

# Contrail Service Orchestration Release Notes

Release 6.1.0  
June 28, 2021  
Revision 1

These Release Notes accompany Release 6.1.0 of Juniper Networks® Contrail Service Orchestration (CSO). These Release Notes describe new and changed features, limitations, and known and resolved issues in the software.

Contents

Introduction | 3

Software Support | 4

- Software Downloads | 4
- Software Installation Requirements for NFX Series Network Services Platform | 17

Accessing the CSO GUIs | 17

New and Changed Features in Contrail Service Orchestration Release 6.1.0 | 18

- Zero Touch Provisioning | 19
- SD-WAN | 19
- Miscellaneous | 21

VNFs Supported | 22

Licensing | 23

Known Behavior | 24

- Device Management | 24
- Dynamic VPN (DVPN) | 25
- Policy Deployment | 25
- SD-WAN | 26
- Site and Tenant Workflow | 26
- User Interface | 27
- General | 28

Known Issues | 29

SD-WAN | 29

High Availability | 31

Security Management | 31

Site and Tenant Workflow | 31

General | 32

Resolved Issues | 33

Documentation Feedback | 35

Requesting Technical Support | 36

Self-Help Online Tools and Resources | 36

Creating a Service Request with JTAC | 37

Revision History | 37

# Introduction

Juniper Networks offers Contrail Service Orchestration (CSO) Release 6.1.0 as a cloud-based service. You can also deploy CSO Release 6.1.0 on-premises for customers that demand full control over their deployments.

CSO Release 6.0.0 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 6.1.0:

- Zero Touch Provisioning
  - Simplified Zero Touch Provisioning (ZTP) process
- **SD-WAN**
  - Support for SD-WAN Essentials service
  - PPPoE or PPP support per WAN link
  - Create static tunnels between branch site and enterprise hubs
  - Support to configure aggregated Ethernet on enterprise hub WAN links
  - Support for automatic cluster formation for SRX Series dual CPE devices
  - Support for IPv6 connectivity on WAN links
  - Support for MAP-E functionality on NFX150 devices
  - Support for editing hub configuration of a WAN link
  - Support for editing LAN segments
  - Support to view throughput for WAN links
  - Support to automatically revert AppQoE traffic to the preferred link
- **Miscellaneous**
  - Discover an EX Series switch or an AP configured behind an SRX Series CPE
  - View information about SRX Series CPE, EX Series switch, or AP on Juniper Mist

- Change related to site type
- Enhancements to the Device Details page
- Support for editing site name
- Support for NAT Configuration Template for Provider Hub Breakout
- Support for configuring two WAN links on a physical port
- Support to generate device RSI
- Remote CLI access using Junos login credentials

## Software Support

### IN THIS SECTION

- [Software Downloads | 4](#)
- [Software Installation Requirements for NFX Series Network Services Platform | 17](#)

## Software Downloads

[Table 1 on page 5](#) displays the supported versions and download links for software components associated with CSO Release 6.1.0.

### NOTE:

- Before you onboard devices, ensure that the device is running the software version that is recommended in this release notes.
- All new site onboarding must be with Junos Release 20.2R2-S3.5. Whereas, the exiting CSO 5.4 sites should continue to work with Junos Release 19.3R2-S5.7. To use the CSO 6.0.0 features for existing sites, refer to the site upgrade workflow.

Table 1: Software Components Associated with CSO Release 6.1.0

Product	Supported Version	Download Link
Juniper Identity Management Service (JIMS)	1.1.5R1	Pre-bundled with CSO.
NFX150 CPE device	Junos OS Release 20.2R2-S3.5	<ul style="list-style-type: none"> <li>• Install media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125809.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125809.html</a></li> <li>• Install package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125788.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125788.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	<ul style="list-style-type: none"> <li>• Install media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119341.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119341.html</a></li> <li>• Install package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119270.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119270.html</a></li> </ul>
NFX250 CPE device	Junos OS Release 20.2R2-S3.5 for vSRX2.0	<ul style="list-style-type: none"> <li>• Install media: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125809.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125809.html</a></li> <li>• Install package: <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125788.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125788.html</a></li> </ul>
	Junos OS Release 18.4R3-S5	<ul style="list-style-type: none"> <li>• Install package (non flex): <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114821.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/114821.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
SRX Series CPE devices	Junos OS Release 20.2R2-S3.5	<p>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125782.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125782.html</a></li> </ul> <p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	

Table 1: Software Components Associated with CSO Release 6.1.0 (*continued*)

Product	Supported Version	Download Link
		<p>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html</a></li> </ul> <p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (*continued*)

Product	Supported Version	Download Link
SRX Series next-generation firewall devices	Junos OS Release 20.2R2-S3.5	<p>SRX300, SRX320, SRX340, SRX345, and SRX550 High Memory Services Gateway (SRX550M) (as spoke devices):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125782.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125782.html</a></li> </ul> <p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	

Table 1: Software Components Associated with CSO Release 6.1.0 (*continued*)

Product	Supported Version	Download Link
		<p>SRX300, SRX320, SRX340, SRX345, SRX550, SRX550M:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119295.html</a></li> </ul> <p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
SRX Series provider hub devices	Junos OS Release 20.2R2-S3.5	<p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	

Table 1: Software Components Associated with CSO Release 6.1.0 (*continued*)

Product	Supported Version	Download Link
		SRX1500: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html</a></li> </ul> SRX1500 USB: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html</a></li> </ul> SRX1500 PXE: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html</a></li> </ul> SRX4100, SRX4200: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html</a></li> </ul> SRX4100, SRX4200 USB: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html</a></li> </ul> SRX4100, SRX4200 PXE: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
SRX Series enterprise hub devices	Junos OS Release 20.2R2-S3.5	<p>SRX1500:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125781.html</a></li> </ul> <p>SRX1500 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125824.html</a></li> </ul> <p>SRX1500 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125875.html</a></li> </ul> <p>SRX4100, SRX4200:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125783.html</a></li> </ul> <p>SRX4100, SRX4200 USB:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125825.html</a></li> </ul> <p>SRX4100, SRX4200 PXE:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125876.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	

Table 1: Software Components Associated with CSO Release 6.1.0 (*continued*)

Product	Supported Version	Download Link
		SRX1500: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119294.html</a></li> </ul> SRX1500 USB: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119324.html</a></li> </ul> SRX1500 PXE: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119366.html</a></li> </ul> SRX4100, SRX4200: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119296.html</a></li> </ul> SRX4100, SRX4200 USB: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119325.html</a></li> </ul> SRX4100, SRX4200 PXE: <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119367.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
vSRX for SD-WAN devices	Junos OS Release 20.2R2-S3.5	<p>vSRX Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125914.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125914.html</a></li> </ul> <p>vSRX KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125927.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125927.html</a></li> </ul> <p>vSRX Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125926.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125926.html</a></li> </ul> <p>vSRX VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125929.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125929.html</a></li> </ul> <p>vSRX VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125928.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125928.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	<p>vSRX Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html</a></li> </ul> <p>vSRX KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html</a></li> </ul> <p>vSRX Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html</a></li> </ul> <p>vSRX VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html</a></li> </ul> <p>vSRX VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
vSRX for next-generation firewall devices	Junos OS Release 20.2R2-S3.5	<p>vSRX Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125914.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125914.html</a></li> </ul> <p>vSRX KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125927.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125927.html</a></li> </ul> <p>vSRX Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125926.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125926.html</a></li> </ul> <p>vSRX VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125929.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125929.html</a></li> </ul> <p>vSRX VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125928.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125928.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	<p>vSRX Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119388.html</a></li> </ul> <p>vSRX KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119397.html</a></li> </ul> <p>vSRX Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119396.html</a></li> </ul> <p>vSRX VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119399.html</a></li> </ul> <p>vSRX VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119398.html</a></li> </ul>

Table 1: Software Components Associated with CSO Release 6.1.0 (continued)

Product	Supported Version	Download Link
vSRX3.0 for SD-WAN devices, next-generation firewall, and hub devices	Junos OS Release 20.2R2-S3.5	<p>vSRX3.0 Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125915.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125915.html</a></li> </ul> <p>vSRX3.0 KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125931.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125931.html</a></li> </ul> <p>vSRX3.0 Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125933.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125933.html</a></li> </ul> <p>vSRX3.0 VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125932.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125932.html</a></li> </ul> <p>vSRX3.0 VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125930.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/125930.html</a></li> </ul>
	Junos OS Release 19.3R2-S5.7	<p>vSRX3.0 Upgrade TGZ:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119389.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119389.html</a></li> </ul> <p>vSRX3.0 KVM Appliance:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119401.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119401.html</a></li> </ul> <p>vSRX3.0 Hyper V Image:</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119403.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119403.html</a></li> </ul> <p>vSRX3.0 VMware Appliance with SCSI virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119402.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119402.html</a></li> </ul> <p>vSRX3.0 VMware Appliance with IDE virtual disk (.ova):</p> <ul style="list-style-type: none"> <li>• <a href="https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119400.html">https://webdownload.juniper.net/swdl/dl/secure/site/1/record/119400.html</a></li> </ul>

## Software Installation Requirements for NFX Series Network Services Platform

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

1. Upload the software image to CSO.

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

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

For more information on NFX series documentation, see [https://www.juniper.net/documentation/product/en\\_US/nfx150](https://www.juniper.net/documentation/product/en_US/nfx150) and [https://www.juniper.net/documentation/product/en\\_US/nfx250](https://www.juniper.net/documentation/product/en_US/nfx250).

## 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 *Access the Contrail Services Orchestration (CSO) GUIs* topic in the *CSO Deployment Guide*.

# New and Changed Features in Contrail Service Orchestration Release 6.1.0

## IN THIS SECTION

- [Zero Touch Provisioning | 19](#)
- [SD-WAN | 19](#)
- [Miscellaneous | 21](#)

This section describes the new features or enhancements to existing features in Contrail Service Orchestration (CSO) Release 6.1.0.

You can view and read the features that are available in the CSO Releases 5.1.2, 5.2.0, 5.3.0, and 5.4.0 through the following links:

- [CSO 6.0.0 Release Notes](#)
- [CSO 5.4.0 Release Notes](#)
- [CSO 5.3.0 Release Notes](#)
- [CSO 5.2.0 Release Notes](#)
- [CSO 5.1.2 Release Notes](#)

## Zero Touch Provisioning

- **Simplified Zero Touch Provisioning (ZTP) process**—Starting from CSO Release 6.0.0, the ZTP process is simplified to provide more flexibility and enable faster deployment of devices in a network. The device management and service provisioning processes are separated, thus reducing the time required for CSO to onboard and manage a device. For branch and enterprise hub sites, you can choose to either onboard a device with a service (SD-WAN or next-generation firewall) configured on it or configure the service later.

## SD-WAN

- **Support for SD-WAN Essentials service**—Starting in Release 6.0.0, CSO supports SD-WAN Essentials service. You can choose from the following SD-WAN service levels for a tenant:
  - *Essentials*—Provides the basic SD-WAN service (called Secure SD-WAN Essentials). This service level is ideal for small enterprises looking for managing simple WAN connectivity with comprehensive NGFW security services at the branch sites, using link-based application steering. The SD-WAN Essentials service allows Internet traffic to breakout locally, and thus avoids the need to backhaul web traffic over costly VPN or MPLS links. You can upgrade the SD-WAN service level of a tenant from Essentials to Advanced seamlessly (without downtime) by editing the tenant parameters, provided that you have purchased the corresponding license.
  - *Advanced*—Provides the complete SD-WAN service (called Secure SD-WAN Advanced). This service level is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. You can establish site-to-Site connectivity by using a hub in a hub-and-spoke topology or through static or dynamic full mesh VPN tunnels. Enterprise wide intent based SD-WAN policies and service-level agreement (SLA) measurements allow to differentiate and dynamically route traffic for different applications.

**NOTE:** Tenants with SD-WAN service on CSO Release 5.4.0 or earlier versions are treated as Secure SD-WAN Advanced tenants.

- **PPPoE or PPP support per WAN link**—Starting in CSO Release 6.0.0, you can enable PPPoE (Point-to-Point Protocol over Ethernet) or PPP (Point-to-Point Protocol) per WAN link on a branch site device, and specify the PPPoE or PPP authentication parameters per WAN link. You can enable PPPoE or PPP on MPLS-based or Internet-based WAN links. You can also enable PPPoE or PPP per WAN link on the devices in existing sites after the CSO upgrade, by editing the site information.

**NOTE:**

- The access type LTE can be used for only one WAN link on the device.
- MPLS-based links support only Ethernet or LTE as access types.

- **Support for creation of static tunnels between branch site and Enterprise hub based on user inputs**—Starting in CSO Release 6.0.0, you can create static tunnels between a branch site and enterprise hub sites (primary and secondary enterprise hubs). By default, CSO uses mesh tags to setup tunnels between branch sites and enterprise hubs. You need to disable the mesh tag-based tunnel creation to manually connect the branch site to an enterprise hub. This feature gives you control on how you want to define the tunnels. You can select a tunnel type to be used, the enterprise hub device to be connected, and the WAN links on the enterprise hubs with which connection needs to be established.
- **Support to configure aggregated Ethernet on enterprise hub WAN links** — In CSO Release 6.0.0, you can preconfigure an enterprise hub (SRX Series devices) with aggregated Ethernet links and Link Aggregation Control Protocol configurations before Zero Touch Provisioning is initiated to onboard the device in CSO.
- **Support for automatic cluster formation for SRX Series dual CPE devices**—Starting from CSO Release 6.0.0, you can enable automatic cluster formation for SRX Series dual CPE devices when you add a branch site or enterprise hub site.
- **Support for IPv6 connectivity on WAN links**—Starting from Release 6.0.0, CSO supports IPv6 for underlay connectivity on WAN links of SRX Series (CPE and provider hub) devices and NFX150 devices.
- **Support for MAP-E functionality on NFX150 devices**—Starting from CSO Release 6.0.0, for branch sites with NFX150 as the CPE, you can enable the Mapping of Address and Port with Encapsulation (MAP-E) functionality to transport IPv4 packets across an IPv6 network by using IPv4-in-IPv6 encapsulation.

**NOTE:** This feature is compliant only with the Japan Network Enabler (JPNE) standards.

- **Support for editing hub configuration of a WAN link**—Starting from CSO Release 6.0.0, you can edit the hub configuration associated with a branch site or an enterprise hub site. You can add, delete, or swap roles of primary and secondary provider hubs and enterprise hubs respectively.
- **Support for editing LAN segments**—Starting from CSO Release 6.0.0, you can edit the LAN segments deployed on a branch site or an enterprise hub site. You can also edit the associated department and add a LAG interface.
- **Support to view throughput for WAN links**—Starting from Release 6.0.0, you can view the throughput (in bps) for all WAN links associated to a branch site, an enterprise hub, or a provider hub.
- **Support to automatically revert AppQoE traffic to the preferred link type**—Starting from CSO Release 6.0.0, you can:

1. Select either Internet or MPLS or Any as the preferred link type for an SLA profile. By default, the preferred link type is Any.
2. Configure the link affinity for the preferred link.
3. Specify the link priority for WAN links in branch, enterprise hub, or cloud spoke sites.

The following is the behavior for link affinity:

- **Strict link affinity is selected for a preferred link type**—In the event of an SLA violation on the preferred link type, AppQoE ensures that the path selected is always of the preferred link type. If multiple links of the preferred link type are available, then the traffic selects the link that has the highest priority and meets the SLA.
- **Strict link affinity is not selected for a preferred link type**—In the event of an SLA violation on the preferred link type, the traffic switches over to a link that meets the SLA. If multiple links meeting the SLA are available, then the traffic switches over to the link with the highest priority. If the traffic switches over to a non-preferred link type, then the traffic automatically reverts to the preferred link type when the preferred link type recovers and conforms to the SLA.
- **Integration of CentOS-based Contrail Analytics Nodes**—Starting from CSO Release 6.0.0, Contrail Analytics Nodes (CAN) run on CentOS version 7.7.1908. Upgrading CAN data from CSO Release 5.1.2 to CSO 6.0.0 is not supported because of the database schema changes. As a workaround, after the upgrade procedure is completed, maintain the CSO Release 5.1.2 CAN VMs for 30 days. For details, see [Upgrade Contrail Service Orchestration from Release 5.1.2 to Release 6.0.0](#).

## Miscellaneous

- **Discover an EX Series switch or an AP configured behind an SRX Series CPE**—Starting from Release 6.0.0, CSO supports discovering an EX Series switch or an access point (AP) connected to an SRX Series Customer Premise Equipment (CPE) device. To discover the switch, CSO allows you to enable LLDP on the CPE interface and create a management connectivity between the CPE and the switch or AP through a zone-based LAN segment. You can use a physical port, a LAG interface, or a redundant Ethernet (reth) interface (for dual-CPE sites) to connect a CPE to a switch. This feature includes support to:
  - Create a LAG interface, reth interface (for dual-CPE sites), and redundancy groups.
  - Create a zone-based LAN segment and include the CPE interface (physical port, LAG interface, or reth interface) in it.
- **View information about SRX Series CPE, EX Series switch, or AP on Juniper Mist**—Starting from CSO Release 6.0.0, you access Juniper Mist from CSO Device page (**Resources > Devices**) to view information about the following devices (if they are available in the Juniper Mist portal):
  - SRX Series CPE devices.

- The EX Series switches that are connected to SRX Series CPE devices and are discovered by CSO.
- The access points that are connected to SRX Series CPE devices and are discovered by CSO.
- **Change related to site type**—Starting from CSO Release 6.0.0, on-premise spoke sites are called branch sites.
- **Enhancements to the Device Details page**—Starting from CSO Release 6.0.0, you can use the following enhancements on the Device Details page:
  - **Inventory** tab to view the chassis information, physical and logical interfaces from the CSO GUI. You can also view and manage the licenses and software images from this tab.
  - **Running Configuration** tab under the **Configuration** tab to view the current configuration on the device. This tab also provides the option to access the device console remotely.
- **Support for editing site name**—Starting from CSO Release 6.0.0, site name and device host name can be edited for branch sites, enterprise hubs, and DATA\_ONLY provider hubs.
- **Support for NAT Configuration Template for Provider Hub Breakout**—Starting from CSO Release 6.0.0, CSO provides a NAT template to configure NAT on provider hubs for central breakout of data traffic. The NAT can be applied to existing WAN interfaces in provider hubs with DATA\_ONLY and DATA\_and\_OAM capabilities. The preconfigured breakout/NAT template is available for CSOaaS and on-premises deployments.
- **Support for configuring and mapping two WAN interfaces to a single physical port on an NFX150 device**—Starting from CSO Release 6.0.0, you can configure and map up to two WAN (ge-1/0/x) interfaces to a single physical port (heth-0-x) on an NFX150 device. In releases before CSO Release 6.0.0, you can configure and map only one WAN interface to a single physical port on an NFX150 device.
- **Support to generate device RSI**—Starting from Release 6.0.0, CSO enables you to generate the request support information (RSI) log file for provider hub, enterprise hub, and spoke devices.
- **Remote CLI access using Junos login credentials**—Starting from CSO Release 6.0.0, you can remotely access the CPE device CLI in read-write (configuration) mode using your Junos login credentials. Alternatively, you can access the CLI in read-only (operational) mode.

## VNFs Supported

CSO supports the VNFs listed in [Table 2 on page 23](#).

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"> <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>	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 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 | 24](#)
- [Dynamic VPN \(DVPN\) | 25](#)
- [Policy Deployment | 25](#)
- [SD-WAN | 26](#)
- [Site and Tenant Workflow | 26](#)
- [User Interface | 27](#)
- [General | 28](#)

This section lists known behavior, system maximums, and limitations in hardware and software in Juniper Networks CSO Release 6.1.0.

## 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.
- 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 18.4R.

- 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.
- You cannot add a LAN segment to a Dual SRX site in CSO upgraded to Release 6.0.0 if the site has not been upgraded.

So, to add a LAN segment to a site, you must first do the following:

- Upgrade the site (See [Upgrading Sites](#)).
- Update the Dual\_SRX\_Platform template with the correct FAB interface details (See [Configuring Template Settings in a Device Template](#)).

After the above steps, add the LAN segment to the site from Device page on the LAN tab. While adding the LAN segment details, remember to create RETH interface and enable LACP. See [Add a Branch Site with SD-WAN Capability](#).

## Site and Tenant Workflow

- Sites are automatically upgraded to the current CSO version after performing RMA of an old site (prior to site upgrade).

Workaround: There is no known workaround.

Bug Tracking Number: CXU-55740

- 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/g4Kw7r9lys9XWnUGbGnPpTlcc5jGq1Qbb8Nu286QsVGfrUy7Qh9sU
FJkIQI9bOMNadLL7wklsnwBCVAoAYjX+haizSaZzDphT6XBzph35BN9M0Zmb+Kpn
fH5i5FZx8FJixbnonCmaVrWFGWcwUi+ijUKp/h9NfE5c2W5m2VBdmRjBfjWo9jcH
HV5gkkoG0Gdx7Kv60HKOMDl2YkjL4zfAzBS8J8BMmk5x6sY+GqNQOdgs7m4oXYCH
1loOYS6n9l0WDZcxXYWWeINlu6zOSilZYVIdwaE0OMDvoA82tzTHFmMy2kA48FHJ

```

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 | 29](#)
- [High Availability | 31](#)
- [Security Management | 31](#)
- [Site and Tenant Workflow | 31](#)
- [General | 32](#)

This section lists known issues in Juniper Networks CSO Release 6.1.0.

### SD-WAN

- In case of SRX3xx chassis cluster, data tunnels on secondary node are reported as down. Traffic continues to flow through tunnels connected to the primary node.

Workaround: There is no known workaround.

Bug Tracking Number: PR 1574912

- When an SD-WAN controller is down or not reachable from CSO, you cannot delete a site or tenant from CSO.

Workaround: Recover the SD-WAN controller and retry deleting the site or tenant.

Bug Tracking Number: CXU-43724

- 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: 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

- 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

- 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

## High Availability

- On an SRX4200 chassis cluster, LAN segment with aggregated interface with LLDP enabled fails.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-54985

## Security Management

- On NFX150 and NFX250 devices, firewall policies are not applied automatically after RMA.

Workaround: After the RMA is done, you must apply the policy configurations again after adding the necessary licenses, certificates, and signatures.

Bug Tracking Number: CXU-51335

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

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

Bug Tracking Number: CXU-23927

## Site and Tenant Workflow

- When the non-preferred link-type for an application transitions from **SLA violated** to **SLA met**, during the time when the non-preferred link-type is being used. The application flow does not transition to preferred link type even if it is available. This happens till the time non-preferred link-type again transitions to **SLA violated**.

Workaround: Bounce the non-preferred link type.

Bug Tracking Number: CXU-55353

- Site edit might fail in case of conflicting user defined templates deployed on the device.

Workaround: Undeploy the user defined templates prior to edit operations and re-deploy the user defined templates post edit.

Bug Tracking Number: CXU-55399

- When you enable Local Internet Breakout (LBO) on the WAN by using site edit workflow, the underlay traffic might drop.

Workaround: Deploy new firewall policy post WAN edit operation.

Bug Tracking Number: CXU-53095

## General

- In some cases, bootstrap job is not triggered if SRX ZTP is executed over LTE WAN link with factory default configuration. On SRX345 devices running CSO, ZTP fails with factory-default configuration if the internet connectivity is through the LTE interface.

Workaround: Run the **delete chassis auto-image-upgrade** command from the factory-default configuration and commit.

Bug Tracking Number: PR 1569595

- On NFX150 Series devices, Class of Service (CoS) does not work for PPP interface.

Workaround: There is no known workaround.

Bug Tracking Number: PR 1581489

- Even after you change the Site name by using **site-edit** option, some of the job logs might still refer to the old site-name. However, this does not affect the service.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-54355

- You should not select OPCO name in SRX-HUB-BREAKOUT template and deploy. The template deployment fails in such cases.

Workaround: You should remove the OPCO name selected in in SRX-HUB-BREAKOUT template and redeploy the template.

Bug Tracking Number: CXU-54312

- 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

- 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

- Ubuntu service chaining instance fails on NFX150.

Workaround: There is no known workaround.

Bug Tracking Number: CXU-52512

## Resolved Issues

The following issues are resolved in Juniper Networks CSO Release 6.1.0:

- Fortinet and Ubuntu service chaining instance fails on NFX250.

Bug Tracking Number: CXU-52817

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

Bug Tracking Number: CXU-52896

- When you upgrade an image from 15.1X49-D173.1 to 19.3r2.s3.3 Release, it was observed that the upgrade of Gateway Router (GWR) without staging takes about 1 hour and 30 minutes, which is very high when compared to the manual upgrade.

Bug Tracking Number: CXU-48845

- After you reboot the server, the docker process in the CAN node stops working.

Bug Tracking Number: CXU-48126

- After you reboot the server, all MS nodes change to **Pending** state and return to 1/1 **Running** state when the node is ready. However, the `secmgt-sm` and `monitoring` pods are seen in 0/1 **Running** state occasionally.

Bug Tracking Number: CXU-48125

- After you reboot the server, the docker process is not started automatically and is in **Loaded** state instead of **Running** state. Hence, if you run the `kubecttl get nodes` command, those nodes are in **NOT READY** state.

Bug Tracking Number: CXU-48027

- After you reboot the server, Rocks engine database corruption occurs.

Bug Tracking Number: CXU-47812

- After you reboot the server, a few of pods in kube-system such as etcd and kube-api are seen in **CrashLoopBackOff** state.

Bug Tracking Number: CXU-46754

- On a chassis cluster, when you reboot one of the servers, workflows such as configure site or delete site fails with an error: **"vhost '/' is down or inaccessible"**.

Bug Tracking Number: CXU-46490

- During a server reboot, the calico pod might remain in 0/1 Init:0/3 or **CrashLoopBackOff** state if the IP\_AUTODETECTION\_METHOD environment variable is not configured.

Bug Tracking Number: CXU-44871

- Active-Active mode is not supported with cloud breakout for GRE tunnels.

Bug Tracking Number: CXU-43757

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

Bug Tracking Number: CXU-43085

- On CSO Release 5.1.1 on-premise chassis cluster, the CSO installation fails due to CAN installation failure.

Bug Tracking Number: CXU-42965

- On NFX250 devices, Fortinet service chaining instantiation fails.

Bug Tracking Number: CXU-42188

- EX4600 and EX4650 switches running Junos OS Release 18.4R2 do not support ZTP,

Bug Tracking Number: CXU-41608

- When you add a second switch under the Site, the Site state changes from PROVISIONED to CONFIGURED.

Bug Tracking Number: CXU-40647

- Zero touch provisioning of an EX Series switch fails if you add an EX Series switch behind an enterprise hub.

Bug Tracking Number: CXU-38994

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

Bug Tracking Number: CXU-37846

- 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.

Bug Tracking Number: CXU-51919

- 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

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

Bug Tracking Number: CXU-45171

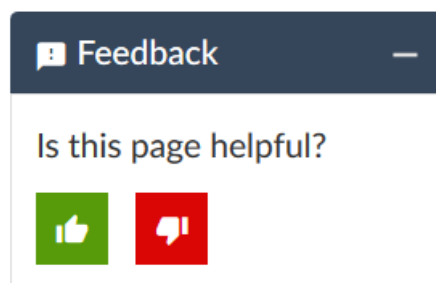
- Installation of licenses on SRX1500 and SRX4200 dual CPE clusters by using CSO is failing.

Bug Tracking Number: CXU-40522

## 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

June 28, 2021—Revision 1, CSO Release 6.1.0

Copyright © 2021 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.