

# Contrail Service Orchestration Release Notes

**Release 5.0.0**  
**08 August 2019**  
**Revision 3**

These Release Notes accompany Release 5.0.0 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 .....	3
Software Downloads .....	3
Software Installation Requirements for NFX Series Network Services	
Platform .....	5
New and Changed Features in Contrail Service Orchestration Release 5.0.0 .....	5
VNFs Supported .....	7
Licensing .....	7
Accessing the CSO GUIs .....	7
Known Behavior .....	8
Device Management .....	8
Dynamic VPN (DVPN) .....	9
Policy Deployment .....	9
SD-WAN .....	10
Security Management .....	11
Site and Tenant Workflow .....	11
Topology .....	12
User Interface .....	12
General .....	12
Known Issues .....	13
SD-WAN .....	13
Site and Tenant Workflow .....	14
General .....	14
Resolved Issues .....	16
Documentation Updates .....	17
Documentation Feedback .....	17

Requesting Technical Support .....	17
Self-Help Online Tools and Resources .....	18
Creating a Service Request with JTAC .....	18
Revision History .....	18

## Introduction

Contrail Service Orchestration (CSO) Release 5.0.0 is a Juniper Networks-hosted public cloud-based Software as a Service (SaaS) solution. CSO Release 5.0.0 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 5.0.0:

- Juniper Networks-hosted public cloud-based SaaS solution
- Enhancements to tenant and site onboarding
- LAN device management
- Next-generation firewall device management
- Bulk site creation by using site templates
- Enhanced SD-WAN policy management
- Mist access point integration

## Software Support

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

### Software Downloads

[Table 1 on page 3](#) displays the supported versions and download links for software components associated with CSO Release 5.0.0.



**NOTE:** Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes documentation.

**Table 1: Software Components Associated with CSO Release 5.0.0**

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.0R1	Pre-bundled with CSO.

**Table 1: Software Components Associated with CSO Release 5.0.0 (continued)**

Product	Supported Version	Download Link
EX Series switches	Junos OS Release 18.3R1.9	<ul style="list-style-type: none"> <li>EX2300: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81637.html?pf=EX2300">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81637.html?pf=EX2300</a></li> <li>EX3400: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81637.html?pf=EX3400">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81637.html?pf=EX3400</a></li> <li>EX4300: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81599.html?pf=EX4300">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/81599.html?pf=EX4300</a></li> </ul>
NFX150 CPE device	Junos OS Release 18.2X85-D11	<ul style="list-style-type: none"> <li>Install Media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88051.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/88051.html</a></li> <li>Install Package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87999.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/87999.html</a></li> </ul>
NFX250 CPE device	Junos OS Release 15.1X53-D497	<ul style="list-style-type: none"> <li>Install Media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/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 device	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> <li>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92321.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92321.html</a></li> <li>SRX1500: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92323.html</a></li> <li>SRX1500 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92325.html</a></li> <li>SRX1500 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92326.html</a></li> <li>SRX4100, SRX4200: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92322.html</a></li> <li>SRX4100, SRX4200 (USB): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92324.html</a></li> <li>SRX4100, SRX4200 (PXE): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92327.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 5.0.0 (continued)

Product	Supported Version	Download Link
vSRX	Junos OS Release 15.1X49-D172	<ul style="list-style-type: none"> <li>vSRX (Compressed TAR file (TGZ) for upgrade): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92328.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92328.html</a></li> <li>vSRX (KVM appliance): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92331.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92331.html</a></li> <li>vSRX (Hyper-V image): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92332.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92332.html</a></li> <li>vSRX (VMware appliance with SCSI virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92330.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92330.html</a></li> <li>vSRX (VMware appliance with IDE virtual disk (.ova)): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92329.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/92329.html</a></li> </ul>

## 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 5.0.0

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.0.0.

- **Enhancements for tenant onboarding**—From CSO Release 5.0.0 onward, a tenant can use one or more of the following services:
  - SD-WAN
  - Hybrid WAN
  - Next-generation firewall
  - LAN

When the tenant logs in to Customer Portal for the first time, the tenant must read and agree to the terms of use and can then review the tenant settings on the Tenant Review Settings page.

- **Support for EX Series switches**—From CSO Release 5.0.0 onward, you can provision, deploy, and monitor EX Series switches in branch deployments. You can connect an

EX Series switch to a Customer Premise Equipment (CPE) device such as an SRX Series device functioning as a secure SD-WAN router, enterprise hub, or next-generation firewall. You can also connect an EX Series switch to a third-party Internet gateway device.

In CSO Release 5.0.0, the following EX Series switches are supported: EX2300, EX3400, and EX4300.

- **Support for next-generation firewall sites**—From CSO Release 5.0.0 onward, you can add a standalone site with next-generation firewall capabilities. You can also add a site with LAN capabilities along with next-generation firewall capabilities.
- **Integration with Mist access points**—From CSO Release 5.0.0 onward, you can enable integration of Mist access points with CSO and provide the credentials for accessing the Mist portal from CSO. If you enable integration with Mist access points, the Mist access points are listed among the devices for a site, and you can click the item to launch the Mist portal and view the details about the access points.
- **Support for site templates**—From CSO Release 5.0.0 onward, you can add site templates in CSO. A site template enables you to specify values for many of the attributes used to add a site. You can then use the site template to add multiple sites that share the same set of values (for attributes already specified in the site template) and specify values only for site-specific attributes.

Site templates are applicable only for on-premise spoke sites.

- **Support for firewall device configuration**—From CSO Release 5.0.0 onward, you can configure zones, routing instances, and logical interfaces for a firewall device. You can use these zones, routing instances, and logical interfaces when you define firewall and NAT policies.
- **Support for firewall policy management**—From CSO Release 5.0.0 onward, CSO supports both zone-based intents (intents with zones as source and destination) and enterprise-based intents (intents with sites, site groups, departments, and addresses as source and destination) for a firewall policy.



**NOTE:**

- SSL profile is applicable for zone-based intents.
  - SSL policy is not applicable for enterprise-based intents.
- 

- **Support for automatically allocating OAM hubs**—From CSO Release 5.0.0 onward, CSO automatically allocates an OAM hub for an on-premise spoke site and an enterprise hub site.
- **Identify connectivity issues by using ping and traceroute**—From CSO Release 5.0.0 onward, you can identify connectivity issues between a device and a remote host by using the ping and traceroute options.
- **Enhancements to SD-WAN policy management**—From Release 5.0.0 onward, CSO provides predefined SD-WAN intent policies, application groups and SLA profiles.

The enhancements to SLA profiles are as follows:

- Predefined SLA parameters (target metrics) for specific traffic type
- SLA profile recommendations for system defined application groups
- SLA profiles are categorized as follows:
  - SLA-based steering profile—A profile for which you define one or more SLA parameters.
  - Path-based steering profile—A profile for which you define only the path preference (MPLS or Internet) but no SLA parameters.

## VNFs Supported

CSO supports the Juniper Networks VNFs listed in [Table 2 on page 7](#).

**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

---

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.0.0.

- [Device Management](#)
- [Dynamic VPN \(DVPN\)](#)
- [Policy Deployment](#)
- [SD-WAN](#)
- [Security Management](#)
- [Site and Tenant Workflow](#)
- [Topology](#)
- [User Interface](#)
- [General](#)

### 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.
- EX2300 and EX3400 devices do not support the PHC. 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.
- If you are not using PHC for activating a device, **recovery.config** is not created automatically. This means that the recall with recovery configuration option fails to apply the recovery configuration to the device. So, if you are not using PHC for activating a device, manually create the recovery configuration and save as **/config/recovery.conf**.



## 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** values 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 CPE is behind a NAT device.

## 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 condition 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 ensures that when a WAN link matching the SLA becomes available, traffic is routed through that link.
- The policy intents defined for a firewall or an SD-WAN policy must not have conflicts with other policy intents in that policy because such conflicts lead to inconsistent behavior. For example:
  - You cannot define an SD-WAN policy with one policy intent for application X and SLA profile S-1 and another policy intent for application X and SLA profile S-2.
  - You cannot define two firewall policy intents with the same source and destination endpoints but one with action Allow and another with action Deny.

## SD-WAN

- From CSO Release 5.0 onward, pre-defined SD-WAN policy intents are available for the tenants. The pre-defined SD-WAN policy intents are available only if the service provider administrator has downloaded the signature database prior to creating the tenants. The tenants that are added prior to signature download cannot view the pre-defined SD-WAN policy intents.
- 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 created the intents.
- Between spoke 1 (attached to the provider hub) and spoke 2 (attached to the provider hub and the gateway site), traffic occurs in the following paths:
  - From spoke 1 to spoke 2, forward traffic goes through the provider hub (to spoke 2) and reverse traffic goes through the gateway site (to spoke 1).
  - From spoke 2 to spoke 1, forward traffic goes through the gateway site (to spoke 1) and the reverse traffic goes through the provider hub to spoke 2.
- 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, that 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 source interface and 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 device cluster.
- Intrusion prevention system (IPS) is not supported. Therefore, in the IPS report, the attack name from the IPS signatures is displayed as UNKNOWN.
- SSL Proxy is not supported on SRX300 and SRX320 series devices.

## Site and Tenant Workflow

- In the 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
FJkIQI9bOMNadLL7wk1snwBCVAoAYjX+haizSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWFgWcwUi+ijUKp/h9NfE5c2W5m2VBdmRjBfjWo9jch
HV5gkkoG0Gdx7Kv60HKOMD12YkjL4zfAzBS8J8BMmk5x6sY+GqNQ0dgs7m4oXYCH
11o0YS6n910WDZcxXYWweINl6z0SI1ZYVIdwaE00MDvoA82tzTHFmMy2kA48FHJ
```

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

## General

- 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.

## Known Issues

This section lists known issues in Juniper Networks CSO Release 5.0.0.

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

### 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

## Site and Tenant Workflow

- An error occurs when you modify an SD-WAN rule that has a site group as the source.

Workaround: Instead of modifying an existing rule, add a new rule with the required changes and the site group as the source.

Bug Tracking Number: CXU-36715

- When you create an SD-WAN site with an EX Series switch for the branch network by using a site template, CSO fails to deploy the configuration to the primary enterprise hub if there are more than one enterprise hub sites.

Workaround: When there are more than one enterprise hub sites, do not use site templates to create sites.

Bug Tracking Number: CXU-36513

- When you create an SD-WAN site with an EX Series switch for the branch network by using a site template that has LAN segments for both the CPE device and the switch, CSO displays the error **Select at least one switch port for the CPE LAN Segment**.

Workaround: In the site template, add a LAN segment only for the switch. For the CPE device, add a LAN segment after ZTP is completed.

Bug Tracking Number: CXU-36474

- 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

- 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

## General

- 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

- 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.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-36594

- 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 the ZTP.

Bug Tracking Number: CXU-35385

- The job log for an EX Series device reboot does not show details of the reboot job.

Workaround: View the progress of the reboot job on the **Monitor > Jobs** page.

Bug Tracking Number: CXU-35366

- The status of GRE\_IPSEC tunnel between an on-premise spoke site with SRX340 as a CPE device and an enterprise hub is down.

Workaround: Reboot the device.

Bug Tracking Number: CXU-35348

- 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 interface, zones, or routing instances.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-35021

- ZTP of SRX Series devices fails because the default CA certificate is not installed on the device.

Workaround: Install the certificates on the device by using the CLI, reboot the device, and then retry ZTP.

Bug Tracking Number: CXU-34578

- 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 a Return Material Authorization (RMA) of a spoke, the LAN segment fails to connect to the enterprise hub.

Workaround: Reboot the spoke device.

Bug Tracking Number: CXU-35379

---

## Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.0.0:



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

Bug Tracking Number: CXU-32604

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

Bug Tracking Number: CXU-32812

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

Bug Tracking Number: CXU-32450

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

Bug Tracking Number: CXU-31304

---

## Documentation Updates

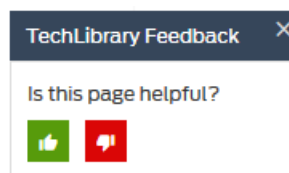
This section lists the errata and changes in the CSO documentation:

---

## Documentation Feedback

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

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



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

---

## Requesting Technical Support

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

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

## Self-Help Online Tools and Resources

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

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

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

## Creating a Service Request with JTAC

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

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

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

## Revision History

---

01 July 2019—Revision 1, CSO Release 5.0.0

08 July 2019—Revision 2, CSO Release 5.0.0

08 August 2019—Revision 3, CSO Release 5.0.0

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.