

# Contrail Service Orchestration Release Notes

Release 5.0.2

April 7, 2020

Revision 3

These Release Notes accompany Release 5.0.2 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 | 4

Software Installation Requirements for NFX Series Network Services Platform | 6

New and Changed Features in Contrail Service Orchestration Release 5.0.2 | 6

VNFs Supported | 8

Licensing | 8

Accessing the CSO GUIs | 9

Known Behavior | 9

Device Management | 9

Dynamic VPN (DVPN) | 10

Policy Deployment | 11

SD-WAN | 11

Security Management | 12

Site and Tenant Workflow | 12

Topology | 13

User Interface | 13

General | 14

Known Issues | 15

SD-WAN | 16

Site and Tenant Workflow | 16

General	17
Resolved Issues	20
Documentation Feedback	22
Requesting Technical Support	22
Self-Help Online Tools and Resources	23
Creating a Service Request with JTAC	23
Revision History	23

# Introduction

Contrail Service Orchestration (CSO) Release 5.0.2 is a Juniper Networks-hosted public cloud-based Software as a Service (SaaS) solution. CSO Release 5.0.2 supports two types of accounts:

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

The following are the highlights of the features available in Release 5.0.2:

- Enhancements to CSO license management
- Support for a unified firewall policy
- Support for IPS profiles
- LTE support for SRX Series devices
- Chassis view support for EX Series devices
- Support for custom application signatures
- Support for cloud spoke sites on AWS VPC
- Predefined configuration templates for LAN and Next-Generation Firewall CPE devices

## Software Support

### IN THIS SECTION

- [Software Downloads | 4](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 6](#)

## Software Downloads

Table 1 on page 4 displays the supported versions and download links for software components associated with CSO Release 5.0.2.

**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 5.0.2**

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.5R1	Pre-bundled with CSO.
EX Series switches	Junos OS Release 18.4R2.7	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=EX3400">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/93859.html?pf=EX3400</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>
SRX Series Next-Generation Firewall devices	Junos OS Release 18.4R1	Junos OS Release 18.4R1 <ul style="list-style-type: none"> <li>SRX300, SRX320, SRX340, SRX345, and SRX550: <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>

Table 1: Software Components Associated with CSO Release 5.0.2 (continued)

Product	Supported Version	Download Link
vSRX	Junos OS Release 15.1X49-D172  Junos OS Release 18.4R1	<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> <p>For next-generation firewall devices:</p> <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>
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>

Table 1: Software Components Associated with CSO Release 5.0.2 (continued)

Product	Supported Version	Download Link
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.
2. Specify this image as the boot image when you configure activation data.

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

## New and Changed Features in Contrail Service Orchestration Release 5.0.2

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.0.2.

- **Enhancements to CSO license management**—From CSO Release 5.0.2 onward, OpCo administrators can assign CSO licenses to their tenants, update or unassign license assignments, and view the tenants assigned to a CSO license.
- **Support for installing predefined IPS signatures**—From Release 5.0.2 onward, tenant administrators can install the active signature database, which also contains predefined IPS signatures, on one or more devices (SRX Series and vSRX).
- **Support for IPS profiles**—From CSO Release 5.0.2 onward, you can use predefined or customized IPS profiles and add IPS rules and exempt rules to customized profiles. You can then reference the IPS profiles in a firewall policy intent and deploy the IPS and exempt rules on the device (by deploying the firewall policy).
- **LTE support for SRX Series devices**—From CSO Release 5.0.2 onward, you can configure LTE as an access type for WAN links on SRX320, SRX340, and SRX345 CPE devices in an SD-WAN deployment. In CSO releases before Release 5.0.2, you can configure LTE as an access type only for NFX150 and NFX250 CPE devices.

You can also configure access point name (APN) settings for LTE WAN links for SRX320, SRX340, and SRX345 CPE devices on the *Device-Name* page in Customer Portal.

- **Chassis view support for EX Series devices**—From Release 5.0.2 onward, for an EX Series switch, CSO displays the chassis view of ports, port statistics, and information about switch health on the *Device-Name* page.
- **Support for custom application signatures**—From CSO Release 5.0.2 onward, you can create custom application signatures and use them in SD-WAN policies. CSO supports the following custom application signatures:
  - ICMP-based mapping
  - IP address-based mapping
  - IP protocol-based mapping
  - Layer 7-based signatures
- **Support for cloud spoke sites on AWS VPC**—From CSO Release 5.0.2 onward, a tenant administrator or an OpCo administrator can add and configure a cloud spoke site for an SD-WAN endpoint in an Amazon Web Services (AWS) virtual private cloud (VPC). To add a cloud spoke site, log in to Customer Portal and select **Resources > Site Management > Add > Add Cloud Spoke**.
- **Predefined configuration templates for LAN and Next-Generation Firewall CPE devices**—From CSO Release 5.0.2 onward, the following predefined configuration templates are added for LAN and Next-Generation Firewall CPE devices:
  - **Pre ID Default Policy**—Use this template to configure default policy settings for the Unified L4/L7 policy, before the final dynamic application is identified.
  - **Static Routes**—Use this template to configure static routes (for IPv4 and IPv6 networks) and advanced route settings.

- Service—Use this template to configure system services for SSH and NETCONF.
- Syslog—Use this template to configure Complete System Syslog Host, File, User, and Console settings.
- DNS—Use this template to configure Domain Name Servers (DNS) on the device.
- NTP—Use this template to configure Network Time Protocol (NTP) servers on the device.
- Banner—Use this to configure a message that is displayed before logging in to the device.

## VNFs Supported

CSO supports the Juniper Networks VNFs listed in [Table 2 on page 8](#).

**Table 2: 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

## Licensing

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. When the account is activated, you receive an e-mail with the URL information and access credentials for logging in to the CSO portal.



# 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 | 9](#)
- [Dynamic VPN \(DVPN\) | 10](#)
- [Policy Deployment | 11](#)
- [SD-WAN | 11](#)
- [Security Management | 12](#)
- [Site and Tenant Workflow | 12](#)
- [Topology | 13](#)
- [User Interface | 13](#)
- [General | 14](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.0.2.

### 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.
- 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.

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.
- 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.

- Site-to-Site DVPN tunnels fail to establish if the WAN interface of the CPE is behind a NAT device.
- DVPN is not supported for cloud spoke sites.

## Policy Deployment

- 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.
- 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.

## 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/g4Kw7r9lYs9XWnUGbGnPpT1cc5jGq1Qbb8Nu286QsVGfrUy7Qh9sU
FJkIQI9bOMNadLL7wklSnwBCVAoAYjX+haiZSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWFGWcwUi+ijUKp/h9NfE5c2W5m2VBdmRjBfjWo9jcH
HV5gkkoG0Gdx7Kv60HKOMDl2YkjL4zfAzBS8J8BMmk5x6sY+GqNQOdgs7m4oXYCH
1loOYS6n9l0WDZcxXYWWeINlu6zOSilZYVIIdwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

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

## General

- 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.
- 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.
  - LAN routes are not advertised to the neighbor in case of a data center deployment on a gateway site that uses routing protocols such as BGP or OSPF. In such cases, configure source NAT on the gateway site from the CSO UI or configure reverse routes on the routing device.
  - Overlapping LAN segments are not supported within a tenant network.
  - CSO Release 5.0.2 does not support service chaining.
  - Enterprise hub is not supported for cloud spoke sites.

## Known Issues

### IN THIS SECTION

- [SD-WAN | 16](#)
- [Site and Tenant Workflow | 16](#)
- [General | 17](#)

This section lists known issues in Juniper Networks CSO Release 5.0.2.

## SD-WAN

- 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

- 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.

Workaround: There is no known workaround.

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.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-38894

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

Workaround: Add a LAN segment and redeploy the site.

Bug Tracking Number: CXU-38882

## Site and Tenant Workflow

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

Workaround: Delete the site and add it again, and then try ZTP.

Bug Tracking Number: CXU-34298

- On a site with an NFX250 device and EX Series switch, the EX Series switch is not be 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 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.

Workaround: Copy and paste the stage-1 configuration to the device CLI instead of performing ZTP.

Bug Tracking Number: CXU-36661

- 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

- 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

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

Workaround: After you commit the **recovery.conf** file, you must manually restart the PHC by running the **restart phone-home-client** command, and then perform ZTP.

Bug Tracking Number: CXU-35385

- 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

- 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

- 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

- 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, the LAN segment fails to connect to the enterprise hub.

Workaround: Reboot the spoke device.

Bug Tracking Number: CXU-35379

- 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

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

Workaround: Do not cancel the activation process. After a couple of minutes, the device activation process will proceed toward completion.

Bug Tracking Number: CXU-38642

- During zero touch provisioning (ZTP) of an EX Series switch, the recovery configuration is overwritten by the stage-1 configuration.

Workaround: Save a copy of the recovery configuration before performing the ZTP or use prestage to provision an EX Series switch.

Bug Tracking Number: CXU-38594

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

Workaround: Enable the **Auto activate** field to automatically trigger ZTP.

Bug Tracking Number: CXU-38421

- 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

- 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

- 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

- 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

- 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

## Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.0.2:

- An SRX Series device remains in the **DEVICE\_DETECTED** state for 3 to 4 minutes during ZTP.

Workaround: There is no functional impact. The ZTP continues after the delay of around four minutes.

Bug Tracking Number: CXU-31813

- If you deploy multiple firewall policies that have multiple devices, The View Configuration page shows only devices from one of the policies even though the policies have been successfully deployed to all devices.

Bug Tracking Number: CXU-36594

- If you configure a PPPoE-enabled xDSL link for exclusive breakout, it may not work as expected.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-36706

- Over an SD-WAN CPE, traffic flow from the LAN side is not monitored for AppQoE passive probes if the destination (UDP or TCP) port for the traffic is set to 36000.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-37413

- The firewall policy deployment fails if you deploy the *Default\_FW\_policy* firewall policy on an SD-WAN site.

Workaround: The *Default\_FW\_policy* firewall policy is for only next-generation firewall sites. Create a new policy, add rules that are specific to SD-WAN sites, and then deploy the policy on the SD-WAN site.

Bug Tracking Number: CXU-37567

- The **More** options on the **Site Management** page shows **Reboot** for a provider hub device. However, tenant administrators do not have the permissions to reboot a provider hub device and the reboot job initiated by a tenant administrator fails.

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

Bug Tracking Number: CXU-37698

- For Provider Hub devices that are provisioned by an OpCo administrator, the OpCo administrator is unable to access the **Remote Console** option in the **Resources > Cloud Hub Devices** page.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-37706

- If tenant administrators select an enterprise hub site while adding a static tunnel for a full-mesh topology network by using the + icon on the WAN page, CSO returns the error **Error NoneType object is not iterable**. This problem occurs because static tunnels are already present between the enterprise hub and spoke sites.

Bug Tracking Number: CXU-37758

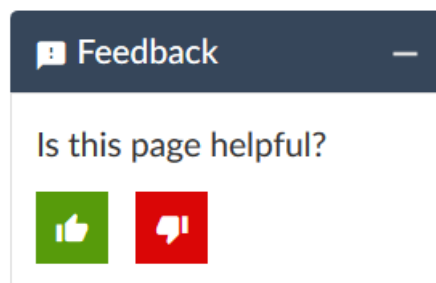
- OpCo administrators (created in CSO Release 5.0.0) are able to delete a data hub even if one of their tenants have sites associated with the data hub or if the tenant imports the data. Because there is no warning, before deleting a data hub the OpCo administrators must ensure that there are no sites associated with the data hub.

Bug Tracking Number: CXU-37800

# 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

April 7, 2020—Revision 3, Removed SRX550M as next-generation firewall

04 November 2019—Revision 2, CSO Release 5.0.2

26 September 2019—Revision 1, CSO Release 5.0.2

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.