2-S3	<ul style="list-style-type: none"> Junos OS 19.3R2-S3 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110795.html?pf=NFX150 Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110724.html?pf=NFX150
NFX250 CPE device	Junos OS Release 18.4R3-S3 Junos OS Release 19.3R2-S3 for vSRX	<ul style="list-style-type: none"> Junos OS Release 18.4R3-S3 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109826.html?pf=NFX250 Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/109672.html?pf=NFX250
SRX Series CPE devices	Junos OS Release 19.3R2-S3	SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices): <ul style="list-style-type: none"> Junos OS 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110749.html?pf=SRX300
SRX Series Next-Generation Firewall devices	Junos OS Release 19.3R2-S3	SRX300, SRX320, SRX340, SRX345, and SRX550: <ul style="list-style-type: none"> Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110749.html?pf=SRX300

Table 1: Software Components Associated with CSO Release 5.1.2 (continued)

Product	Supported Version	Download Link
SRX Series Provider Hub device	Junos OS Release 19.3R2-S3	<p>SRX1500</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500 <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100
SRX Series Enterprise Hub devices	Junos OS Release 19.3R2-S3	<ul style="list-style-type: none"> SRX4100, SRX4200: <ul style="list-style-type: none"> Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110750.html?pf=SRX4100 Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110779.html?pf=SRX4100 SRX1500: <ul style="list-style-type: none"> Junos OS Release 19.3R2-S3 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110748.html?pf=SRX1500 Junos OS Release 19.3R2-S3 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110778.html?pf=SRX1500

Table 1: Software Components Associated with CSO Release 5.1.2 (continued)

Product	Supported Version	Download Link
vSRX for SD-WAN devices	Junos OS Release 19.3R2-S3	<p>For hub devices and spoke devices:</p> <ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110842.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110851.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110850.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110853.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110852.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.1.2 (*continued*)

Product	Supported Version	Download Link
vSRX for next-generation firewall devices	Junos OS Release 19.3R2-S3	<ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110842.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110851.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110850.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110853.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S3: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110852.html?pf=vSRX

NOTE: For limitations and caveats related to devices, see [Device Management on page 11](#) in the Known Behavior section.

Software Installation Requirements for NFX Series Network Services Platform

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

1. Upload the software image to CSO.

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

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

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

Installation and Upgrade Instructions

NOTE: You can upgrade to CSO Release 5.1.2 only from CSO Release 4.1.2. If your installed version of CSO is not Release 4.1.2, then you must perform a fresh installation of CSO 5.1.2.

For more information on installation and upgrade instructions, see the [Installation and Upgrade Guide](#).

New and Changed Features in Contrail Service Orchestration Release 5.1.2

There are no new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.1.2. To view and read the features that are available in CSO Release 5.1.1, see [CSO Release 5.1.1 Release Notes](#).

VNFs Supported

CSO supports the VNFs listed in [Table 2 on page 10](#).

Table 2: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX	For Hybrid WAN and SD-WAN deployments: Junos OS Release 19.3R2-S3	<ul style="list-style-type: none"> • Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM) 	Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.
Ubuntu	16.04		Hybrid WAN and SD-WAN (all LAN-side functions) deployments–NFX250 and NFX150 platforms.
Fortinet	5.6.3		Hybrid WAN and SD-WAN (all LAN-side functions) deployments–NFX250 and NFX150 platforms.

Licensing

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

Accessing the CSO GUIs

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

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

Known Behavior

IN THIS SECTION

- [Install and Upgrade | 11](#)
- [Device Management | 11](#)
- [Dynamic VPN \(DVPN\) | 12](#)
- [Policy Deployment | 13](#)
- [SD-WAN | 13](#)
- [SD-LAN | 14](#)
- [Security Management | 14](#)
- [Site and Tenant Workflow | 14](#)
- [Topology | 15](#)
- [User Interface | 15](#)
- [General | 15](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.1.2.

Install and Upgrade

- After you upgrade CSO from Release 4.1.2 to Release 5.1.2, the new functionality for the site is available only after you upgrade the site.
- While you upgrade from CSO Release 4.1.2 to CSO Release 5.1.2, MariaDB might fail to restore at the first attempt. MariaDB is restored successfully in the next attempt.

Device Management

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

- Phone-home client (PHC)—The devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX4100 and SRX4200 devices, and then committing the stage-1 configuration.
- LTE and xDSL interfaces.
- In a dual SRX Series cluster, the devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX Series device, and then committing the configuration.
- LTE and xDSL interfaces are not supported for dual CPE devices.
- xDSL interfaces are not supported for an NFX250 device with Junos OS Release 18.4R3.3.
- You cannot remotely access a cloud spoke device and edit the configuration.
- You can install and use only an external LTE Vodafone K5160 dongle to the NFX250 device.
- DVPN is not supported for cloud spoke sites.
- NFX150 is not supported in cluster mode.
- PHC is supported for EX2300, EX3400, and EX4300 switches (except EX4300-MP) with Junos OS Release 18.4R2 and later. The CSO release is qualified for Junos OS Release 18.3R1, and the PHC capability is currently not supported for EX Series switches that are onboarded with Junos OS Release 18.3R1.

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

- Performance of SSL proxy may not be as expected on SRX300 and SRX320 devices.
- Class-of-service (CoS) configuration on Layer 2 interfaces (*ge-0/0/port number*) is not supported on NFX150 CPE devices.
- Do not zeroize EX2300 and EX3400 devices as doing so might result in unexpected behavior.
- Service chaining is not supported for an NFX150 device with Junos OS Release 19.3R2-S3.

Dynamic VPN (DVPN)

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

- DVPN create and delete thresholds are based on the **APPTRACK_SESSION_CLOSE** messages. When **APPTRACK_SESSION_CLOSE** messages reach the specified threshold, an alarm is generated for creating or deleting a DVPN tunnel. However, the alarms are not cleared until the **APPTRACK_SESSION_CLOSE** message count goes below the threshold (for create alarms) or above the threshold (for delete alarms) to trigger a fresh cycle. This causes the create and delete alarms to remain active and prevent further alarms and to, thus, slow down the creation or deletion of tunnels.
- Passive probes created by an SD-WAN policy time out because of inactivity in 60 seconds. This causes CSO to close the corresponding sessions and trigger **APPTRACK_SESSION_CLOSE** messages. The **APPTRACK_SESSION_CLOSE** messages are tracked and added to the number of sessions closed. The sessions closed count is used to calculate the DVPN delete threshold.

Policy Deployment

- An SD-WAN policy deployment is successful even if there is no matching WAN link meeting the SLA. This is expected behavior and it ensures that when a WAN link matching the SLA becomes available, traffic is routed through that link.
- The policy intents defined for a firewall or an SD-WAN policy must not have conflicts with other policy intents in that policy because such conflicts lead to inconsistent behavior. For example:
 - You cannot define an SD-WAN policy with one policy intent for application X and SLA profile S-1 and another policy intent for application X and SLA profile S-2.
 - You cannot define two firewall policy intents with the same source and destination endpoints but one with action Allow and another with action Deny.

SD-WAN

- If WAN link endpoints are not of similar type but overlay tunnels are created based on matching mesh tags, the static policy for site-to-site or central Internet breakout traffic gives preference to the remote link type.
- Advanced SLA configurations, such as CoS rate limiting, are not supported during local breakout if no specific application is selected; that is, if Application is set to ANY. Choose specific applications if you want to enable advanced SLA configurations, such as CoS rate limiting.
- If two or more SD-WAN policy rules are configured for the same application with different levels of granularity, such as all, sites, and departments, then CSO applies the CoS rate limiter in the same order in which you have created the intents.

SD-LAN

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

Security Management

- UTM Web filtering is not supported in an active-active SRX Series cluster device.

Site and Tenant Workflow

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

To specify a root password for the device:

1. Log in to Administration Portal.
 2. Select **Resources > Device Templates**.
 3. Select the device template and click **Edit**.
 4. Specify the plain text root password in the **ENC_ROOT_PASSWORD** field.
 5. Click **Save**.
- When you try to deploy a LAN segment on an SRX Series spoke device, the CSO GUI allows you to select more than one port for a LAN segment. However, for SRX Series devices, only one port for a LAN segment can be deployed; multiple ports in a LAN segment can be deployed only on NFX Series devices.
 - On a site with an NFX Series device, if you deploy a LAN segment without the VLAN ID specified, CSO uses an internal VLAN ID meant for internal operations and this VLAN ID is displayed in the LAN section of the Site Detail View page. There is no impact on the functionality.
 - Do not create departments that have names starting with **default**, **default-reverse**, **mpls**, **internet**, or **default-hub** because CSO uses the following departments for internal use:

- `Default-vpn_name`
- `Default-reverse-vpn_name`
- `mpls-vpn_name`
- `internet-vpn_name`
- `Default-hub-vpn_name`

Topology

- The time take to upgrade a site or an image is dependant on the time taken to copy the image to a device. To reduce the time, ensure that you stage the image before you upgrade a site or an image.

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 fails.

General

- On an NFX Series device:

- To activate a virtualized network function (VNF), perform the following steps:
 1. Add the VNF to the device.
 2. Initiate the activation workflow and ensure that the job is 100% completed.
- To retry the activation of a VNF that failed, perform the following steps:
 1. Deactivate the VNF.
 2. Remove the VNF.
 3. Add the VNF to the device.
 4. Initiate the activation workflow and ensure that the job is 100% completed.
- Class-of-service (CoS) configuration on Layer 2 interfaces (*ge-0/0/port number*) is not supported on NFX150 CPE devices.
- Enterprise hub is not supported for cloud spoke sites.
- CSO internally uses IP addresses starting from 100.112.0.0 through 100.127.255.255. You must avoid using these IP addresses in LAN subnets.
- NFX250 uses some IP addresses in the 192.0.2.0/24 subnet for VNF management. You must avoid using these IP addresses in LAN. For more information on the usage of this subnet, see the [NFX250 documentation](#).

Known Issues

IN THIS SECTION

- [SD-WAN | 17](#)
- [SD-LAN | 18](#)
- [CSO High Availability | 19](#)
- [Security Management | 25](#)
- [Site and Tenant Workflow | 26](#)
- [General | 26](#)

This section lists known issues in Juniper Networks CSO Release 5.1.2.

SD-WAN

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

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

Bug Tracking Number: CXU-21291

- After you upgrade from CSO Release 4.1.1 to CSO Release 5.1.2, the Firewall Policy and SDWAN policy pages show incorrect count for undeployed intents.

Workaround: Modify the policy and redeploy.

Bug Tracking Number: CXU-45171

- After you delete the last LAN segment of a site, you cannot view the WAN links on **Monitor > Geographic Map** and **Site Management > Site Site-Name > WAN** pages. This issue is applicable *only* to sites that are added before upgrading to CSO Release 5.1.2, and not for the sites that are added after you upgrade to CSO Release 5.1.2.

Workaround: Add a LAN segment and redeploy.

Bug Tracking Number: CXU-48454

- For an SD-WAN site with a Zscaler tunnel, if the IKE source IP address for Zscaler tunnels is a pool of IP addresses and if you reboot the spoke device, the Zscaler tunnel may fail to come up.

Workaround: Re-apply the configuration for Zscaler groups on the device.

Bug Tracking Number: CXU-47338

- You cannot upgrade an enterprise hub site if one of the enterprise hubs is not reachable and is in the configured state.

Workaround: Upgrade the enterprise hub site after deleting the enterprise hub that is not reachable and is in the configured state.

Bug Tracking Number: CXU-50060

SD-LAN

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

Workaround:

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

Bug Tracking Number: CXU-39629

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

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

Bug Tracking Number: CXU-42865

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

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

Bug Tracking Number: CXU-40647

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-42866

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

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

Bug Tracking Number: CXU-42181

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

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

Bug Tracking Number: CXU-38994

CSO High Availability

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

Workaround: Contact JTAC for the recovery procedure.

Bug Tracking Number: CXU-43001

- When the virtual route reflector (VRR) is down or not reachable from CSO, you cannot delete a site or tenant from CSO.

Workaround: Recover the VRR and retry deleting the site or tenant.

Bug Tracking Number: CXU-43724

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

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

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

Bug Tracking Number: CXU-42125

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

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

Bug Tracking Number: CXU-42965

- While you are installing CSO 5.1.2, the Contrail_analytics component is reported as unhealthy when you run the **deploy.sh** script for the first time.

Workaround:

1. Reboot the Contrail Analytics Node and wait for around 10 minutes.
2. Run the **./components_health.sh** script to check the health of the components.
3. If all components are healthy, then run the following commands:

```
./python.sh micro_services/deploy_micro_services.py
```

```
./python.sh micro_services/load_services_data.py
```

Bug Tracking Number: CXU-48269

- After you reboot the server, the docker containers within the Contrail Analytics Node are not started.

Workaround:

To restart the docker containers:

1. Run the **sudo fsck /dev/vda1** command.
2. Reboot the Contrail Analytics Node.
3. After you reboot the server, check the status of the docker container by running the **docker ps** command.
4. To ensure all services inside the Contrail Analytics Node are proper, run the **components_health.sh** script from the CSO folder in the startup server.

Bug Tracking Number: CXU-48126

- When you reboot a server, the status of all microservices is initially displayed as pending. Only when the node is ready, the status of the microservices is changed to Running . However, the secmgmt and monitoring pods are occasionally not up and running.

Workaround: Restart the pods manually by running the **kubectrl delete pods pod-name -n** command.

Bug Tracking Number: CXU-48125

- When you reboot a server, if you run the **kubectrl get nodes** command, the status of all nodes is displayed as Not Ready. This is because the docker containers in the infraservices or microservices are not automatically started and the status is displayed as Loaded.

Workaround: To bring back the node status to Ready, log in to the infraservices or microservices node, and run the following commands:

```
rm -f /var/lib/docker/network/files/local-kv.db
```

```
service docker start
```

Bug Tracking Number: CXU-48027

- After you reboot the server, a few pods in kube-system are in the Crashloop Backoff state.

Workaround: You must replace the entire k8 master node.

1. Log in to the startup server.
2. From the CSO folder, run the **./deploy.sh -r replace_vm** command.

3. Select the appropriate k8 virtual machine, which is corrupted and must be replaced.
4. After the virtual machine is spawned, run the following command from the startup server to ensure all the pods are in theRunning state:

```
root@startupserver1:~/Contrail_Service_Orchestration_5.1.2# kubectl get pods -n kube-system -o wide
```

Bug Tracking Number: CXU-46754

- After you reboot the server, ArangoDB gets corrupted and the arangodb3 service will not be in the Running state.

Workaround: Log in to Infra Node and execute the following commands:

```
cd /mnt/data/arangodb3/cluster/dbserver8530/data/engine-rocksdb/journals
mkdir -p /mnt/data/arango/
mv * /mnt/data/arango/archive1
systemctl start arangodb3.service
```

Bug Tracking Number: CXU-47812

- The installation of CSO Release 5.1.2 fails while you are configuring Contrail Analytics Node.

Workaround: On the startup server, run the following commands and rerun the `./deploy.sh` script:

```
salt -C "G@roles:contrail_analytics" state.apply contrail_analytics.post_configure saltenv='central'
salt 'contrail_analytics1' cmd.run "server-manager provision --cluster_id demo-cluster
contrail_networking_docker --no_confirm"
```

Bug Tracking Number: CXU-48745

- After you reboot the BareMetal servers, occasionally Contrail Analytics Node processes are not running as expected.

Workaround:

- If there is an NTP Server-related issue, run the following command on the CSO installer VM:

```
salt *contrail* state.apply ntp saltenv=central
```

- If there is a RabbitMQ-related issue, run the following commands on all three Contrail Analytics Nodes:

```
docker exec -it controller bash
service rabbitmq-server stop
ps -ef | grep epmd
rm -rf /var/lib/rabbitmq/mnesia/
service rabbitmq-server start
```

docker restart analytics && docker restart analyticsdb && docker restart controller

Bug Tracking Number: CXU-48572

- After you reboot the startup server, the status of some pods (for example, etcd , kube-api and so on) in kube-system and infra node is displayed as CrashLoopBackOff.

Workaround: You need to replace the k8 master node.

1. Log in to startup server.
2. From the CSO folder, run the following command:

```
./deploy.sh -r replace_vm
```

3. Select the appropriate k8 VM or the infra node that is corrupted and must be replaced.
4. After the VM is spawned, run the following command from startup server to ensure all the pods are in the Running state:

```
root@startupserver1:~/Contrail_Service_Orchestration_5.1.2# kubectl get pods -n kube-system -o wide
```

Bug Tracking Number: CXU-46754

- After you reboot one of the startup servers, the Add Site or Delete Site workflows might fail with the following error:

vhost '/' is down or inaccessible.

Workaround: Restart all RabbitMQ pods sequentially. Log in to the startup server and run the following commands:

```
kubectl delete pod rabbitmq-ha-0 -n infra
```

```
kubectl delete pod rabbitmq-ha-1 -n infra
```

```
kubectl delete pod rabbitmq-ha-2 -n infra
```

Bug Tracking Number: CXU-46490

- During the server reboot, for a considerable time the status of the Calico pod is displayed as the following:

```
calico-node-65dbg 0/1 Init:0/3 0. (or) calico-node-hzcsh 0/1 CrashLoopBackOff
```

This is because the IP_AUTODETECTION_METHOD environment variable not set.

Workaround: Reboot the server again.

Bug Tracking Number: CXU-44871

- You cannot view the latest csplogs in Kibana.

Workaround:

1. On the installer VM, navigate to the CSO 5.1.2 directory.
2. Replace content in the **deployments/central/file_root/elk_elasticsearch/configs/csplogs_template.json** file with the following:

```
{
  "order" : 0,
  "template" : "csplogs-",
  "settings" : {
    "index" : {
      "refresh_interval" : "30s",
      "number_of_replicas": "{{no_of_es_nodes}}"
    }
  },
  "mappings" : {
    "default" : {
      "dynamic_templates" : [ {
        "message_field" : {
          "mapping" : {
            "fielddata" : false,
            "index" : "analyzed",
            "omit_norms" : true,
            "type" : "text"
          },
          "match_mapping_type" : "string",
          "match" : "message"
        }
      }, {
        "string_fields" : {
          "mapping" : {
            "fielddata" : false,
            "index" : "not_analyzed",
            "omit_norms" : true,
            "type" : "keyword"
          },
          "match_mapping_type" : "string",
          "match" : ""
        }
      } ],
    "_all" : {
      "omit_norms" : true,
      "enabled" : true
    },
    "properties" : {
      "@timestamp" : {
```

```

"type" : "date"
},
"geoip" : {
  "dynamic" : true,
  "properties" : {
    "ip" : {
      "type" : "ip"
    },
    "latitude" : {
      "type" : "float"
    },
    "location" : {
      "type" : "geo_point"
    },
    "longitude" : {
      "type" : "float"
    }
  }
},
"@version" : {
  "index" : "not_analyzed",
  "type" : "keyword"
},
"Thread_id" : {
  "index" : "not_analyzed",
  "type" : "keyword"
},
"large_text" : {
  "index" : "no",
  "type" : "keyword"
},
"request" : {
  "index" : "analyzed",
  "type" : "text"
},
"request_id" : {
  "index" : "analyzed",
  "omit_norms" : true,
  "type" : "text"
},
"task_id" : {
  "index" : "analyzed",
  "omit_norms" : true,
  "type" : "text"
}

```



```

    },
    "url" : {
      "index" : "analyzed",
      "omit_norms" : true,
      "type" : "text"
    }
  }
},
"aliases" : { }
}

```

3. Open **upgrade_logstash.sls** in the **deployments/central/file_root/upgrade/** folder, and replace **^-Xmx3g** with **^-Xmx2g**.
4. Run the following command:

```
salt -C "G@roles:elk_logstash" state.apply upgrade.upgrade_elk_logstash saltenv='central'
```

Bug Tracking Number: CXU-49881

Security Management

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

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

Bug Tracking Number: CXU-23107

- If UTM Web-filtering categories are installed manually (by using the **request system security UTM web-filtering category install** command from the CLI) on an NFX150 device, the intent-based firewall policy deployment from CSO fails.

Workaround: Uninstall the UTM Web-filtering category that you installed manually by executing the **request security utm web-filtering category uninstall** command on the NFX150 device and then deploy the firewall policy.

Bug Tracking Number: CXU-23927

Site and Tenant Workflow

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

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

Bug Tracking Number: CXU-42985

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

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

Bug Tracking Number: CXU-43024

General

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

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

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

Bug Tracking Number: CXU-32731

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

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

Bug Tracking Number: CXU-39167

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

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

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

Bug Tracking Number: CXU-35450

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41210

- On an SRX Series device, the deployment fails if you use the same IP address in both the Global FW policy and the Zone policy.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41259

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

Workaround: Reboot the device.

Bug Tracking Number: CXU-41922

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

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

Bug Tracking Number: CXU-41666

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

NOTE: You cannot add Tenant-owned Public IP pool after you create an SD-WAN site for the tenant.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41139

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

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

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

1. Navigate to the **/etc/apt** directory and execute the following commands:

- **cp sources.list sources.list.cso**
- **cp orig-sources.list sources.list**

2. Install the **python2.7-dev** script by running the following commands:

- **apt-get update && apt-get install python2.7-dev**

- `cp sources.list.cso sources.list`

3. Navigate to the `/root/Contrail_Service_Orchestration_5.1.0` folder and then run the `deploy.sh` script.

Bug Tracking Number: CXU-41845

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

Workaround: Manually refresh the page.

Bug Tracking Number: CXU-41793

- After ZTP of an NFX Series device, the status of some tunnels are displayed as down. This issue occurs if you are using the subnet IP address 192.168.2.0 on WAN links, which causes an internal IP address conflict.

Workaround: Avoid using the 192.168.2.0 subnet on WAN links.

Bug Tracking Number: CXU-41511

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

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

Bug Tracking Number: CXU-42608

- Installation of licenses on an SRX4200 dual CPE cluster by using CSO is failing.

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

1. Copy the license files for both the devices to the primary node of the cluster.
2. Install the license on the primary device.

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

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

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

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

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

Bug Tracking Number: CXU-40522

- When you configure a DVPN tunnel between an Internet link that is behind NAT and an Internet link that is not behind NAT the IPSec tunnel may not come up.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-43217

- You cannot change PKI properties (CA Server URL, Password, CRL Server, Auto Renew) on the Tenant Settings page.

Workaround: Only a tenant administrator can change PKI properties on the Administration > Certificate Management > VPN Authentication page.

Bug Tracking Number: CXU-41231

- Even though you successfully upgrade a spoke site from CSO Release 4.1.1 to CSO Release 5.1.2, the MPLS flow mode settings are not applied. This issue is not applicable if the MPLS flow mode settings are already applied to the CPE device during CSO Release 4.1.1 through stage-2 templates.

Workaround: Reboot the server.

Bug Tracking Number: CXU-42670

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32157

- CSO Release 5.1.2 does not support the installation of third-party certificates.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-49827

- You cannot delete the last LAN segment from the department if there is no connectivity between,
 - The spoke device and CSO, or
 - The designated hub of the spoke device and CSO.

Workaround: Delete the last LAN segment from the department after the connectivity is restored.

Bug Tracking Number: CXU-49439

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.1.2:

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

Bug Tracking Number: CXU-44158

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

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

Bug Tracking Number: CXU-43157

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

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

Bug Tracking Number: CXU-43277

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

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

1. `kubect exec -it etcd-etcd-0 bash -n infra`
2. `etcdctl set /csp/infra/fmpmlb/host <virtual IP address of SBLB in CSO Release 4.1.1>`
3. `etcdctl set /telemetryconverter/virtualhostname '{"regional": "SBLB hostname in CSO Release 4.1.1", "central": ""}'`

Bug Tracking Number: CXU-43570

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

Bug Tracking Number: CXU-42395

- Provisioning an SRX Series device as next-generation firewall by using CSO is failing.

Bug Tracking Number: CXU-43362

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

Bug Tracking Number: CXU-43726

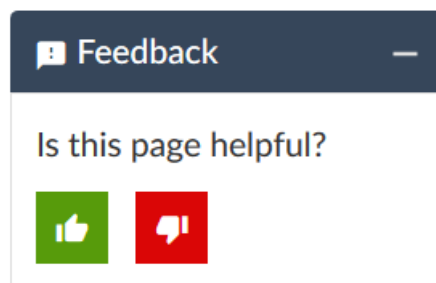
- If you have installed CSO Release 5.1 on a single node and if there is a power failure, the UI is not accessible even if the power resumes.

Bug Tracking Number: CXU-41460

Documentation Feedback

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

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



- Click the thumbs-up icon if the information on the page was helpful to you.
- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

Revision History

13 July, 2020—Revision 1, CSO Release 5.1.2

23 July, 2020—Revision 2, CSO Release 5.1.2

21 August, 2020—Revision 3, CSO Release 5.1.2

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.