

Contrail Service Orchestration Release Notes

Release 5.4.0
December 09, 2020
Revision 3

These Release Notes accompany Release 5.4.0 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 | 4
- Software Installation Requirements for NFX Series Network Services Platform | 11

Accessing the CSO GUIs | 12

New and Changed Features in Contrail Service Orchestration Release 5.4.0 | 12

- SD-WAN | 13
- Miscellaneous | 14
- Deprecated Feature | 15

VNFs Supported | 15

Licensing | 16

Known Behavior | 16

- Device Management | 16
- Dynamic VPN (DVPN) | 17
- Policy Deployment | 18
- SD-WAN | 18
- Site and Tenant Workflow | 19
- User Interface | 20
- General | 20

Known Issues | 21

SD-WAN | 22

Security Management | 27

General | 27

Resolved Issues | 32

Documentation Feedback | 32

Requesting Technical Support | 33

Self-Help Online Tools and Resources | 33

Creating a Service Request with JTAC | 34

Revision History | 34

Introduction

You can use CSO Release 5.4.0 as a cloud-based service.

CSO Release 5.4.0 supports the following types of accounts:

- OpCo accounts (for multitenant, managed service providers)—OpCo (operating company) administrators can add tenants to and enable services such as SD-WAN, 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 accounts (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 5.4.0:

- **SD-WAN features**

- Support for overlapping addresses across departments in a tenant
- Support to enable or disable quality of service (QoS) from CSO
- Support for an OpCo administrator to configure traffic type profiles
- Support for configuring IEEE 802.1p in an application traffic profile
- Support for LTE access type for MPLS links
- Support for a configuration template to disable autonegotiation

- **Miscellaneous**

- Support for connecting CSO-managed tenants' networks to any existing IP (Layer 3) VPN
- Support for customizing portals and reports
- Support for adding serial numbers during site activation

Software Support

IN THIS SECTION

- [Software Downloads | 4](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 11](#)

Software Downloads

[Table 1 on page 4](#) displays the supported versions and download links for software components associated with CSO Release 5.4.0.

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 5.4.0

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.5R1	Pre-bundled with CSO.
NFX150 CPE device	Junos OS Release 19.3R2-S5	<ul style="list-style-type: none"> • Junos OS 19.3R2-S5 <ul style="list-style-type: none"> • Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110795.html?pf=NFX150 • Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/110724.html?pf=NFX150

Table 1: Software Components Associated with CSO Release 5.4.0 (*continued*)

Product	Supported Version	Download Link
NFX250 CPE device	<p>Junos OS Release 19.3R2-S5 for vSRX2.0</p> <p>Junos OS Release 18.4R3-S5</p>	<ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 <ul style="list-style-type: none"> Install media: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119341.html?pf=NFX250 Install package: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119270.html?pf=NFX250 Junos OS Release 18.4R3-S5 <ul style="list-style-type: none"> Install package (non flex): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114821.html?pf=NFX250

Table 1: Software Components Associated with CSO Release 5.4.0 (continued)

Product	Supported Version	Download Link
SRX Series CPE devices	Junos OS Release 19.3R2-S5	<p>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):</p> <ul style="list-style-type: none"> Junos OS 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html?pf=SRX300 <p>SRX1500</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html?pf=SRX1500 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html?pf=SRX1500 Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html?pf=SRX1500 <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html?pf=SRX4100 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html?pf=SRX4100 Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.4.0 (continued)

Product	Supported Version	Download Link
SRX Series next-generation firewall devices	Junos OS Release 19.3R2-S5	<p>SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M:</p> <ul style="list-style-type: none"> • Junos OS 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html?pf=SRX300 • Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html?pf=SRX1500 • Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html?pf=SRX1500 • Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html?pf=SRX1500 <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html?pf=SRX4100 • Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html?pf=SRX4100 • Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.4.0 (continued)

Product	Supported Version	Download Link
SRX Series provider hub devices	Junos OS Release 19.3R2-S5	<p>SRX1500</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html?pf=SRX1500 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html?pf=SRX1500 Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html?pf=SRX1500 <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html?pf=SRX4100 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html?pf=SRX4100 Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html?pf=SRX4100
SRX Series enterprise hub devices	Junos OS Release 19.3R2-S5	<ul style="list-style-type: none"> SRX1500: <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html?pf=SRX1500 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html?pf=SRX1500 SRX4100, SRX4200: <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5 (install package): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html?pf=SRX4100 Junos OS Release 19.3R2-S5 (install media): https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html?pf=SRX4100 Junos OS Release 19.3R2-S5 PXE: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html?pf=SRX4100

Table 1: Software Components Associated with CSO Release 5.4.0 (*continued*)

Product	Supported Version	Download Link
vSRX for SD-WAN devices	Junos OS Release 19.3R2-S5	<p>For hub devices (enterprise hub and provider hub) and spoke devices:</p> <ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.4.0 (continued)

Product	Supported Version	Download Link
vSRX for next-generation firewall devices	Junos OS Release 19.3R2-S5	<p>For hub devices (enterprise hub and provider hub) and spoke devices:</p> <ul style="list-style-type: none"> • vSRX (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html?pf=vSRX • vSRX (KVM appliance): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html?pf=vSRX • vSRX (Hyper-V image): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html?pf=vSRX • vSRX (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html?pf=vSRX • vSRX (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> • Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html?pf=vSRX

Table 1: Software Components Associated with CSO Release 5.4.0 (continued)

Product	Supported Version	Download Link
vSRX3.0 for SD-WAN devices, next-generation firewall, and hub devices	Junos OS Release 19.3R2-S5	<ul style="list-style-type: none"> vSRX3.0 (compressed tar file (TGZ) for upgrade): <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119389.html?pf=vSRX3.0 vSRX3.0 (KVM appliance): <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119401.html?pf=vSRX3.0 vSRX3.0 (Hyper-V image): <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119403.html?pf=vSRX3.0 vSRX3.0 (VMware appliance with SCSI virtual disk (.ova)): <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119402.html?pf=vSRX3.0 vSRX3.0 (VMware appliance with IDE virtual disk (.ova)): <ul style="list-style-type: none"> Junos OS Release 19.3R2-S5: https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119400.html?pf=vSRX3.0

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

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

For more information on NFX series documentation, see

https://www.juniper.net/documentation/product/en_US/nfx150 and

https://www.juniper.net/documentation/product/en_US/nfx250.

Accessing the CSO GUIs

NOTE: We recommend that you use Google Chrome (Version 60 or later) or Firefox (Version 78 or later) to access the CSO GUIs.

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

New and Changed Features in Contrail Service Orchestration Release 5.4.0

IN THIS SECTION

- [SD-WAN | 13](#)
- [Miscellaneous | 14](#)
- [Deprecated Feature | 15](#)

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 5.4.0.

You can view and read the features that are available in the CSO Releases 5.1.2, 5.2.0, and 5.3.0 through the following links:

- [CSO 5.3.0 Release Notes](#)
- [CSO 5.2.0 Release Notes](#)

- [CSO 5.1.2 Release Notes](#)

SD-WAN

NOTE: If you are a managed service provider who wants both the convenience of a CSO SaaS solution and the control of a CSO on-premises installation (possibly due to regulatory or compliance requirements), contact Juniper Networks to learn more about a dedicated CSO SaaS instance. CSO Release 5.4.0 with a dedicated CSO SaaS instance has a provider hub with both Data and OAM capabilities. The provider hub is connected to CSO through AWS Direct Connect.

- **Support for overlapping IP addresses across departments in a tenant**—From CSO Release 5.4.0 onward, you can use overlapping IP addresses across departments in a tenant when network segmentation is enabled for the tenant. For more information on overlapping IP addresses across departments, see the *Multidepartment CPE Device Support* in the *Customer Portal User Guide*.
- **Support to enable or disable QoS from CSO**—In CSO Release 5.4.0, we've added an attribute, Class of Service, to the Add Tenant page. If you disable this attribute, the tenant must configure quality of service (QoS) by using configuration templates instead of deriving the configuration from an application traffic type profile.
- **Support for an OpCo Administrator to configure application traffic type profiles**—In addition to a global application traffic type profile configured by the service provider, from CSO Release 5.4.0 onward, an OpCo Administrator can create, edit, or delete application traffic type profiles at the OpCo level.

Henceforth, all the tenants of an OpCo will use the application traffic type profiles added by that OpCo. Only the direct tenants of a service provider will use the application traffic type profiles added by the service provider.
- **Support for configuring IEEE 802.1p in an application traffic type profile**—From CSO Release 5.4.0 onward, you can configure IEEE 802.1p value and the drop priority of packets in an application traffic type profile to expedite traffic forwarding in a service provider network. You can assign an Expedited Forwarding (ef), Assured Forwarding (af), the Best Effort (be), or a Class Selector (CS) value for the IEEE 802.1p parameter. For more information on configuring IEEE 802.1p in an application traffic type profile, see, *Add Traffic Type Profiles* in the *Customer Portal User Guide*.
- **Support for LTE access type for MPLS links**—From CSO Release 5.4.0 onward, for SD-WAN on-premises spoke sites, you can configure LTE as the access type for MPLS links.

You configure LTE as the access type for MPLS links for the following single-CPE devices:

- NFX150 and NFX250
- SRX320, SRX340, and SRX345

NOTE: This is a Beta-quality feature.

- **Support for configuration templates to disable Ethernet autonegotiation**—From Release 5.4.0 onward, CSO provides configuration templates to disable Ethernet autonegotiation on the interfaces of SRX Series devices and NFX250 devices (Junos Control Plane (JCP) component only).

Miscellaneous

- **Support for connecting CSO-managed tenant networks to an existing IP (Layer 3) VPN**— From CSO Release 5.4.0 onward, Service Provider (SP) or Operating Company (OpCo) Administrator users in the tenant context can use the IP VPN (Layer 3) configuration to connect their existing networks (for example, traditional branch offices or data centers) that are not managed by CSO to a network managed by CSO through a provisioned provider hub site with OAM_AND_DATA or DATA_ONLY capability.
- **Support for customizing portals and reports**—From CSO Release 5.4.0 onward, Service Provider (SP) Administrators can customize themes and reports in the Administration and Customer Portals that can be used by tenant and OpCo Administrators.
- **Support for adding serial numbers during site activation**—From CSO Release 5.4.0 onward, tenant administrators can add on-premises spoke sites and enterprise hub sites, and Service Provider or OpCo Administrators can add provider hub sites without entering the serial number of the device associated with sites. The administrators must enter the serial numbers later while manually activating the sites.
- **Changes related to the anti-replay service**—From CSO Release 5.4.0 onward, the anti-replay service is disabled for CSO-provisioned IPSec tunnels.
- **Changes related to the routing model**—From CSO Release 5.4.0 onward, for SD-WAN the following are the changes in the routing model:
 - A unique routing instance (type virtual-router) is created for each WAN interface, named as WAN_X
 - A unique security untrust zone is created for each WAN interface, named as untrust-WAN_X. (X represents the WAN link number. Range: 0 through 3).

These changes are applicable for all WAN links on an on-premises spoke site and for MPLS WAN links on an enterprise hub site and will be applied automatically after Site upgrade.

If you have deployed a zone-based firewall policy or a NAT policy with zone as untrust, after you upgrade the site you must modify the policy with the new WAN interface zones and redeploy the policy.

Deprecated Feature

- **SD-LAN**—From CSO Release 5.4.0 onward, CSO does not support SD-LAN deployments. If you have added an EX Series switch in releases earlier than CSO Release 5.4.0, the management status of the switch is changed to Unmanaged.

VNFs Supported

CSO supports the VNFs listed in [Table 2 on page 15](#).

Table 2: VNFs Supported by Contrail Service Orchestration

VNF Name	Version	Network Functions Supported	Deployment Model Support
Juniper Networks vSRX3.0	For SD-WAN deployments: vSRX3.0 19.3R2-S5	<ul style="list-style-type: none"> • Network Address Translation (NAT) • Demonstration version of Deep Packet Inspection (DPI) • Firewall • Unified threat management (UTM) 	SD-WAN deployments supports NAT, firewall, and UTM.
Ubuntu	16.04		SD-WAN (all LAN-side functions) deployments—NFX250 and NFX150 platforms.
Fortinet	5.6.3		SD-WAN (all LAN-side functions) deployments—NFX250 and NFX150 platforms.

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.

Known Behavior

IN THIS SECTION

- [Device Management | 16](#)
- [Dynamic VPN \(DVPN\) | 17](#)
- [Policy Deployment | 18](#)
- [SD-WAN | 18](#)
- [Site and Tenant Workflow | 19](#)
- [User Interface | 20](#)
- [General | 20](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 5.4.0.

Device Management

- The SRX4100 and SRX4200 devices support all existing SD-WAN features, except the following:
 - Phone-home client (PHC)—The devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX4100 and SRX4200 devices, and then committing the stage-1 configuration.

- LTE and xDSL interfaces.
- In a dual SRX Series cluster, the devices must be manually activated by copying the stage-1 configuration from the CSO portal, pasting it to the console of the SRX Series device, and then committing the configuration.
- LTE and xDSL interfaces are not supported on dual CPE devices.
- You cannot remotely access a cloud spoke device and edit the configuration.
- You can install and use only an external LTE Vodafone K5160 dongle to the NFX250 device.
- NFX150 is not supported in cluster mode.
- UTM Web filtering is not supported in an active-active SRX Series cluster device.
- ADSL and VDSL are not supported on an NFX250 device running Junos OS Release 18.4R3.3.
- Prestaging is required for ZTP over PPPoE-enabled WAN link.
- For SRX series devices, you must manually install the device certificates after the ZTP is complete. To manually install the certificate, select the SRX series device on the **Resources > Devices** page and click **More > Install Certificates**.

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

Policy Deployment

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

SD-WAN

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

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*

User Interface

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

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

                                ADD A NEW LINE HERE

2C638z/Lgr/g4Kw7r9lys9XWnUGbGnPpT1cc5jGq1Qbb8Nu286QsVGfrUy7Qh9sU
FJkIQI9bOMNadLL7wklsnwBCVAoAYjX+haizSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWFGwCwUi+ijUKp/h9NfE5c2W5m2VBdmRjBfjWo9jcH
HV5gkkoG0Gdx7Kv60HKOMDl2YkjL4zfAzBS8J8BMmk5x6sY+GqNQOdgs7m4oXYCH
1loOYS6n9l0WDZcxXYWWeINlu6zOSIlZYVIIdwaE0OMDvoA82tzTHFmMy2kA48FHJ
```

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

General

- On an NFX Series device:
 - To activate a virtualized network function (VNF), perform the following steps:
 1. Add the VNF to the device.
 2. Initiate the activation workflow and ensure that the job is 100% completed.
 - To retry the activation of a VNF that failed, perform the following steps:
 1. Deactivate the VNF.
 2. Remove the VNF.
 3. Add the VNF to the device.
 4. Initiate the activation workflow and ensure that the job is 100% completed.
- Enterprise hub is not supported for cloud spoke sites.

- CSO internally uses IP addresses starting from 100.112.0.0 through 100.127.255.255. You must avoid using these IP addresses in LAN subnets.
- NFX250 uses some IP addresses in the 192.0.2.0/24 subnet for VNF management. You must avoid using these IP addresses in a LAN. For more information about the usage of this subnet, see the [NFX250 documentation](#).
- VLAN IDs 4050 through 4094 are reserved for CSO configurations.
- If a tenant has an overlapping IP address configured across departments, then to access the resources in the enterprise hub's data center, you must apply a source NAT rule with source as the trust zone and destination as the data center department zone on the enterprise hub device.
- If an overlapping IP address is configured on the same site across departments, hosts in the overlapping subnet are unable to deterministically access data center routes behind nonprimary enterprise hubs.
- The end-to-end traffic cannot be established if two LAN hosts within a tenant have traffic such that all the 5 tuples are exactly the same and the destination IP address is in the data center that is hosted behind nonprimary enterprise hubs.

Known Issues

IN THIS SECTION

- [SD-WAN | 22](#)
- [Security Management | 27](#)
- [General | 27](#)

This section lists known issues in Juniper Networks CSO Release 5.4.0.

SD-WAN

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

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

Bug Tracking Number: CXU-23107

- When configuring a DVPN tunnel between two devices, if one device is not functional while the other is functional, the DVPN tunnel should not be configured on the device that is functional.

Workaround: There is no known workaround. If a DVPN tunnel is configured on the functional device, delete the tunnel manually.

Bug Tracking Number: CXU-46188

- VNFs are not coming up in NFX150 running on Junos OS Release 19.3R2-S3 due to non availability of the required number of CPUs.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-49268

- Upgrade of Junos OS Release 15.1X49-D172 to Junos OS Release 19.3R2-S3 fails on SRX 4100, SRX4200, and SRX300 dual CPE clusters, when functioning as enterprise hubs, due to incorrect IPsec configuration and CLI validations.

Workaround: To upgrade the Junos OS image from Release 15.1X49-D172 to Release 19.3R2-S5:

1. Log in to Customer Portal.
2. Navigate to **Resources > Templates > Configuration Template**.
3. Select the **srx-router** template and click **Deploy to Devices**.
4. Select the device that you want to upgrade and click **Next**.
5. Select **Is Admin** for the device and click **Next**.

The Configure Device Parameters tab is displayed.

6. Select the device that you want to upgrade and click the **Set Parameters** button above the Device table.

The Device Configuration for the Device page appears.

7. Click the **Is Admin** toggle button to enable the **Is Admin** option.

The router gets administrator privileges.

8. Click **Save** to save the configuration.

9. Click **Next**.

The Deploy tab is displayed.

10. Select **Run now** for Choose Deployment Time.

11. Click **Finish**.

12. Access the terminal of the primary device.

To access the device terminal:

- a. Navigate to **Resources > Devices**.
- b. Select the device and click **More > Remote Console**.

13. On the device console, access the shell and enter the following command:

```
cli -c 'show configuration | display set | grep encryption-algorithm | grep cbc
| grep "ike proposal"' | awk -Fencryption-algorithm '{b=$1"
authentication-algorithm sha-256"; print b}'
```

14. Copy the output displayed to a text file.

15. Again, enter the following command:

```
cli -c 'show configuration | display set | grep encryption-algorithm | grep cbc
| grep "ipsec proposal"' | awk -Fencryption-algorithm '{b=$1"
authentication-algorithm hmac-sha-256-128"; print b}'
```

16. Append the text file with the output of the command executed in Step 15.

17. Switch to edit mode on the device by typing **Edit** at the command prompt.

18. Copy the commands from the text file and paste them into the device CLI.

19. Copy the Junos OS Release 19.3R2-S3 image to the device either by using CSO or manually.

To copy the image to the device by using CSO:

- a. Switch to Administration Portal.
- b. Navigate to **Resources > Images**.
- c. Click the **Add** icon (+) to upload the image.
- d. Wait until the upload is successful.
- e. Switch to Customer Portal.
- f. Navigate to **Resources > Images** and select the uploaded image.
- g. Click **Stage**.
- h. On the Stage Image page, select the device, ensure **Run Now** is selected for Choose Deployment time, and click **OK**.

The device image is copied only to the primary device.

20. Copy the image to the backup device.

To copy the image to the backup device, access the remote terminal of the backup device by referring to [Step 12](#) and enter the following command:

```
file copy <image location> nodex <new image location>
```

Where, <image with location> nodex is the location of the image on node x, and

<new image location> is the location to where the image should be copied to the backup device.

21. After the image is copied to both the primary and the backup devices, access the **Remote Console** option of the primary device from CSO.

22. Log in to the backup device from the primary device:

```
primary:node0}
user@node0> request routing-engine login node 1
```

23. On the backup device, issue the upgrade command **request system software add /var/tmp/image-name no-validate**.

```
{backup:node1}
user@node1> request system software add
/var/tmp/<junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

Host OS upgrade staged. Reboot the system to complete installation!

```
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete junos'
WARNING:      command as soon as this operation completes.
```

```
WARNING:      The DHCP configuration command used will be deprecated in future
Junos releases.
```

```
WARNING:      Please see documentation for updated commands.
```

```
Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

24. After the image on the backup device is upgraded successfully, open another remote console on the primary device and upgrade the image on the primary device.

```
{primary:node0}
user@node0> request system software add
/var/tmp/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

Host OS upgrade staged. Reboot the system to complete installation!

```
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete junos'
WARNING:      command as soon as this operation completes.
```

```

WARNING:      The DHCP configuration command used will be deprecated in future
               Junos releases.
WARNING:      Please see documentation for updated commands.

Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...

```

25. Reboot the backup device.

```

{backup:node1}
root@node1> request system reboot
Reboot the system ? [yes,no] (no)yes

```

26. Immediately open another remote console and reboot the primary device.

```

{primary:node0}
root@node0> request system reboot
Reboot the system ? [yes,no] (no)yes

```

27. After both the devices are up, redeploy the srx-router template on the primary device by disabling the **Admin** option.

Bug Tracking Number: CXU-50068

- If you are an Opco administrator and edit the OAM and CONTROL traffic profiles after your tenants have deployed SD-WAN policy intents, then the changes are not immediately applied on your tenant devices.

Workaround: The changes are applied to the device only when your tenants redeploy the SD-WAN policy.

Bug Tracking Number: CXU-52482

- For a site-to-site tunnel, if the WAN link on one site is marked as active and the WAN link for the other site is marked as backup, then the tunnel is not considered as a backup tunnel for the site with the WAN link marked as active.

Workaround: You must avoid configuring WAN links with the same mesh tag as active on one site and backup on the other site.

Bug Tracking Number: CXU-51919

- You must specify the same value for the Loss Priority field on the SLA Profile page and the Traffic Type Profile page; otherwise, the Loss Priority parameter might not be applied during the traffic congestions.

Workaround: Ensure that you specify the same value for the Loss Priority field on the SLA Profile and Traffic Type Profile pages.

Bug Tracking Number: CXU-52516

Security Management

- 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

General

- 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

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41210

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-41259

- Tenant owned Public IP Pool can be edited until the first SD-WAN site is onboarded in that tenant. After you onboard an SD-WAN site, Tenant owned Public IP Pool cannot be edited.

Bug Tracking Number: CXU-41139

- 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

- Installation of licenses on SRX1500 and SRX4200 dual CPE clusters by using CSO is failing.

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

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

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

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

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

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

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

Bug Tracking Number: CXU-40522

- Image upgrade on an SRX4X00 Series cluster fails as the ISSU upgrade command throws an error due to real-time performance monitoring (RPM) configuration. This issue is only applicable when you upgrade from Junos Release 15.149-D172.

Workaround: To upgrade an SRX4X00 Series cluster:

1. Log in to CSO Customer Portal and apply the *srx-router* configuration template on the primary device in the cluster.
2. Deploy the configuration template on the primary device by enabling the **Admin** option for the device.
3. Copy the image to be upgraded on to both the primary and the backup devices by using CSO or manually.
4. After the image is copied on both the primary and the backup devices, access the **Remote Console** option for the device from CSO.

5. Log in to the backup device from the primary device:

```
primary:node0}
user@node0> request routing-engine login node 1
```

6. On the backup device, issue the upgrade command **request system software add /var/tmp/<image-name> no-validate**.

```
{backup:node1}
user@node1> request system software add
/var/tmp/<junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

Host OS upgrade staged. Reboot the system to complete installation!

```
WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete junos'
WARNING:      command as soon as this operation completes.
```

```
WARNING:      The DHCP configuration command used will be deprecated in future
Junos releases.
```

```
WARNING:      Please see documentation for updated commands.
```

```
Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...
```

7. After the image on the backup device is upgraded successfully, open another remote console on the primary device and upgrade the image on the primary device.

```
{primary:node0}
user@node0> request system software add
/var/tmp/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz no-validate
```

Host OS upgrade staged. Reboot the system to complete installation!

```

WARNING:      A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:      'request system reboot' command when software installation is
WARNING:      complete. To abort the installation, do not reboot your system,
WARNING:      instead use the 'request system software delete junos'
WARNING:      command as soon as this operation completes.

WARNING:      The DHCP configuration command used will be deprecated in future
Junos releases.
WARNING:      Please see documentation for updated commands.

Saving package file in /var/sw/pkg/junos-srxmr-x86-64-19.3R2-S1.2-signed.tgz
...

```

8. Reboot the backup device.

```

{backup:node1}
root@node1> request system reboot
Reboot the system ? [yes,no] (no)yes

```

9. Immediately open another remote console and reboot the primary device.

```

{primary:node0}
root@node0> request system reboot
Reboot the system ? [yes,no] (no)yes

```

10. After both the devices are up, redeploy the srx-router template on the primary device by disabling the **Admin** option.

The image is now upgraded on both the devices of the cluster.

Bug Tracking Number: CXU-39491

- Link metric widgets do not show data as expected when an analytics node is down.

Workaround: Bring up the analytics node to view link metric widgets correctly.

Bug Tracking Number: CXU-30813

- When you install the license on the backup node of an SRX dual CPE cluster, the installation fails.

Workaround: To install license on the backup node of an SRX dual CPE cluster by using CSO:

1. Install license on the primary node by using CSO

2. Reboot the primary node to switch the backup node to function as the primary node.
3. After the backup node becomes the primary node, install license for the backup node (currently working as the primary node) by using CSO.

Bug Tracking Number: CXU-43085

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

Workaround: There is no known workaround.

Bug Tracking Number: CXU-32157

- When you upgrade the image for SRX4200 dual CPE device, the job status is displayed as Success even though the reboot is in progress for the secondary node.

Workaround: Check the status of the cluster and the FPC status on the primary node before proceeding with any other activity on the CPE device.

Bug Tracking Number: CXU-52974

- The Initiate RMA option is disabled if the bootstrapping of the device fails and if the device status is Bootstrap_Failed.

Workaround: Delete the site and add a new site.

Bug Tracking Number: CXU-52896

- Fortinet and Ubuntu service chaining instance fails on NFX250.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-52817

- Ubuntu service chaining instance fails on NFX150.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-52512

- The site upgrade fails if a site is associated with the SRX340 device.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-52898

Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 5.4.0:

- Sometimes, jobs to update NAT information are not getting triggered. Therefore, NAT port assigned to a DVPN IPsec configuration is incorrect.

Bug Tracking Number: CXU-46183

- While creating an IPsec tunnel between an Internet link that is behind NAT in a spoke to an MPLS link in an ENT hub, wrong NAT interface is configured on the IPsec tunnel. Therefore, the tunnel fails to be created.

Bug Tracking Number: CXU-46185

- When you edit an enterprise hub site by adding a WAN link, static tunnels are not established with connected spoke sites automatically.

Bug Tracking Number: CXU-44427

- While you deploy the VRRP configuration templates on SRX Series devices, the template does not render as expected on the Devices page of the CSO GUI.

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

Bug Tracking Number: CXU-41793

- When CSO is upgraded to Release 5.2.0 and if an enterprise hub site is in an earlier release (for example, 5.1.0 or 5.1.1), then adding a LAN segment to a spoke or an enterprise hub using a new department or deleting a LAN segment from the spoke or enterprise hub might fail.

Bug Tracking Number: CXU-47394

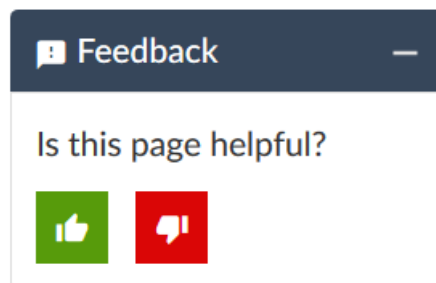
- In case of an AppQoE event (packet drop or latency), the application may not switch to the best available path among the available links.

Bug Tracking Number: CXU-41922

Documentation Feedback

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

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



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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>

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

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

Creating a Service Request with JTAC

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

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

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

Revision History

Nov 20, 2020—Revision 1, CSO Release 5.4.0

Nov 24, 2020—Revision 2, CSO Release 5.4.0

Dec 09, 2020—Revision 3, CSO Release 5.4.0

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.