

# Contrail Service Orchestration Release Notes

Release 5.1.0  
17 January 2020  
Revision 3

These Release Notes accompany Release 5.1.0 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction | 3

Software Support | 4

Software Downloads | 5

Software Installation Requirements for NFX Series Network Services Platform | 7

New and Changed Features in Contrail Service Orchestration Release 5.1.0 | 8

SD-WAN | 8

SD-LAN | 11

Next-Generation Firewall | 13

Miscellaneous | 14

VNFs Supported | 15

Licensing | 15

Accessing the CSO GUIs | 16

Known Behavior | 16

Device Management | 17

Dynamic VPN (DVPN) | 17

Policy Deployment | 18

SD-WAN | 18

SD-LAN | 19

Security Management | 19

Site and Tenant Workflow | 20

Topology | 21

User Interface | 21

General | 21

Known Issues | 22

SD-WAN | 23

SD-LAN | 24

CSO High Availability | 26

Security Management | 27

Site and Tenant Workflow | 28

General | 28

Resolved Issues | 36

Documentation Feedback | 37

Requesting Technical Support | 38

Self-Help Online Tools and Resources | 38

Creating a Service Request with JTAC | 39

Revision History | 39

# Introduction

Juniper Networks offers Contrail Service Orchestration (CSO) Release 5.1.0 as a cloud-based service that gives enterprises of all sizes access to its simple and intuitive GUI for WAN and LAN use cases. You can also deploy CSO Release 5.1.0 on-premises for customers that demand full control over their deployments.

CSO Release 5.1.0 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.

The following are the highlights of the features available in CSO Release 5.1.0:

- **SD-WAN features**

- Support for full mesh on an LTE WAN link
- Support for multiple WAN links on the same physical interface
- Support for OAM and data capability for OpCo provider hub
- Enhancements to cloud breakout settings
- Support for pool-based NAT for local breakout
- Enhancements to certificate authority (CA) configuration
- SD-WAN support for CPE devices behind NAT in full mesh topology
- Support for provider-edge resiliency
- Support for BGP underlay route advertisements
- Support for flexible (mixed) VLAN tagging
- Support for class of service at the logical interface level

- Edit support for site properties
- Edit support for tenant properties
- **SD-LAN features**
  - Deploying SD-LAN using EX4600 and EX4650 switches
  - Support for EX Series Virtual Chassis
  - Image upgrade for Virtual Chassis members
  - Return Material Authorization (RMA) support for EX Series switches
  - Configuration and monitoring of the ports of an EX Series switch
  - Firewall configurations for EX Series switches
- **Next-generation firewall features**
  - Support for custom application signatures in firewall policies
  - Support for customized IPS signatures, static groups, and dynamic groups
  - Support for importing policy configurations
- **Miscellaneous**
  - Support for configuration templates
  - Support for predefined stage-2 templates
  - Support for retrying failed bootstrap jobs
  - Enhancements to CSO licenses

## Software Support

### IN THIS SECTION

- [Software Downloads | 5](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 7](#)

## Software Downloads

Table 1 on page 5 displays the supported versions and download links for software components associated with CSO Release 5.1.0.

**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 5.1.0**

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.5R1	Pre-bundled with CSO.
EX Series switches	Junos OS Release 18.4R2.7	Junos OS Release 18.4R2.7 <ul style="list-style-type: none"> <li>EX2300: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX2300</a></li> <li>EX3400: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX3400">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93890.html?pf=EX3400</a></li> <li>EX4300: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93859.html?pf=EX4300">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93859.html?pf=EX4300</a></li> <li>EX4600: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93861.html?pf=EX4600">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93861.html?pf=EX4600</a></li> <li>EX4650: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93900.html?pf=EX4650">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93900.html?pf=EX4650</a></li> </ul>
NFX150 CPE device	Junos OS Release 18.2X85-D12	<ul style="list-style-type: none"> <li>Install Media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94797.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94797.html</a></li> <li>Install Package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94794.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/94794.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/92335.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92335.html</a></li> <li>Install Package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92333.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92333.html</a></li> </ul>
SRX Series CPE devices	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> <li>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices): <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> </ul>

Table 1: Software Components Associated with CSO Release 5.1.0 (continued)

Product	Supported Version	Download Link
SRX Series Next-Generation Firewall devices	Junos OS Release 18.4R1	<p>Junos OS Release 18.4R1</p> <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/85904.html?pf=SRX300">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/85904.html?pf=SRX300</a></li> </ul>
vSRX for SD-WAN devices	Junos OS Release 15.1X49-D172	<p>For hub devices and spoke devices:</p> <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>
vSRX for next-generation firewall devices	Junos OS Release 18.4R1	<ul style="list-style-type: none"> <li>vSRX (KVM appliance): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86042.html?pf=vSRX">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86042.html?pf=vSRX</a></li> <li>vSRX (Hyper-V image): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86041.html?pf=vSRX">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86041.html?pf=vSRX</a></li> <li>vSRX (VMware appliance with SCSI virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86044.html?pf=vSRX">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86044.html?pf=vSRX</a></li> <li>vSRX (VMware appliance with IDE virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86043.html?pf=vSRX">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/86043.html?pf=vSRX</a></li> </ul>

Table 1: Software Components Associated with CSO Release 5.1.0 (continued)

Product	Supported Version	Download Link
SRX Series Provider Hub device	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> <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> </ul>
SRX Series Enterprise Hub devices	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> <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>

## 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](https://www.juniper.net/documentation/product/en_US/nfx150) and [https://www.juniper.net/documentation/product/en\\_US/nfx250](https://www.juniper.net/documentation/product/en_US/nfx250).

# New and Changed Features in Contrail Service Orchestration Release 5.1.0

## IN THIS SECTION

- [SD-WAN | 8](#)
- [SD-LAN | 11](#)
- [Next-Generation Firewall | 13](#)
- [Miscellaneous | 14](#)

You can view the features that are available in the previous CSO releases in the following links:

- [CSO 5.0.0 Release Notes](#)
- [CSO 5.0.1 Release Notes](#)
- [CSO 5.0.2 Release Notes](#)
- [CSO 5.0.3 Release Notes](#)

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.1.0.

## SD-WAN

- **Support for full mesh on an LTE WAN link**—From CSO Release 5.1.0 onward, you can use LTE WAN links on a spoke site to connect the spoke site to enterprise hubs by enabling full mesh on the LTE WAN link and configuring a matching mesh-tag with the WAN link on the enterprise hubs.
- **Support for multiple WAN links on the same physical interface**—From CSO Release 5.1.0 onward, for on-premise SD-WAN spoke sites, you can configure more than one WAN link on the same physical interface. The WAN links are connected from the same physical interface to the provider edge (PE) nodes through logical subinterfaces with VLAN separation.
- **Support for OAM and data capability for OpCo provider hub**—From CSO Release 5.1.0 onward, Operating Companies (OpCos) can add provider hubs with OAM (Operation, Administration, and Maintenance) and data capability. In CSO releases before Release 5.1.0, OpCos can add provider hubs with only data capability.



- **Enhancements to cloud breakout settings**—From Release 5.1.0 onward, CSO supports the following:
  - Generic routing encapsulation (GRE) tunnels (with public IP addresses for the WAN links) for cloud breakout traffic.
  - IPsec phase 1 parameters, phase 2 parameters, and domain name while adding cloud breakout settings.
  - IP address or hostname validation for cloud breakout nodes.
  - Auto-populate FQDN, preshared key, WAN links, and an option to change the respective values.
  - High availability between the WAN links of an SD-WAN spoke site and the cloud breakout node.
  - WAN link modes as active/active or active/backup for creating the tunnels.

**NOTE:**

- For cloud breakout with GRE tunnels, CSO does not support CPE devices behind NAT.
- Maximum of two WAN links are supported between SD-WAN spoke site and the cloud breakout node.

- **Support for pool-based NAT for local breakout**—From CSO Release 5.1.0 onward, for on-premise SD-WAN spoke sites, on a WAN link with local breakout enabled, you can specify that pool-based NAT be used instead of interface-based NAT, which is the default.
- **Enhancements to certificate authority (CA) configuration**—From Release 5.1.0 onward:
  - CSO supports the configuration of CA servers of up to five tiers.
  - As a tenant administrator, you can edit the CA server URL and password from Customer Portal.
- **SD-WAN support for CPE devices behind NAT in full mesh topology**—From Release 5.1.0 onward, CSO supports site-to-site tunnels for WAN links of CPE devices behind NAT in full mesh topology. You can now provide private IP addresses for WAN links behind NAT and create the tunnels to enterprise hub or spoke sites. In releases before Release 5.1.0, CSO supports private IP addresses for WAN links behind NAT only for the WAN links that are not selected for meshing, and such WAN links can establish the tunnels only to provider hubs.

The support for CPE devices behind NAT in full mesh topology is applicable only for spoke devices. The OAM hubs, data hubs, and enterprise hubs or on-premise gateways require static public IP addresses for their WAN interfaces.

The supported NAT types are listed in [Table 2 on page 9](#).

**Table 2: CPE Behind NAT in Full Mesh Topology**

WAN IP Address	NAT Type	Spoke-to-Hub Tunnel	Spoke-to-Spoke Tunnel
Public IP address	No NAT	Supported	Supported

Table 2: CPE Behind NAT in Full Mesh Topology (*continued*)

WAN IP Address	NAT Type	Spoke-to-Hub Tunnel	Spoke-to-Spoke Tunnel
Private IP address	Full cone NAT	Supported	Supported
Private IP address	Restricted NAT	Supported	Supported
Private IP address	Symmetric NAT	Supported	Not supported

**NOTE:** This feature is present in the application but has not yet been fully qualified by Juniper Networks.

- **Support for provider edge resiliency**—From Release 5.1.0 onward, for on-premise SD-WAN spoke sites, you can connect a WAN link to primary and secondary PE nodes, thereby providing PE resiliency on the underlay. CSO establishes a BGP peering relationship between the customer premises equipment (CPE) device and the PE nodes. PE resiliency is supported only when local breakout is enabled.
- **Support for BGP underlay route advertisements**—From CSO Release 5.1.0 onward, for on-premise SD-WAN spoke sites with local breakout enabled, you can enable BGP underlay routing. Route advertisements to the primary PE node and, if configured, the secondary PE node occur as follows:
  - CSO advertises the WAN interface subnet.
  - If you specify a tenant public IP address pool and enable the option to advertise public LAN prefixes, for LAN segments that are created with a subnet that falls under the tenant public IP address pool, CSO advertises the LAN segment subnet.
  - If you configure pool-based translation, CSO advertises the NAT address pool.
- **Support for flexible (mixed) VLAN tagging**—From CSO Release 5.1.0 onward, when the same physical interface is used for multiple WAN links, CSO supports simultaneous tagged and untagged WAN links for single CPE devices with the condition that only one WAN link can be untagged.
- **Support for class of service at the logical interface level**—From CSO Release 5.1.0 onward, when the same physical interface is used for multiple WAN links, CSO supports class of service (CoS) provisioning of the shaping rate at the logical interface level. In CSO releases before Release 5.1.0, CSO supports CoS provisioning of the shaping rate only at the physical interface level.
- **Edit support for site properties**—From CSO Release 5.1.0 onward, you (as a tenant administrator) can edit the following properties configured for a site from the Sites page:
  - Address and Contact Information—Street Address, City, State/Province, ZIP/Postal Code, Country, Contact Name, Email, and Phone Number.
  - Advanced Configuration—Name Server IP List, NTP Server, and Time zone.

- In-band Management Port (available only for sites with next-generation firewall capability).
- **Edit support for tenant properties**—From CSO Release 5.1.0 onward, you can edit the following parameters configured for a tenant, from Administration Portal and Customer Portal:
  - Common tenant parameters—Password Expiration Days, Services (applicable only for SP administrators or OpCo administrators).
  - Parameters for tenants with SD-WAN capability:
    - Parameters that you can modify only before sites are added for the tenant: SSL Settings, VPN Authentication, Network Segmentation, and Overlay Tunnel Encryption.
    - Parameters that you can modify before or after sites are added for the tenant: Threshold for Creating a Tunnel, Threshold for Deleting a Tunnel, Cloud Breakout Settings, Tenant-specific Attributes.
    - Parameters for tenants with Hybrid WAN, Next-generation Firewall, or LAN capabilities: Tenant-specific Attributes.

## SD-LAN

- **Deploy SD-LAN using EX4600 and EX4650 switches**—: From CSO Release 5.1.0, you can manage EX4600 and EX4650 devices for SD-LAN in enterprise networks.

**NOTE:** CSO Release 5.1.0 does not support EX4600 and EX4650 virtual chassis.

- **Support for EX Series Virtual Chassis**—From Release 5.1.0 onward, you can add a Virtual Chassis with EX2300, EX3400, and EX4300 devices as members. However, you cannot add a Virtual Chassis with EX4600 and EX4650 devices as members.

All the devices in the Virtual Chassis must be of the same device type and model.

You can add the following number of devices in a Virtual Chassis, based on the device type:

- EX2300: 4 member devices
- EX3400: 10 member devices
- EX4300: 10 member devices

**NOTE:** In Release 5.1.0, the Virtual Chassis is autoprovisioned, that is, CSO discovers the members from the fully-formed Virtual Chassis, during provisioning.

- **Image upgrade for Virtual Chassis members**—From Release 5.1.0 onward, CSO supports the upgrade of images for an EX Series Virtual Chassis:

Images for each member of the Virtual Chassis are upgraded one after the other in the order – Linecard, Backup, and Primary.

- **RMA support for EX Series switches**—From CSO Release 5.1.0 onward, you can initiate the Return Material Authorization (RMA) workflow for a defective EX Series switch (physical standalone switch) when the switch is behind an SRX Series device acting as an SD-WAN CPE, next-generation firewall, or internet gateway.

CSO Release 5.1.0 supports RMA for an EX Virtual Chassis member when the Virtual Chassis is deployed as a standalone switch (that is, behind an internet gateway).

**NOTE:** RMA support for an EX Series switch (physical standalone switch) behind a next-generation firewall is present in the application, but has not yet been fully qualified by Juniper Networks.

- **Configure and monitor the ports of an EX Series switch**—From Release 5.1.0, you can use CSO to configure and monitor the ports of an EX Series switch. You can either configure the ports by accessing each port individually or by using a port profile, from the Ports tab of the Devices page in the Customer Portal UI.

You can configure and deploy port authentication profiles to implement network access control (NAC), and firewall filters to enforce security on the switch ports. After you configure the switch ports, you can monitor the ports from the Devices page.

**NOTE:** You can add port profile to CSO and configure one or more switch ports by using a port profile. However, the addition of a port profile to CSO and configuring a port by using a port profile has not yet been fully qualified by Juniper Networks.

- **Firewall configurations for EX Series switches**—From CSO Release 5.1.0 onward, you can configure firewall filters for EX Series switches. A firewall filter defines the rules to permit or deny packets that are transiting a switch port. You can assign the firewall filter as an ingress filter or egress filter to a switch port either while manually configuring the port or through port profiles.

**NOTE:**

- On EX2300 devices, the egress filters support only MAC addresses as source and destination endpoints.
- This feature is present in the application but has not yet been fully qualified by Juniper Networks.

## Next-Generation Firewall

- **Support for custom application signatures in firewall policies**—From Release 5.1.0 onward, CSO supports custom application signatures in firewall policies, in addition to its existing support in SD-WAN policies.
- **Support for customized IPS signatures, static groups, and dynamic groups**—From CSO Release 5.1.0 onward, you can create, modify, or delete customized intrusion prevention system (IPS) signatures, IPS signature static groups, and IPS signature dynamic groups. In addition, you can clone predefined or customized IPS signatures, static groups, and dynamic groups. You can then use the IPS signatures, static groups, and dynamic groups in an IPS profile that can contain one or more IPS or exempt rules.
- **Support for importing policy configurations**—From Release 5.1.0 onward, CSO supports importing policy configurations from next-generation firewall devices. The following features are supported:
  - Manage next-generation firewall sites for enterprise customers with brownfield deployments.
  - Discover existing policy configuration while onboarding next-generation firewall device (without enabling ZTP).
  - Import policy configurations from Firewall and NAT policy pages.
  - Deploy policies after importing them to CSO.

## Miscellaneous

- **Support for configuration templates**—From CSO Release 5.1.0 onward, you can view, create, modify, clone, and delete configuration templates from Administration Portal and Customer Portal. In addition, you can assign a configuration template to one or more device templates and deploy configuration templates on one or more devices. You can use the preview and render workflow to validate a configuration template.

**NOTE:** In CSO releases before Release 5.1.0, configuration templates are called stage-2 configuration templates.

- **Predefined configuration templates**—From CSO Release 5.1.0 onward, the following predefined configuration templates are added:
  - LACP—Use this template to bundle several physical interfaces to form one logical interface and link monitoring.
  - SNMP—Use this template to configure the minimum requirements for SNMP, including community, client list, trap group, and trap options.
  - COS/QoS—Use this template to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs.
  - IGMP Snooping—Use this template to configure Internet Group Management Protocol.
  - RSTP—Use this template to configure switching ports.
- **Retry failed bootstrap jobs**—From CSO Release 5.1.0 onward, you can retry the bootstrap jobs that did not complete successfully on your devices.
- **Enhancements to CSO licenses**—From CSO Release 5.1.0 onward, users with the SP Administrator role can edit and delete CSO licenses in Administration Portal.
- **Introducing Quick Help in Administration Portal and Customer Portal**—From CSO Release 5.1.0 onward, you can access the help documentation within Administration Portal and Customer Portal user interfaces. You can launch Quick Help from **Help Menu (?) > Quick Help**. Alternatively, you can use the **More...** hyperlinks on the user interface to access Quick Help. You no longer need to switch between windows to get help. Now, get quick help on all topics or the most popular ones, and also FAQs, in a tabbed interface.

# VNFs Supported

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

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

VNF Name	Version	Network Functions Supported	Deployment Model Support	Element Management System Support
Juniper Networks vSRX	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>	Hybrid WAN and SD-WAN deployments supports NAT, firewall, and UTM.	Element Management System (EMS) microservice, which is included with CSO
Ubuntu	16.04	-	Hybrid WAN and SD-WAN deployments–NFX250 and NFX150 platforms.	Element Management System (EMS) microservice, which is included with CSO
Fortinet	5.6.3	-	Hybrid WAN and SD-WAN deployments–NFX250 and NFX150 platforms.	Element Management System (EMS) microservice, which is included with CSO

## Licensing

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

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

# Accessing the CSO GUIs

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

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

## Known Behavior

### IN THIS SECTION

- [Device Management | 17](#)
- [Dynamic VPN \(DVPN\) | 17](#)
- [Policy Deployment | 18](#)
- [SD-WAN | 18](#)
- [SD-LAN | 19](#)
- [Security Management | 19](#)
- [Site and Tenant Workflow | 20](#)
- [Topology | 21](#)
- [User Interface | 21](#)
- [General | 21](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.1.0.



## Device Management

- CSO does not support cluster-level Return Material Authorization (RMA) for SRX Dual CPE devices. Only cluster node-level RMA is supported.
- The SRX4100 and SRX4200 devices support all existing SD-WAN features, except the following:
  - Phone-home client (PHC)—The CPE 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.
  - Service chaining.
- To activate an NFX150 device, you must configure the phone-home server to contact the CSO instance running on AWS. Contact the Juniper team for more information.
- LTE is not supported for dual CPE devices.
- You cannot remotely access a cloud spoke device and edit the configuration.

## 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 by CAN, and are added to the number of sessions closed. The sessions closed count is used to calculate the DVPN delete threshold.
- DVPN is not supported for cloud spoke sites.

## Policy Deployment

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

## SD-WAN

- If WAN link endpoints are not of similar type but overlay tunnels are created based on matching mesh tags, the static policy for site-to-site or central Internet breakout traffic gives preference to the remote link type.
- Advanced SLA configurations, such as CoS rate limiting, are not supported during local breakout if no specific application is selected; that is, if Application is set to ANY. Choose specific applications if you want to enable advanced SLA configurations, such as CoS rate limiting.
- If two or more SD-WAN policy rules are configured for the same application with different levels of granularity, such as all, sites, and departments, then CSO applies the CoS rate limiter in the same order in which you have created the intents.
- On the WAN tab of the *Site-Name* page, the link metrics graph displays aggregated data. Therefore, in cases where the aggregation interval overlaps between source and destination link data, the link metrics graph displays incorrect data.
- 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 hover the mouse over the **Reason** field of link switch events, sometimes **Above Target** is displayed instead of the absolute SLA metric value for very large values (for example, for an SLA metric value that is 100 times the target value).

- When an SD-WAN policy is deployed and a high rate of traffic flows through the CPE device, this might lead to network congestion and introduce delays or cause traffic loss. However, even though an SLA violation is reported, the traffic does not switch to a different link.
- In device redundancy mode, when you reboot a node, the device fails to generate a few system logs. Because a few system logs are not generated, the link switch event in CSO displays the same interface as the source interface and the destination interface.
- Sometimes duplicate link switch events are displayed on the Link Switch Events page.
- 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.

## SD-LAN

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

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

- Do not zeroize EX2300 and EX3400 devices as doing so might result in unexpected behavior.
- You cannot add more than one switch (physical standalone switch or Virtual Chassis) on a site.

## Security Management

- UTM Web filtering is not supported in an active-active SRX Series cluster device.
- SSL Proxy is not supported on SRX300 and SRX320 series devices.

## Site and Tenant Workflow

- When tenants are created, ensure that the tenant name is unique across the CSO instance; that is, the same tenant name should not be there in any of the OpCo networks on the CSO instance.
- In the Add Site workflow, use IP addresses instead of hostnames for the NTP server configuration. If you are using hostnames instead of IP addresses, ensure that the hostname is DNS-resolvable; if the hostname is not DNS-resolvable, ZTP for the device fails.
- CSO uses RSA-key-based authentication when establishing an SSH connection to a managed CPE device. The authentication process requires that the device has a configured root password, and you can use Administration Portal to specify the root password in the device template.

To specify a root password for the device:

1. Log in to Administration Portal.
2. Select **Resources > Device Templates**.
3. Select the device template and click **Edit**.
4. Specify the plain text root password in the **ENC\_ROOT\_PASSWORD** field.
5. Click **Save**.

- When you try to deploy a LAN segment on an SRX Series spoke device, the CSO GUI allows you to select more than one port for a LAN segment. However, for SRX Series devices, only one port for a LAN segment can be deployed; multiple ports in a LAN segment can be deployed only on NFX Series devices.
- On a site with an NFX Series device, if you deploy a LAN segment without the VLAN ID specified, CSO uses an internal VLAN ID meant for internal operations and this VLAN ID is displayed in the LAN section of the Site Detail View page. There is no impact on the functionality.
- Do not create departments that have names starting with **default**, **default-reverse**, **mpls**, **internet**, or **default-hub** because CSO uses the following departments for internal use:
  - *Default-vpn\_name*
  - *Default-reverse-vpn\_name*
  - *mpls-vpn\_name*
  - *internet-vpn\_name*
  - *Default-hub-vpn\_name*

## Topology

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

## User Interface

- When you use Mozilla Firefox to access the CSO GUIs, a few pages do not work as expected. We recommend that you use Google Chrome version 60 or later to access the CSO GUIs.
- When you copy and paste a stage-1 configuration from Chrome version 71.0.3578.98, insert a new line, as shown in the following example, in the private key text:

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC, 1F6A1336016A8239

                                ADD A NEW LINE HERE

2C638z/Lgr/g4Kw7r9lys9XWnUGbGnPpTlcc5jGq1Qbb8Nu286QsVGfrUy7Qh9sU
FJkIQI9bOMNadLL7wkl snwBCVAoAYjX+hai zSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWfGwCwUi+i jUKp/h9NfE5c2W5m2VBdmRjBf jWo9jcH
HV5gkkoG0Gdx7Kv60HKOMDl2YkjL4zfAzBS8J8BMmk5x6sY+GqNQOdgs7m4oXYCH
1loOYS6n9l0WDZcxXYWWeINlu6zOSIlZYVI dwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

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

## General

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

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

- 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.
- On an NFX Series device:
  - To activate a virtualized network function (VNF), perform the following steps:
    1. Add the VNF to the device.
    2. Initiate the activation workflow and ensure that the job is 100% completed.
  - To retry the activation of a VNF that failed, perform the following steps:
    1. Deactivate the VNF.
    2. Remove the VNF.
    3. Add the VNF to the device.
    4. Initiate the activation workflow and ensure that the job is 100% completed.
- Class-of-service (CoS) configuration on Layer 2 interfaces (*ge-0/0/port number*) is not supported on NFX150 CPE devices.
- Enterprise hub is not supported for cloud spoke sites.

## Known Issues

### IN THIS SECTION

- [SD-WAN | 23](#)
- [SD-LAN | 24](#)
- [CSO High Availability | 26](#)
- [Security Management | 27](#)
- [Site and Tenant Workflow | 28](#)
- [General | 28](#)

This section lists known issues in Juniper Networks CSO Release 5.1.0.

## SD-WAN

- 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

- When you add or remove any intent on the SD-WAN Policy page, a +0 is added after every element even though you selected only one element.

Workaround: This issue does not have any functional impact. The +0s disappear when you refresh the page.

Bug Tracking Number: CXU-32068

- Traffic from a spoke site that has a dynamic SLA policy enabled and is connected to an MX Series 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

- On gateway site, when there are no non-data center 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-data center 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 to fail.

Workaround: Delete the LAN segment and retry the deploy. 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 device that you have deactivated as cloud hub from CSO.

Workaround: Manually remove the configuration from the device.

Bug Tracking Number: CXU-25412

- 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

## SD-LAN

- At times, recall with the recovery configuration fails to revert EX2300 and EX3400 devices to the recovery configuration because some devices do not have the `/var/db/scripts/events` directory.

Workaround: Keep a copy of the recovery configuration and use the **load override *recovery filename*** command to revert the devices to the required configuration.

Bug Tracking Number: CXU-34430

- For an EX Series switch, on the Configuration Template page the Maximum Power field is not validated. The range for Maximum Power is 0 through 30 watts. The deployment fails if you specify any other values.

Workaround: Specify a value within the range (0 through 30 watts).

Bug Tracking Number: CXU-38850

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

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

Bug Tracking Number: CXU-38994



- For an EX Series switch, if you enable or disable a port from the UI, the port status is reflected in Port Chassis View and Port Grid only after an approximate time of 5 minutes.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-37846

- For an EX Series switch, you cannot filter or search for the device ports on the **Resources > Devices Device-Name > Ports** tab.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-38564

- If you reboot an NFX250 device, the EX Series switch behind the NFX250 device might not renew the DHCP request, and the operational status of the switch might be displayed as down.

Workaround: On the EX Series switch, manually run the **request dhcp client renew all** command.

Bug Tracking Number: CXU-39127

- The phone-home process might not be triggered if you zeroize an EX Series switch and disable the management interface on the switch.

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

Bug Tracking Number: CXU-39129

- If you are using an EX Series switch with Junos OS Release 18.3R1.9, the Current System Users widget always displays the login time as Jan 1, 1970.

Workaround: Upgrade the EX Series switch to Junos OS Release 18.4R2.7.

Bug Tracking Number: CXU-38647

- 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

- The Chassis View page for an EX Series switch is not automatically refreshed to display the status of the newly configured ports.

Workaround: Manually refresh the *Device-name* page. Alternatively, navigate to some other page on the UI and then revisit the *Device-name* page to view the status of the newly configured ports on the chassis view page.

- The Zero Touch Provisioning toggle button is displayed for EX4600 and EX4650 switches although these switches do not support ZTP.

Workaround: Disable the Zero Touch Provisioning toggle button and manually configure the stage-1 configuration on the switches.

Bug Tracking Number: CXU-41608

- The Chassis View page for an EX Series Virtual Chassis incorrectly displays member 0 as the primary member although the Virtual Chassis was successfully provisioned without member 0, through ZTP.

Workaround: Add an EX Series device as member 0 before provisioning the Virtual Chassis.

Bug Tracking Number: CXU-40322

- If you upgrade a CSO Release 5.0.3 site with an EX Series switch to CSO Release 5.1, the port profile configuration or manual configuration of a port profile on an already configured port may not work as expected.

Workaround: Delete and re-create the site with an EX Series switch.

Bug Tracking Number: CXU-41763

## CSO High Availability

- In an HA setup, some of the VRRs are incorrectly reported as down even though those VRRs are up and running. This problem occurs because some of the alarms that are created 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, deployment of NAT and firewall policies fail if secmgt-sm pods fail to initialize after a snapshot process and remain in 0/1 Running state.

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

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

Bug Tracking Number: CXU-31446

- In a multinode CSO installation, CSO workflows do not work as expected if you restart any of the three available servers. This is because of the Cassandra database-related issue.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41620

## Security Management

- 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

## Site and Tenant Workflow

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

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

Bug Tracking Number: CXU-38960

## General

- App Visibility functionality for NFX250 and NFX150 Hybrid WAN Managed Internet CPE may not work as expected because application tracking is not enabled by default.

Workaround: Enable application-tracking through device configuration from the CSO UI. Go to **Devices**, select an NFX250 or NF150 site, and then select **Configuration > Zones > Edit Untrust Zone**, and select the **Application-Tracking** check box and deploy the configuration.

Bug Tracking Number: CXU-37713

- When a WAN link that is configured with DHCP is used as a DVPN tunnel endpoint, a change in the DHCP IP address of the WAN link causes the DVPN tunnel to be down.

Workaround: Delete the DVPN tunnel from the **Resources > Resource Name > WAN** tab and create a new tunnel.

Bug Tracking Number: CXU-36761

- The display name field of the monitor object deleted alarm shows the UUID of deleted sites instead of the name of the site.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-36367

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

Workaround: Manually clean up the EX2300 and EX3400 devices.

Bug Tracking Number: CXU-35208

- For Hybrid sites that use NFX150 or NFX250 CPE, you cannot use default configuration templates to configure physical interfaces, zones, or routing instances.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-35021

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32826

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

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

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

Bug Tracking Number: CXU-32731

- After you do an RMA of a spoke device, the LAN segment fails to connect to the enterprise hub.

Workaround: Reboot the spoke device.

Bug Tracking Number: CXU-35379

- On the Shared Objects page, if you edit a custom application or application group settings, the firewall policies or SD-WAN policies are marked as Pending Deployment even though there are no changes to the policies.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-38706

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-38388

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

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

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

Bug Tracking Number: CXU-35379

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

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

Bug Tracking Number: CXU-39167

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

Workaround: Delete and redeploy the LAN segments.

Bug Tracking Number: CXU-37770

- The Contrail health check fails for a non-HA deployment after you run the **deploy.sh** script on a startup server.

Workaround: Reboot Contrail Analytic Node (CAN). Wait for 10 minutes and rerun the **components\_health\_check.sh** script to see if all components are healthy. If all the components are healthy, then proceed with the installation.

Bug Tracking Number: CXU-41463

- On a newly installed CSO setup, core files are generated in the CAN virtual machines (VMs).

Workaround: No workaround. However, to see whether the processes are running as expected, check the Contrail Status in all the dockers.

Bug Tracking Number: CXU-41338

- When DVPN tunnels (GRE\_IPSEC tunnels) are established between a pair of SRX3XX devices that have Internet WAN links behind NAT, the GRE OAM status of the tunnels is displayed as DOWN and hence the tunnels are marked as DOWN and not usable for traffic.

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

Bug Tracking Number: CXU-41281

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

Workaround:

1. Log in to the CAN node.
2. Run the **docker restart analyticsdb analytics controller** command and wait for around 10 minutes.
3. Rerun the **components\_health\_check.sh** script on the startup server.
4. If the CAN node components are still unhealthy, repeat [2](#) and [3](#).

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

Bug Tracking Number: CXU-41232

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

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

Bug Tracking Number: CXU-40815

- UTM Web filtering is not supported in the active-active SRX Series chassis cluster. The UTM Web filter will be up only on one node of the cluster. The up status depends on which node was able to setup connection to the cloud server from the **PFE** directory.

Workaround: None

Bug Tracking Number: CXU-32738

- The bootstrap process remains in the In Progress state because the phone-home server fails to receive the bootstrap completion notification from the phone-home client.

Workaround: Reconfigure the name server and the phone-home server (<https://redirect.juniper.net>), and restart the phone-home client.

Bug Tracking Number: CXU-41449

- Signature database installation might fail for an SRX Series device, with the following error message:

**Application signature version 3229 install failed for device 4100HAEH. Error copy on device/node failed : file copy /tmp/application\_groups2.xml.gz  
node0:/var/db/idpd/nsm-download/application\_groups2.xml.gz error: put-file failed error: could not send local copy of file {primary:node0} cspuser@4100HAEH.4100HAEH**

Workaround: Run the following commands as the root user on the device shell:

- **chmod -R 777 /var/db/idpd/nsm-download**
- **chmod -R 777 /var/db/appid/sec-download**

For dual CPE devices, you must run these commands on node 0 and node 1.

Bug Tracking Number: CXU-41678

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

Workaround: In the **elasticsearch.yml** file, update the **index.max\_result\_window** parameter to **20000**.

Bug Tracking Number: CXU-41678

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

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

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

Bug Tracking Number: CXU-35450

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41210

- You cannot edit a device profile for an NFX150 device.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41719

- 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

- The deployment of the MariaDB pod fails if you are installing CSO on an installation server or a startup server.

Workaround: Redeploy the MariaDB pod by running the deploy script again.

Bug Tracking Number: CXU-41734

- 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

- You must have access to the Internet while you are installing CSO at the customer premises.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41920

- The IP addresses for the Contrail Analytics Nodes (CAN) are not populated in the HAproxy service during the deployment.

Workaround: Log in to the startup server and run the following command:

```
salt -C 'G@roles:haproxy_conf' state.apply haproxy_conf saltenv='central'
```

Bug Tracking Number: CXU-41914

- You cannot delete a LAN segment in a site that is associated with an EX Series standalone switch.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41907

- ZTP of an SRX Series device with a WAN link fails, if the SRX Series device is connected to a provider data hub that was onboarded in releases earlier than CSO Release 5.1.

Workaround:

As a user with SP admin or OpCo admin privileges, perform the following steps:

1. For an On-prem instance, create a custom stage-2 template with the following command:



```
set policy-options community ipvpn-community members target:192.168.0.1:10
```

2. Associate the stage-2 template with the provider hub.

**NOTE:** For a SAAS instance, Juniper Networks has created the P-HUB-UPGRADE stage-2 template and associated it with the SRX as SD-WAN hub device template.

3. Upgrade the provider data hub to CSO 5.1.0 by using REST API (POST <https://cso-ui/tssm/upgrade-site>).

The following is a sample for using the REST API:

1. Obtain the UUID of the provider hub site by using the GET <https://cso-ui/tssm/site/> API:

```
{
  "fq_name": [
    "default-domain",
    "default-project",
    "default-project",
    "PSK-OAMHUB-01"
  ],
  "uuid": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "uri": "/tssm/site/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

2. Upgrade the site by using the POST <https://cso-ui/tssm/upgrade-site> API:

```
{
  "input": {
    "site_uuids": [
      "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
    ]
  }
}
```

Bug Tracking Number: CXU-41861

- 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

- In case of a central breakout (traffic breaking out over hub links), because the GRE tunnel on the hub device is down, the hub device may not forward the return traffic from the Internet to the spoke device.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41239

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41139

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

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

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

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

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

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

- **apt-get update && apt-get install python2.7-dev**
- **cp sources.list.cso sources.list**

3. Navigate to the **/root/Contrail\_Service\_Orchestration\_5.1.0** folder and then run the **deploy.sh** script.

Bug Tracking Number: CXU-41845

- If you create two users with same names but different roles (SP administrator and OpCo administrator) and delete one of the users, the Users page continues to display the name of the user that you deleted. This is because the Users page is not automatically refreshed.

Workaround: Manually refresh the page.

Bug Tracking Number: CXU-41793

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

Workaround: Avoid using the 192.168.2.0 subnet on WAN links.

Bug Tracking Number: CXU-41511

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

Workaround:

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

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

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

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

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

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

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

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

3. Restart the kubernetes and dockers on both infra service and microservice by running the **service docker start** and **service kubelet start** commands.
4. Navigate to the **Contrail\_Service\_Orchestration\_5.1.0** folder and run the **setup\_NAT\_rule.sh** script on the bare-metal server to enable traffic flow from outside the network.

```
root@ccra-68:~/Contrail_Service_Orchestration_5.1.0/ci_cd#
./setup_NAT_rule.sh
```

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

Bug Tracking Number: CXU-41460

## Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.1.0:

- If you create an audit log purge with a recurring schedule and select the **Run Now** option, the recurrence fails to get scheduled.

Workaround: When you schedule an audit log purge with a recurring schedule, use the **Schedule at a later time** option instead of the **Run Now** option.

Bug Tracking Number: CXU-32608

- Site-to-Site DVPN tunnels fail to establish if the WAN interface of the CPE is behind a NAT device.
- The job log message **No update of SD-WAN policy configuration on device with ID *deviceID* due to missing required information** does not indicate an error even though it appears in red. The message only indicates that there is no SD-WAN policy applicable for the site.

Bug Tracking Number: CXU-35169

- For OpCo accounts created in CSO Release 5.0.0, OpCo administrators need to import OAM Hubs from the Site Management page before they could create Provider Hub sites.

Bug Tracking Number: CXU-37357

- When frequent link switches happen, the application throughput data displayed on **Monitor > Application SLA Performance** page and **Resources > Site management > Site details > WAN** page might vary.

Bug Tracking Number: CXU-33050

- The Sites Meeting SLA Without Switching section in an SD-WAN performance report lists the sites that are in the Provision-Failed state.

Bug Tracking Number: CXU-38894

- You cannot view the WAN links on Monitor > Geographic Map and Site Management > Site *Site-Name* > WAN pages.

Bug Tracking Number: CXU-38882

- The bootstrap job for sites that use SRX Series devices remains in the in-progress state. This problem occurs if only MPLS links are enabled with use for OAM.

Bug Tracking Number: CXU-36661

- While you activate an EX Series switch, the Activate Device page displays the status of the stage-1 configuration as failed.

Bug Tracking Number: CXU-38642

- The View link does not appear on the Sites page if you activate an EX Series switch using the activation code.

Bug Tracking Number: CXU-38421

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

Bug Tracking Number: CXU-37770

- When you delete a site and recover the **recovery.conf** file on SRX3XX devices, the Phone-Home Client (PHC) does not automatically restart.

Bug Tracking Number: CXU-35385

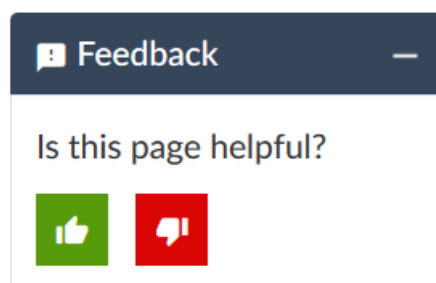
- During ZTP, the bootstrap job times out if the device takes a long time to connect to CSO.

Bug Tracking Number: CXU-34298

## 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

12 December 2019—Revision 1, CSO Release 5.1.0

24 December 2019—Revision 2, CSO Release 5.1.0

17 January 2020—Revision 3, CSO Release 5.1.0

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.