JUNIPER NETWORKS | Engineering Simplicity

Contrail Service Orchestration Administration Portal User Guide

Published
2022-02-21

Release
6.1.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the 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.

Contrail Service Orchestration Administration Portal User Guide
6.1.0
Copyright © 2022 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation | xviii

Documentation and Release Notes | **xviii**

Documentation Conventions | **xviii**

Documentation Feedback | **xxi**

Requesting Technical Support | **xxi**

> Self-Help Online Tools and Resources | **xxii**
>
> Creating a Service Request with JTAC | **xxii**

1 **Introduction**

About the Administration Portal User Guide | 25

Administration Portal Overview | 26

Administration Portal Tasks for SP Administrators And OpCo Administrators | 31

Accessing Administration Portal | 33

Personalize the Administration Portal | 35

Switching the Tenant Scope | 36

About the Administration Portal Dashboard | 37

> Tasks You Can Perform | **37**
>
> Field Descriptions | **38**

Changing the Administration Portal Password | 39

Resetting Your Password | 40

Configuring Two-Factor Authentication | 41

Resend Activation Link in Administration Portal | 43

Changing the Password on First Login | 44

Resetting the Password for OpCo and Tenant Users | 45

Setting Password Duration | 46

Extending the User Login Session | 47

About the Display Preferences | 47

Tasks You Can Perform | 48

Field Descriptions | 48

Add a Theme in Administration Portal | 49

Apply or Modify a Theme | 53

Upload a Custom Font | 54

2 Managing E-Mail

Configuring SMTP Settings | 56

Customizing E-mail Templates | 57

3 Managing Authentication

Authentication Methods Overview | 61

About the Authentication Page | 61

Tasks You Can Perform | 62

Field Descriptions | 62

Editing the Authentication Method | 63

Configuring a Single Sign-On Server | 66

Edit and Delete SSO Servers | 69

Edit SSO Server Configuration | 69

Delete SSO Server Configurations | 70

4 Managing Tenants

Tenant Overview | 73

Full Mesh Topology Overview | 73

Local Breakout in Full Mesh Topology | 75

CPE Devices Behind NAT in Full Mesh Topology | 75

Understanding Specific Route-based Routing Within the SD-WAN Overlay | 76

About the Tenants Page | 77

Tasks You Can Perform | **77**

Field Descriptions | **78**

Adding a Single Tenant | 79

Edit Tenant Parameters | 89

Importing Data for Multiple Tenants | 91

Creating a Tenant Data File | **92**

Importing Tenant Data | **95**

Allocating Network Services to a Tenant | 96

Viewing the Create History of Imported Tenant Data | 97

Delete a Tenant | 99

Viewing the History of Deleted Tenant Data | 100

Dynamic Mesh Tunnels Overview | 102

Configuring Dynamic Mesh Tunnel Thresholds for all Tenants | 104

Updating the Terms of Use | 105

5 **Managing Operating Companies**

Operating Companies Overview | 108

OpCo Hierarchy Management | **108**

OpCo Authentication and Authorization | **109**

Access Privileges for Global SP, OpCo, and Tenant Users | **110**

Benefits of Operating Companies | **115**

About the Operating Companies Page | 115

Tasks You Can Perform | **115**

Field Descriptions | **115**

Creating Operating Companies | 116

Editing and Deleting Operating Companies | 119

Editing Operating Companies | **119**

Deleting Operating Companies | **120**

6

Managing Resources

About the POPs Page | 124

Tasks You Can Perform | **124**

Field Descriptions | **125**

Creating a Single POP | 125

Adding Information About the POP | **126**

Importing Data for Multiple POPs | 127

Customizing a POP Data File | **128**

Uploading a POP Data File | **130**

Viewing the History of POP Data Imports | 131

Viewing the History of POP Data Deletions | 133

View the History of Device Data Deletions | 135

Manually Importing Provider Hub Sites | 137

About the Tenant Devices Page | 138

Tasks You Can Perform | **138**

Field Descriptions | **139**

About the Provider Hub Devices Page | 140

Tasks You Can Perform | **141**

Field Descriptions | **142**

Add a Provider Hub Device | 144

Edit Provider Hub Site Parameters | 153

Manage a Provider Hub Device | 156

Upgrade a Provider Hub Device | 158

Delete a Provider Hub Site | 159

Perform Return Material Authorization (RMA) for a Provider Hub Device | 160

Grant Return Material Authorization (RMA) for a Provider Hub Device | 162

Generate Device RSI for Provider Hub Devices | 164

Managing a Tenant Device | 165

Device Redundancy Support Overview | 167

- Prerequisites for using SRX Series Devices for Device Redundancy | **167**
- Supported Connection Plans | **167**
- Create and Configure an SD-WAN Site | **168**
- Dual CPE Devices Logical Topology for NFX Network Services Platform | **168**
- Dual CPE Devices Logical Topology for SRX Series Gateway Devices | **169**

Viewing the History of Tenant Device Activation Logs | 170

Secure OAM Network Overview | 172

- Topology of a Secure OAM Network | **172**
- Workflow for Establishing a Secure OAM Network | **173**
- Benefits of Secure OAM Network | **174**

Secure OAM Network Redundancy Overview | 174

- Logical Topology | **175**
- BGP Configuration | **176**
- Adding and configuring provider hub devices | **176**
- Adding and configuring a branch spoke site | **177**
- Failure Detection and Recovery | **177**
- Benefits of Secure OAM Network Redundancy | **177**

Rebooting Tenant Devices and Provider Hub Devices | 178

- Rebooting a Tenant Device | **178**
- Rebooting a Provider Hub Device | **179**

Identifying Connectivity Issues by Using Ping | 180

Identifying Connectivity Issues by Using Traceroute | 184

Remotely Accessing a Device CLI | 186

Device Template Overview | 188

- Platform | **189**
- SD-WAN CPE | **189**
- Secure Internet CPE | **190**
- Managed Internet CPE | **191**

Multi-Service Shared Bearer Overview | 192

Benefits of Shared Bearer | **194**

About the Device Template Page | 194

Tasks You Can Perform | **195**

Field Descriptions | **195**

Supported Device Templates | **196**

Cloning a Device Template | 199

Importing a Device Template | 200

Creating a Device Template File | **201**

Importing a Device Template File | **201**

Configuring Template Settings in a Device Template | 202

Updating Stage-2 Configuration Template in a Device Template | 224

Configuring Stage-2 Initial Configuration in a Device Template | 229

Modifying a Device Template Description | 232

Deleting a Device Template | 232

Configuration Templates Overview | 233

Benefits | **234**

Configuration Templates Workflow | 234

About the Configuration Templates Page | 236

Tasks You Can Perform | **236**

Field Descriptions | **237**

Predefined Configuration Templates | 239

Edit, Clone, and Delete Configuration Templates | 243

Edit a Configuration Template | **243**

Clone a Configuration Template | **244**

Delete a Configuration Template | **245**

Deploy Configuration Templates to Devices | 246

- Deploy from the Configuration Templates Page | **246**
- Deploy from the Tenant Devices Page | **250**

Undeploy a Configuration Template from a Device | 251

Dissociate a Configuration Template from a Device | 253

Preview and Render Configuration Templates | 254

Import Configuration Templates | 255

Export a Configuration Template | 257

Assign Configuration Templates to Device Templates | 258

Add Configuration Templates | 261

Jinja Syntax and Examples for Configuration Templates | 271

- Jinja Syntax and CSO Keywords | **272**
- Example 1: Convert a Single Junos OS Command to Jinja Syntax | **274**
- Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax | **275**
- Example 3: Use Conditional Logic | **277**
- Example 4: Use Variable Substitution | **279**
- Example 5: Use Filters, Concatenation, and Set Variables | **280**
- Example 6: Test a Value | **281**

View the Configuration Deployed on Devices | 283

APN Overview | 285

- Benefits of APN Configuration | **285**

Configuring APN Settings on CPE Devices | 286

- Configuring APN Settings with SIM Change on CPE Devices | **286**
- Configuring APN Settings without SIM Change on CPE Devices | **288**

Device Images Overview | 289

About the Device Images Page | 290

- Tasks You Can Perform | **290**
- Field Descriptions | **290**

Staging an Image | 292

Deploying Device Images to Devices | 294

Uploading a Device Image | 296

Deleting Device Images | 298

Network Services Overview | 299

About the Network Services Page | 300

Tasks You Can Perform | 300

Field Descriptions | 300

About the Service Overview Page | 302

Tasks You Can Perform | 302

Field Descriptions | 302

About the Service Instances Page | 304

Tasks You Can Perform | 304

Field Descriptions | 304

Allocating a Service to Tenants | 305

Removing a Service from Tenants | 306

7 Managing Signatures

Signature Database Overview | 309

About the Signature Database Page | 309

Tasks You Can Perform | 310

Field Descriptions | 310

Downloading a Signature Database | 311

Download Locations for Signature Database | 313

Application Signatures Overview | 314

About the Application Signatures Page | 315

Tasks You Can Perform | 315

Field Descriptions | 316

Understanding Custom Application Signatures | 317

Adding Application Signatures | 318

Editing, Cloning, and Deleting Application Signatures | 324

- Editing Application Signatures | **324**
- Cloning Application Signatures | **325**
- Deleting Application Signatures | **325**

Adding Application Signature Groups | 326

Editing, Cloning, and Deleting Application Signature Groups | 327

- Editing Application Signature Groups | **327**
- Cloning Application Signature Groups | **328**
- Deleting Application Signature Groups | **328**

8 **Managing Profiles**

Application Quality of Experience Overview | 332

- Benefits of Application Quality of Experience | **333**

Configure and Monitor Application Quality of Experience | 334

About the Application Traffic Type Profiles Page | 335

- Tasks You Can Perform | **336**
- Field Descriptions | **336**

Predefined Application Traffic Type Profiles | 338

Add Traffic Type Profiles | 340

Edit and Delete Application Traffic Type Profiles | 346

- Edit Application Traffic Type Profiles | **347**
- Delete Application Traffic Type Profiles | **347**

SLA Profiles and SD-WAN Policies Overview | 348

- Traffic-Based Steering Profiles | **349**
- SD-WAN Policies | **352**

About the SLA-Based Steering Profiles Page | 354

Tasks You Can Perform | **354**

Field Descriptions | **354**

Adding SLA-Based Steering Profiles | 357

Editing and Deleting SLA-Based Steering Profiles | 364

Editing an SLA-Based Steering Profile | **365**

Deleting SLA-Based Steering Profiles | **366**

About the Path-Based Steering Profiles Page | 366

Tasks You Can Perform | **367**

Field Descriptions | **367**

Adding Path-Based Steering Profiles | 369

Editing and Deleting Path-Based Steering Profiles | 371

Editing a Path-Based Steering Profile | **372**

Deleting a Path-Based Steering Profile | **373**

About the Breakout Profiles Page | 373

Tasks You Can Perform | **374**

Breakout Profiles Field Descriptions | **374**

Adding Breakout Profiles | 376

Editing and Deleting Breakout Profiles | 378

Editing Breakout Profiles | **379**

Deleting Breakout Profiles | **379**

9 Managing Licenses

About the Device License Files Page | 382

Tasks You Can Perform | 382

Field Descriptions | 382

Uploading a Device License File | 383

Editing and Deleting Device Licenses | 384

Editing a Device License Entry | 385

Deleting a Device License | 385

Pushing a License to Devices | 386

About the CSO Licenses Page | 387

Tasks You Can Perform | 387

Field Descriptions | 388

Add a CSO License | 389

Edit and Delete CSO Licenses | 392

Edit a CSO License | 392

Delete a CSO License | 393

Assign CSO Licenses, and Update or Unassign CSO License Assignments | 394

Assign CSO Licenses to Tenants | 394

Update or Unassign CSO License Assignments | 396

10 Managing Users and Roles

Role-Based Access Control Overview | 399

About the Users Page in Administration Portal | 400

- Tasks You Can Perform | 401
- Field Descriptions | 401

Add Service Provider and OpCo Users | 402

Edit and Delete Service Provider Users and OpCo Users | 406

- Edit Service Provider and OpCo Users | 406
- Delete Service Provider and OpCo Users | 407

Resetting the Password for Service Provider, OpCo, and Tenant Users | 407

Roles Overview | 408

- Types of Roles | 409
- Role Scopes | 409
- Access Privileges | 410
- Relationship Between Users, Roles, and Access Privileges | 411
- Benefits of Roles in CSO | 411

About the Roles Page | 412

- Tasks You Can Perform | 412
- Field Descriptions | 412

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users | 413

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users | 415

- Edit Roles | 415
- Clone Roles | 416
- Delete Roles | 417

Access Privileges for Role Scopes (Operating Company and Tenant) | 417

11 Managing Jobs

About the Jobs Page | 426

Tasks You Can Perform | 426

Field Descriptions | 426

Field Descriptions | 427

Viewing Job Details | 428

Editing and Deleting Scheduled Jobs | 429

Editing Scheduled Jobs | 429

Deleting Scheduled Jobs | 430

Retrying a Failed Job on Devices | 431

12 Managing Audit Logs

Audit Logs Overview | 433

About the Audit Logs Page | 433

Tasks You Can Perform | 434

Viewing the Details of an Audit Log | 435

Exporting Audit Logs | 437

Purging Audit Logs (After Archiving or Without Archiving) | 439

13 Monitoring

About the Monitor Overview Page | 445

Tasks You Can Perform | 445

Field Descriptions | 445

Alerts Overview | 446

About the Generated Alerts Page | 447

Tasks You Can Perform | 447

Field Descriptions | 448

About the Alert Definitions/Notifications Page | 449

Tasks You Can Perform | 449

Managing Security Alerts Definitions | 449

Tasks You Can Perform | **450**

Field Descriptions | **450**

Creating Security Alert Definitions | 451

Editing, Cloning, and Deleting Security Alert Definitions | 452

Editing Security Alert Definitions | **453**

Cloning Security Alert Definitions | **453**

Deleting Security Alert Definitions | **454**

About the Alarms Page | 454

Tasks You Can Perform | **455**

Field Descriptions | **455**

Enable E-mail Notifications for SD-WAN Alarms | 456

Rogue Device Detection | 458

Multitenancy | 459

About the SLA Performance of All Tenants Page | 460

Tasks You Can Perform | **460**

Field Descriptions | **460**

About the SLA Performance of a Single Tenant Page | 463

Tasks You Can Perform | **463**

Field Descriptions | **464**

Application and Link Level SLA Performance | **465**

Monitoring Application-Level SLA Performance for Secure SD-WAN-Advanced | 467

Viewing SLA Performance of Tenants | **468**

Viewing SLA Performance of Sites | **468**

Viewing the SLA Performance of a Site | 469

SLA Not Met by SLA Profiles | **470**

Applications SLA Performance by Throughput | **471**

SLA Performance for ALL | **473**

Viewing the SLA Performance of an Application or Application Group | 474

Understanding SLA Performance Score for Applications, Links, Sites, and Tenants | 476

Application Score | **476**

Site Score | **477**

Tenant Score | **477**

Link Score | **477**

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | **xviii**
- Documentation Conventions | **xviii**
- Documentation Feedback | **xxi**
- Requesting Technical Support | **xxi**

Use this guide to understand the features and tasks that you can configure and perform from the Cloud-based Contrail Service Orchestration (CSO) Administration Portal UI . This guide provides feature overviews and procedures that help you understand the features and perform CSO configuration tasks.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page xix defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page xix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

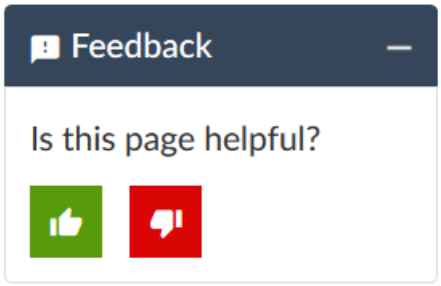
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use 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 Juniper Care or Partner Support Services 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 https://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/.

1

CHAPTER

Introduction

About the Administration Portal User Guide | **25**

Administration Portal Overview | **26**

Administration Portal Tasks for SP Administrators And OpCo Administrators | **31**

Accessing Administration Portal | **33**

Personalize the Administration Portal | **35**

Switching the Tenant Scope | **36**

About the Administration Portal Dashboard | **37**

Changing the Administration Portal Password | **39**

Resetting Your Password | **40**

Configuring Two-Factor Authentication | **41**

Resend Activation Link in Administration Portal | **43**

Changing the Password on First Login | **44**

Resetting the Password for OpCo and Tenant Users | **45**

Setting Password Duration | **46**

Extending the User Login Session | **47**

About the Display Preferences | **47**

Add a Theme in Administration Portal | **49**

Apply or Modify a Theme | **53**

Upload a Custom Font | **54**

About the Administration Portal User Guide

This guide provides an understanding of how to use the Contrail Service Orchestration (CSO) Administration Portal to implement your CSO use cases. This guide is appropriate for network administrators and operators who need to know how to use Administration Portal.

Refer to Table 3 on page 25 for additional CSO documentation resources.

Table 3: Additional CSO Documentation Resources

Title	Available At
What is SD-WAN?	https://www.juniper.net/us/en/products-services/what-is/sd-wan/
What is Network Functions Virtualization (NFV)?	https://www.juniper.net/us/en/products-services/what-is/network-functions-virtualization/
Learn About NFV	https://www.juniper.net/documentation/en_US/learn-about/LearnAbout_NFV.pdf
Customer Portal User Guide	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration (User Guides section)
Designer Tools User Guide	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration (User Guides section)
Deployment Guide	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration (Getting Started section)
Design and Architecture Guide	https://www.juniper.net/documentation/en_US/release-independent/solutions/information-products/pathway-pages/sg-007-sd-wan-sd-lan-design-arch-guide.html
Other Resources	https://www.juniper.net/documentation/product/en_US/contrail-service-orchestration

RELATED DOCUMENTATION

Administration Portal Overview | 26

Administration Portal Overview

The Administration Portal in Contrail Service Orchestration (CSO) provides a Web-based UI that service providers (SPs) and operating companies (OpCos) can use to manage physical and virtual resources, add and manage tenants, monitor system performance, perform administrative tasks (such as manage users and roles), and so on.

Administration Portal supports role-based access control (RBAC), which means that the roles assigned to users determine their access privileges and the actions that they can perform. The following predefined roles are available in Administration Portal:

- SP Admin (SP Administrator)
- SP Operator
- OpCo Admin (OpCo Administrator)
- OpCo Operator

Administrator users have read access and write access to the Administration Portal UI and API capabilities, whereas operator users only have read access. Administrators can also create more users with specific roles and access privileges.

> **NOTE:** In the cloud-hosted version of CSO (managed by Juniper Networks), the SP Admin and SP Operator roles are available only for Juniper Networks.

Administration Portal supports both local authentication and Security Assertion Markup Language (SAML)-based authentication for single sign-on (SSO).

When you log in to Administration Portal, the main menu (left sidebar) that is displayed and the actions that you can perform depend on your access privileges. Table 4 on page 27 displays the main menu available in the Administration Portal and a brief description of each menu item, and a link to the relevant topic in the *Contrail Service Orchestration Administration Portal User Guide*.

Table 5 on page 29 lists the icons on the top right corner of the Administration Portal and a brief description of each icon.

Table 4: Administration Portal Main Menu

Main Menu	Description
Favorites	View the list of pages that you have marked as favorite. You can mark pages that you frequently visit to Favorites. To mark a page as favorites, click the star icon on the right corner of each page.
Dashboard	Access a user-configurable dashboard that you can customize with available widgets (also known as dashlets). For more information, see "About the Administration Portal Dashboard" on page 37.
Monitor	Monitor or view the following: • POPs: See "About the Monitor Overview Page" on page 445. • Alerts and alarms: See "About the Generated Alerts Page" on page 447 and "About the Alarms Page" on page 454. • Service-level agreement (SLA) performance (only for SD-WAN tenants): See "About the SLA Performance of All Tenants Page" on page 460. • Jobs (ongoing or completed): See "About the Jobs Page" on page 426.
Resources	Manage the following resources: • POPs: See "About the POPs Page" on page 124. • Sites: See *About the Sites Page*. • Tenant and provider hub device: See "About the Tenant Devices Page" on page 138 and "About the Provider Hub Devices Page" on page 140. • Device and virtualized network function (VNF) images, and packages: See "About the Device Images Page" on page 290. • Device templates: See "About the Device Template Page" on page 194. • Configuration templates: See "About the Configuration Templates Page" on page 236.

Table 4: Administration Portal Main Menu *(continued)*

Main Menu	Description
Configuration	Configure or manage the following: • SLA-based and path-based steering profiles: See "About the SLA-Based Steering Profiles Page" on page 354and "About the Path-Based Steering Profiles Page" on page 366 • Application traffic type profiles: See "About the Application Traffic Type Profiles Page" on page 335. • SD-WAN breakout profiles • Shared objects (for example, application signatures): See "About the Application Signatures Page" on page 315. • Network services: See "About the Network Services Page" on page 300. **NOTE:** You use the Network Designer tool (part of the Designer Tools) to create and publish network services.
Tenants	Manage tenants and OpCos: See "About the Tenants Page" on page 77 and "About the Operating Companies Page" on page 115.

Table 4: Administration Portal Main Menu *(continued)*

Main Menu	Description
Administration	Perform various administrative tasks including the following: • Set up authentication: See "About the Authentication Page" on page 61. • Manage users and roles: See "About the Users Page in Administration Portal" on page 400 and "About the Roles Page" on page 412. • Monitor audit logs: See "About the Audit Logs Page" on page 433. • Configure dynamic mesh thresholds: See "Configuring Dynamic Mesh Tunnel Thresholds for all Tenants" on page 104. • Manage device and CSO licenses: See "About the Device License Files Page" on page 382 and "About the CSO Licenses Page" on page 387. • Download signature databases: See "About the Signature Database Page" on page 309. • Configure SMTP server: See "Configuring SMTP Settings" on page 56. • Update terms of use: See "Updating the Terms of Use" on page 105. • Customize e-mail templates: See "Customizing E-mail Templates" on page 57. • Personalize the portals: See "About the Display Preferences" on page 47.

Table 5: Administration Portal Icons

Icons	Description
Running Jobs	Displays the list of jobs that are currently in progress. Click **Review All** to view the list of all jobs on the Jobs page. For more information on the Jobs page, see "About the Jobs Page" on page 426.

Table 5: Administration Portal Icons *(continued)*

Icons	Description
Scheduled Jobs	Displays the list of jobs that are scheduled. Click **Review All** to view the list of all scheduled jobs on the Jobs page. For more information on the Jobs page, see "About the Jobs Page" on page 426.
Scope	Displays the scope of a user. If you are an SP administrator or an OpCo administrator, you can change the scope from All Tenants to a specific tenant. For more information on switching the scope, see "Switching the Tenant Scope" on page 36.
Alarms and Alerts	Displays the following two tabs: • Alarms—Displays the list of alarms that are generated by the device along with the timestamp and the severity of the alarm. Click **Review All** to view the details about the generated alarms on the Alarms page. For more information about the Alarms page, see "About the Alarms Page" on page 454. • Alerts—Displays the list of alerts that are generated by the device along with the timestamp and the severity of the alert. Click **Review All** to view the details about the generated alerts on the Alerts page. For more information about the Alerts page, see "About the Generated Alerts Page" on page 447
Feedback	Click this icon to provide feedback about the product or report any issues that you are facing.
User Name	Displays the user name of the user who has currently logged into CSO.
Resize	Click this icon to resize the page to full screen.

Table 5: Administration Portal Icons *(continued)*

Icons	Description
Help Menu (?)	Click this icon to access the following panels and online help documentation: • Getting Started panel • What's New panel • Quick Help panel • Help Center • Release Notes • About Panel

RELATED DOCUMENTATION

Accessing Administration Portal | 33

Administration Portal Tasks for SP Administrators And OpCo Administrators

Before a tenant administrator deploys SD-WAN or next generation firewall (NGFW) in CSO, as an SP administrator (for CSO on-premises) or Operating Company (OpCo) administrator (for CSO SaaS), you must perform the following tasks in the Administration Portal. For more information on roles, see "Role-Based Access Control Overview" on page 399.

If you are an SP Administrator (CSO on-premises version) or the Juniper Networks team (CSO SaaS version):

1. Log in to the CSO Administration Portal. See "Accessing Administration Portal" on page 33.
2. Configure SMTP settings. See "Configuring SMTP Settings" on page 56.
3. Download latest signature database. See "Downloading a Signature Database" on page 311.
4. (Optional) Customize configuration templates. See "Configuration Templates Workflow" on page 234.
5. (Optional) Customize device templates. See "Device Template Overview" on page 188.

6. (Optional) Upload the latest software images to CSO. See "Uploading a Device Image" on page 296.

7. If you are deploying SD-WAN, perform the following tasks:

   a. Add one or more points of presence (POPs). See "About the POPs Page" on page 124.

   b. Add provider hub devices. See "Add a Provider Hub Device" on page 144.

8. (Optional) Add an OpCo. See "Creating Operating Companies" on page 116.

9. Add a tenant with SD-WAN service, NGFW service, or both services. See "Adding a Single Tenant" on page 79.

10. Add CSO licenses. See "Add a CSO License" on page 389.

11. To ensure WAN redundancy in CSO, you can preconfigure aggregated Ethernet links enterprise hub devices for tenants. See *WAN Link Redundancy in Enterprise Hubs Using Aggregated Ethernet* for more information.

If you are an OpCo Administrator:

1. Log in to the CSO Administration Portal. See "Accessing Administration Portal" on page 33.

2. (Optional) Configure SMTP settings. See "Configuring SMTP Settings" on page 56.

   This task is optional because the SMTP settings are configured by the service provider (for CSO on-premises) or Juniper Networks (for CSO SaaS).

3. (Optional) Customize configuration templates. See "Configuration Templates Workflow" on page 234.

4. (Optional) Customize device templates. See "Device Template Overview" on page 188.

5. (Optional) Upload the latest software images to CSO. See "Uploading a Device Image" on page 296.

6. (Optional) If you are deploying SD-WAN and you want to add provider hubs for tenants, do the following:

   a. Add one or more points of presences (POPs). See "About the POPs Page" on page 124.

   b. Add data or data and OAM provider hub devices. See "Add a Provider Hub Device" on page 144.

> **NOTE:** For CSO SaaS, OpCo Administrators should add only provider hub devices with DATA_ONLY capability because Juniper Networks adds the OAM-capable hubs.

7. Add a tenant with SD-WAN service, NGFW service, or both services. See "Adding a Single Tenant" on page 79.

8. Assign CSO licenses to tenants. See "Add a CSO License" on page 389.

9. To ensure WAN redundancy in CSO, you can preconfigure aggregated Ethernet links enterprise hub devices for tenants. See *WAN Link Redundancy in Enterprise Hubs Using Aggregated Ethernet* for more information.

Accessing Administration Portal

To access Administration Portal:

1. If you are an SP administrator, skip to 3.

   If you are an OpCo administrator and logging in to Administration Portal for the first time, do the following. If not, skip to 2.

   > **NOTE:** When your administrator creates a CSO account for you, an e-mail (with the subject line CSO Account Created) is sent. This e-mail contains a URL that allows you to log in to Administration Portal. The URL is active for only 24 hours and is valid only for the first log in.

   a. Click the URL that you have received in the e-mail.

      The Change Password page appears with a message that you must change your password for security purposes.

   b. Change your password following the guidelines provided in Table 6 on page 34.

   c. (Optional) Click the Terms of Use link to view the Terms of Use document.

d. Click the check box to accept CSO terms of use.

e. Click **OK**.

The login password is changed and you are logged out of the system. When you log in you must use the changed password.

2. Login to Administration Portal using the link provided in the account activation e-mail.

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

3. Enter your username and password.

   If you are an SP administrator, login with the username *cspadmin* and the password that you specified for Contrail OpenStack.

   The Welcome page appears listing the key features of the release.

4. (Optional) If you want to hide the Welcome page on your next login, select the **Hide this on next login** check box.

5. Click **Go to Dashboard**. The menu bar on the left-hand side of the every page allows you to access the different tasks easily. The top-level menu items are listed in Table 7 on page 35.

Table 6: Fields on the Change Password Page

Field	Description
New Password	Enter your new password. The password must be between 6 and 21 characters long, and must include at least one lowercase letter, one uppercase letter, one special character, and one number. **NOTE:** The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.
Confirm Password	Reenter the password for confirmation. You can select **Show Password** to view the password.

Table 7: Administration Portal Menu

Menu Name	Description
Dashboard	Configurable dashboard that offers you a customized view of cloud services through its widgets.
Monitor	Monitor alerts and alarms, tenants SLA performance and jobs.
Resources	Manage POPs, tenant devices, provider hub devices, device templates, and device image.
Configuration	Configure network services, SLA-based steering profiles, path-based steering profiles, application traffic profiles and network services.
Tenants	Create tenants and Operating Companies (OpCos).
Administration	Manage users, roles, audit logs, licenses, display preferences, email templates, and the signature database.

RELATED DOCUMENTATION

Administration Portal Overview | 26

Personalize the Administration Portal

You can personalize the navigation mode and the theme in the portal.

To personalize the portal:

1. Click the icon on the lower left corner of the portal. You have an option to personalize the following settings:
   - Navigation Mode
   - Theme
   - Invert colors
2. Select one of the following navigation modes:
   - Side Menu (default option)—Click this option if you want the main menu items to appear on the left pane.

- Horizontal Menu—Click this option if you want the main menu items to appear horizontally on the top bar.

3. Select one of the following themes:
   - Default—Click this option if you prefer the background color of the portal to be blue.
   - Grey—Click this option if you prefer the background color of the portal to be grey.
4. Enable the toggle button if you prefer to invert the colors.

The changes are immediately applied to the portal.

RELATED DOCUMENTATION

Administration Portal Overview | 26

Switching the Tenant Scope

Administration Portal users can change the tenant scope from all tenants to a specific tenant by using the tenant switcher displayed on the banner.

When you switch scope from all tenants to a specific tenant, the menu and pages displayed are almost the same as those displayed for Customer Portal users, with some additional actions visible to the Administration Portal users. When you switch back to the **All Tenants** scope, the menu and pages for the Administration Portal are displayed.

To switch from one scope to another:

- From the top right corner of the page, select the **All Tenants** scope to access Administration Portal or select a specific tenant (for example, aaa) to access Customer Portal. The menu and pages for Administration Portal or Customer Portal are displayed based on the scope selected from the drop-down list.

RELATED DOCUMENTATION

Role-Based Access Control Overview | 399

About the Administration Portal Dashboard

To access this page, click **Administration Portal > Dashboard**.

The user-configurable dashboard offers you a customized view of network services through its widgets.

You can drag these widgets from the carousel at the top of your dashboard to your workspace, where you can add, remove, and rearrange them to meet your needs. For example, you can configure a widget to display a graph with the top five tenants receiving alerts, the status of alerts, and the name of tenant sites.

The dashboard automatically adjusts the placement of the widgets to dynamically fit on your browser window without changing their order. You can manually reorder the widgets using the drag and drop option. In addition, you can press and hold the top portion of the widget to move it to a new location.

Tasks You Can Perform

You can perform the following tasks from this page:

- Customize the dashboard by adding, removing, and rearranging the widgets.
- Update the dashboard or an individual widget by clicking the refresh icon.
- Show or hide widget thumbnails in the carousel by selecting the category of widgets that you want to view from the list at the top left of the carousel; the default is **All Widgets**.
- Add a widget to the dashboard by dragging the widget from the palette or thumbnail container into the dashboard.
- Delete a widget from the dashboard page by clicking the delete icon (**X**) in the title bar of the widget and confirming the delete operation.
- Add a dashboard tab by clicking the **+** icon, (optionally) entering a name, and pressing Enter.

  You can then add widgets to the dashboard as needed.
- Rename a dashboard by double-clicking on the title bar of the dashboard, entering a name, and pressing Enter.
- Delete a dashboard by clicking the delete icon (**X** icon) in the title bar of the dashboard and confirming the delete operation.
- Search for a widget by clicking the search icon (magnifying glass) at the top left of the carousel, entering search text, and pressing Enter.

Field Descriptions

You can quickly view important data using the widgets in your dashboard.

Table 8 on page 38 describes the dashboard widgets.

Table 8: Widgets on the Dashboard

Widget	Description
Device Count By Platform	Displays the number of devices based on the device type (SRX Series devices, NFX Series devices, and vSRX).
Device Count By OS	Displays the number of the devices based on Junos OS releases.
Device Count By Status	Displays the total number of devices and its status (Up or Down).
Tenant Sites: Total Alarms	Displays the total number of alarms grouped by severity level. Click each alarms name to view the total number of tenant sites receiving alarms that are critical, major, or minor.
Top 5 POPs with Alerts	Displays the top five POPs receiving alerts. • **POP**—Name of the POP. • **Tenant**—Number of tenants in the POP. • **Location**—Location of the POP. • **Status**—Type of alerts received that are critical, major or minor.
Top 5 Sites with Alarms	Displays the top five tenant sites receiving alerts. • **Name**—Name of the tenant site. • **Location**—Location of the tenant site. • **Status**—Type of alarms received that are critical, major, or minor.
Top 5 Tenants with Alarms	Displays the top five tenants receiving alarms. • **Name**—Name of the tenant. • **Sites**—Number of sites in the tenant location. • **Status**—Type of alarms received that are critical, major, or minor.

RELATED DOCUMENTATION

Administration Portal Overview | 26

Changing the Administration Portal Password

To change the Administration Portal password:

1. Click the administrative username that is located at the right side of the Administration Portal banner.

   The drop-down list appears.

2. Click **My Profile**. Alternatively, you can access the My Profile page from **Administration > My Profile**.

   The My Profile page appears.

   > **NOTE:** If you change the password for Administration Portal, the new password is saved in Contrail and applies to other GUIs, such as Network Service Designer.

3. Click **Change Password**.

4. Enter the current password.

5. In the New Password text box, enter your new password.

   The login password that you set must conform to a particular set of requirements such as minimum length of 6 characters, a maximum length of 21 characters, and that includes at least one lowercase letter, one uppercase letter, an alpha-numeric character, and a numeric character.

6. In the Confirm Password text box, enter your new password again to confirm it.

7. Click **Save**.

   You are logged out of the system. To log in to Administration Portal again, you must use your new password. Other sessions logged in with the same username are unaffected until the next login.

RELATED DOCUMENTATION

Administration Portal Overview | 26

Accessing Administration Portal | 33

Resetting Your Password

If you have forgotten your password, you can reset the password from the Contrail Service Orchestration (CSO) login page.

> **NOTE:** If you have entered an incorrect password, your account will be locked after five consecutive unsuccessful login attempts.

To reset your password:

1. On the login page, enter the username, and then press **Enter**.

   The Forgot Password link appears on the login page.

2. Click the **Forgot Password** link.

   An e-mail (with the subject Forgot CSO Account Password) is sent to your e-mail address. This e-mail contains a URL (active for 24 hours) to reset your password.

3. Click the **Reset your password** link in the e-mail.

   The Set Password page appears.

4. Change your password following the guidelines provided in Table 9 on page 41.

   > **NOTE:** Fields marked with * are mandatory.

5. Click **OK** to reset the password.

   A confirmation message appears indicating the status of the reset password operation.

If the password reset operation is successful, you can use the new password for subsequent logins to CSO.

Table 9: Fields on the Set Password Page

Field	Description
Password	Enter your new password. The password must be between 6 and 21 characters long, and must include at least one lowercase letter, one uppercase letter, one special character, and one number. **NOTE:** The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.
Confirm Password	Reenter the password for confirmation. You can select **Show Password** to view the password.
Terms of Use	Select the check box to agree to the terms of use document.

RELATED DOCUMENTATION

- Accessing Administration Portal | 33
- Changing the Administration Portal Password | 39
- Changing the Password on First Login | 44
- Setting Password Duration | 46

Configuring Two-Factor Authentication

Two-factor authentication adds an additional authentication level for enhanced login security. CSO uses username and password as the first level of user verification. Starting from Release 6.1.0, CSO supports configuring an optional second level of verification. The second level of verification mandates a user to authenticate through a verification code either sent through an e-mail (default option) or generated using an authentication server.

By default, two-factor authentication is disabled for all users. SP and OpCo administrators can enable or disable two-factor authentication in the Authentication page (**Administration > Authentication**), whereas tenant administrators can perform the same in the Tenant Settings page (**Administration > Tenant Settings**).

- If an administrator enables two-factor authentication at the global, OpCo, or tenant-level, then all existing and new users under that level are automatically configured for two-factor authentication. For example,

if an OpCo administrator enables two-factor authentication, then all the users under that OpCo are configured for two-factor authentication.

Individual users cannot disable two-factor authentication if it is enabled by the administrator. However, users can change the authentication method. The default authentication mechanism is e-mail OTP.

- If two-factor authentication is disabled at the global, OpCo, or tenant-level, then individual users can choose to enable two-factor authentication. Users can also change the authentication mechanism.

  For example, if two-factor authentication is disabled at the tenant-level, then tenant users are required to enter only the username and password to log into CSO. If individual users under that tenant want to use an additional verification level, then they can choose to enable two-factor authentication in the My Profiles page.

- If the administrator enables two-factor authentication initially and then later disables it, then existing users continue to have two-factor authentication enabled. Existing users can opt to disable two-factor authentication in the My Profile page (**Administration > My Profile**).

  However, two-factor authentication is disabled for new users. New users can enable two-factor authentication based on individual requirements.

Individual users can enable two-factor authentication if it is disabled. Users cannot disable two-factor authentication if it is enabled by the administrator.

> **NOTE:** If single sign-on (SSO) is enabled at the global or OpCo level, administrators cannot enable two-factor authentication for the users at that level.

1. Select **Administration > My Profile**.

   The My Profile page appears.

   > **NOTE:** If SSO is enabled in any of the scopes that the user is part of, then the My Profile page displays only the username as the user credentials are managed by the SSO server.

2. Click the toggle button to enable two-factor authentication.

CSO provides two methods for two-factor authentication—e-mail and TOTP authentication. E-mail is the default method. You can opt to select TOTP authentication.

To enable TOTP authentication:

1. Install a Time-Based One-Time Password (TOTP) authenticator application on your mobile phone. You can use a TOTP authenticator application such as Authy, Duo Mobile, or you can use an authenticator from Microsoft, LastPass, or Google.

2. Scan the QR code provided in the My Profile page using the authenticator application to register your mobile phone with CSO.

3. Enter the verification code generated by the authenticator application and click **Verify**.

   After CSO verifies the code, TOTP authentication is enabled. When you log in to CSO, you are prompted for a verification code that is generated by the authenticator application.

If you change your mobile phone, click **Change Phone** to unregister the existing phone from CSO. To register the new phone with CSO, follow steps 1 through 3.

If you do not want to use the TOTP authentication method, click **Delete**.

Resend Activation Link in Administration Portal

When service provider (SP) or operating company (OpCo) administrators create a new user of any role or type, CSO automatically sends an activation link to their e-mail account. The SP or OpCo administrator can resend activation link to the user's account in the following events:

- The initial activation link expired, or
- The e-mail with the activation link does not get delivered, or
- The user's account must be manually re-enabled.

If you are an SP administrator, you can resend the activation link to users with SP, OpCo, and tenant roles (both administrators and operators). If you are an OpCo administrator, you can resend the activation link to users with OpCo and tenant roles (both administrators and operators).

To resend the activation link:

1. Select **Administration > Users** in Administration Portal.

   The Users page appears, displaying a list of users.

2. Select the username to whose account you want to send the activation link, and then select **More > Resend Activation Link**.

   An alert message appears, asking you to confirm the resend activation link operation.

3. Click **Yes** to confirm the resend activation link operation.

   An e-mail is sent to the user's e-mail address with a URL to reset the password in order to activate their account in CSO. The URL is active for 24 hours.

RELATED DOCUMENTATION

Resetting the Password for OpCo and Tenant Users | 45

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users | 413

Changing the Password on First Login

To enhance the security related to login credentials, you are prompted to change the password when you login to the portal for the first time.

To change the password when you log in for the first time:

1. Log in to the portal with the default login credentials.

   The Change Password page appears with a message that you must change your password for security purposes.

   NOTE: The Change Password page appears only if you are logging in to the portal for the first time.

2. Change your password following the guidelines provided in Table 6 on page 34.

3. Click **Ok**.

   NOTE: It is mandatory to change the login password when you log in to the portal for the first time. If you click **Cancel**, you are redirected to the login page.

The login password is changed and you are logged out of the system. To log in to the portal again, you must use your new password.

Table 10: Fields on the Change Password Page

Field	Description
New Password	Enter your new password. The password must be between 6 and 21 characters long, and must include at least one lowercase letter, one uppercase letter, one special character, and one number. **NOTE:** The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.
Confirm Password	Reenter the password for confirmation. You can select **Show Password** to view the password.

RELATED DOCUMENTATION

- Accessing Administration Portal | 33
- Changing the Administration Portal Password | 39
- Resetting Your Password | 40
- Setting Password Duration | 46

Resetting the Password for OpCo and Tenant Users

Users with the OpCo administrator role (or MSP Administrator role) or a tenant administrator role can reset the password for OpCo user and tenant users respectively. Also, users with the Update capability for Users objects can reset the password for both OpCo and tenant users.

To reset the password:

1. Select **Administration > Users** in Administration Portal.

   The Users page appears, displaying a list of users.

2. Select the username for which you want to reset the password, and then select **More > Reset Password**.

   An alert message appears, asking you to confirm the reset password operation.

3. Click **Yes** to confirm the reset password operation.

An e-mail (with the subject Reset Your CSO Password) is sent to the user's e-mail address. This e-mail contains a URL (active for 24 hours) to reset the password. Users can click the URL link in the e-mail and change the password

Setting Password Duration

To enhance the security related to login credentials, you can specify the duration (in days) after which the password expires and must be changed. You must set the duration while you are adding a tenant.

To set the duration (in days) after which the password expires:

1. Log in to Administration Portal.

2. Select **Tenants** > **All Tenants** > **+**.

   The Add Tenant page appears.

3. In the Tenant Info > Password Policy section >Password Expiration Days, specify the duration (in days) after which the password expires and must be changed. You can specify the duration (in days) from 1 through 365. The default value is 180 days.

4. Complete the remaining steps for adding a tenant. For more information about adding a tenant, see "Adding a Single Tenant" on page 79.

If the tenant user (Tenant Administrator role or Tenant Operator role) has the password expiration days specified, then the tenant user must change the password after the specified duration elapses.

RELATED DOCUMENTATION

Accessing Administration Portal | 33

Changing the Administration Portal Password | 39

Changing the Password on First Login | 44

Resetting Your Password | 40

Extending the User Login Session

In the unified portal, a login session expires in 60 minutes. After 55 minutes, the **Extend Session** page is displayed and, prompting you to enter your password. You must enter your password to extend the session. The **Extend Session** page is displayed when the **Local** authentication method is configured.

If you have logged in to the portal with SSO authentication, the **Extend Session** page is displayed and you can authenticate with the external SSO server. However, the SSO expiration is not under the control of CSO and the following can happen:

- If the external SSO session is expired, you will be authenticated in the **Extend Session** page. After successful authentication, the **Extend Session** page is closed automatically.
- If the external SSO session is not expired, the **Extend Session** page is closed automatically.

To extend the login session:

1. On the **Extend Session** page, enter your password in the **Password** field. If you want to end your session and exit from the portal, click **Cancel** instead and you are redirected to the Login page.

2. Click **OK**.

   The success message **Your Session has been successfully extended** is displayed.

RELATED DOCUMENTATION

Changing the Administration Portal Password | 39

About the Display Preferences

To access this page, select **Administration > Display Preferences** in Administration Portal.

Users with Service Provider (SP) Administrator role can use the Display Preferences page to create multiple themes, set a theme active or inactive, and delete a theme in the Administration Portal. A customized theme enables you to personalize the login page, reports, apply a font style, and set a color palette to the navigation bar and menu. In the Customer Portal, the themes are available in the navigation mode icon on the navigation bar.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a new theme — See "Add a Theme in Administration Portal" on page 49.
- Apply or modify a theme — See "Apply or Modify a Theme" on page 53.
- Upload a custom font — See "Upload a Custom Font" on page 54.
- Set a theme for a report. To set a theme for a report, select a theme and click **Set Report Theme** button.
- Delete a custom theme. Select a particular theme in the Display Preferences page and click on the delete icon.

  If you want to delete a customized theme that is applied on the portal, make sure to select the default theme before deleting the custom theme.

  NOTE: The default theme cannot be deleted.

Field Descriptions

Describes the fields on the Display Preferences page.

Table 11: Display Preferences Page Fields

Field	Description
Name	Name of the default and custom themes.
Color Palette	A swatch of the primary color, primary navigation background color, grid (table) action color, and primary button text color.
Font	Typeface chosen in a theme for the GUI.
Default	Displays a boolean status based on whether a theme is default or custom. For default theme, the status shows 'True' and for custom themes, it shows 'False'.
Active	Displays a boolean status based on whether a theme is set active or not. If the theme is active, the status shows 'True' and if not, the status shows 'False'.

Table 11: Display Preferences Page Fields *(continued)*

Field	Description
Report	Displays a boolean status based on whether a particular theme is set as a report theme. A theme set for reports will not be available as an option to be set as an active theme for the portals.
Update Time	Displays the date (in MM/DD/YYYY format) and time (in AM/PM format) of the latest update to a particular theme.

Add a Theme in Administration Portal

Use the Display Preferences page to personalize the following elements:

- Login page background and logo for the portals.
- Logo and banner on the top-left corner of the portals.
- Typeface for the GUI.
- Logo, typeface, company name, and background colors for reports.
- Primary and Secondary color palettes for the navigation panel, text on active tabs, icons, and buttons on the GUI.

> **NOTE:** This topic is applicable only for users with the SP Administrator role who are assigned the Update Preferences capability.

To add a new theme:

1. Click **Administration > Display Preferences**.

   The Display Preferences page appears.

2. Click the **Plus (+)** icon to create a theme.

   The **Add New Theme** page appears.

3. Complete the configuration according to the guidelines in Table 12 on page 50.

NOTE: Fields marked with an * are mandatory.

4. Click **Save** when your changes to the settings are final.

   A confirmation message appears and the new theme is displayed in the **Display Preferences** page.

   Once you create a new theme, it takes a few minutes for CSO to generate the theme.

Table 12: Fields on the Display Preferences Page

Field	Action
Name	Enter the name of your theme.
Logo	
Portal (top-left corner)	Upload an image for the logo that appears on the top-left corner of the portals: 1. Click **Browse**. The File Upload dialog box appears. 2. Navigate to the file location and select the file. SVG is the supported file format for images and 25x25 pixel is the recommended image size. 3. Click **Open** to upload the image. You are returned to the Add New Theme page.
Banner (top-left corner)	Upload an image for the banner that appears on the top-left corner of the portals: 1. Click **Browse**. The File Upload dialog box appears. 2. Navigate to the file location and select the file. SVG is the supported file format for images and 160x30 pixel is the recommended image size. 3. Click **Open** to upload the image. You are returned to the Add New Theme page.

Table 12: Fields on the Display Preferences Page *(continued)*

Field	Action
Login Page	
Logo	Upload an image for the logo that appears on the top-left corner of the login page. SVG is the supported file format for images and 240x25 pixel is the recommended image size. For information on uploading the image, see "Step-by-Step Procedure" on page 50.
Background	Select a background image or background color for the login page: • If you select **Image**, click **Browse** to upload a background image for the login page. SVG is the supported file format for images and 1440x780 pixel is the recommended image size. For information on uploading the image, ses "Step-by-Step Procedure" on page 50. • If you select **Fill Color (Gradient)**, select two colors (**Color 1** and **Color 2**) from the palette for a gradient effect.
Font	
Typeface	Select a typeface (**Arial**, **Helvetica**, or **Open Sans**), for the CSO GUI, from the list or upload a custom typeface. The default typeface is Helvetica.
Report	
Logo	Click **Browse** to upload a logo that appears in the SD-WAN reports and security reports. PNG is the supported file format and 240x25 as the recommended image size.
Company Name	Enter a company name. This name appears in the SD-WAN and Security reports. **NOTE:** If you enter any company's name other than Juniper Networks, the Juniper branding page is automatically hidden.

Table 12: Fields on the Display Preferences Page *(continued)*

Field	Action
Typeface	Select a typeface (**Arial**, **Helvetica**, or **Antenna**) from the list or upload a custom typeface for the reports. The default typeface is Helvetica.
Background Color	Select colors (**Background Color 1** and **Background Color 2**) from the palette for a gradient effect. This effect is visible in the background of the report.
Color Palette Use the default color palette or create a customized palette.	
Colors	
Primary Color	Select a primary color. Primary color is the color of selected menu in the navigation bar, linked texts (tenant names, site names, etc.), and menus (such as More, Filter) on a page in Administration and Customer Portals.
Primary Navigation Background	Select a background color for the primary navigation panel.
Selected Tabs	Select a color for the active tab in a tab container; the tab name changes to the selected color when it is active. For example, the color of the **Configuration Template** tab in **Resources > Tenant Devices > Device-Name**.
Icons	
Grid (Table) Action	Select a color for the icons on the navigation bar and icons on the corner of the portals such as notification, email, full screen, and help.
Grid (Table) Action Hover	Select a color for an icon on top of a grid; the icon changes to the selected color when you hover over it.
Buttons	
Primary Action Button Text	Select a text color on the primary action button. For example, text color of the **Add OpCo** button in **Tenants > Operating Companies**.

Table 12: Fields on the Display Preferences Page *(continued)*

Field	Action
Primary Action Button	Select a color for the primary action button that appears on pages. For example, color of the **Save** button in **Add New Theme** page.
Secondary Action Button Text	Select a text color on the secondary action button.
Secondary Action Button	Select a color for the secondary action button such as radio buttons in GUI.

Apply or Modify a Theme

To apply a theme to your portal, you must first set it active. This operation adds the theme in the navigation mode icon on the navigation bar.

To activate and apply a custom theme:

1. Click **Administration > Display Preferences** in the navigation bar.

   The Display Preferences page appears.

2. Select a particular theme other than the default option.

3. Click **Set Active**.

   A message displays that the theme activation is successful. In the navigation mode icon, the theme you added is displayed.

4. To apply a custom theme to the portals, click on the custom theme in the navigation mode icon.

To modify a customized theme:

1. Select a particular theme and click on the edit icon.

   The Add New Theme page appears.

2. Click **Save** after making necessary changes.

   When a theme is modified, its status automatically changes from **Active** to **Inactive**. See the previous procedure to reactivate and apply the theme so that, the changes reflect in the portals.

RELATED DOCUMENTATION

Add a Theme in Administration Portal | 49

Upload a Custom Font

Custom typeface or fonts can be used to change the font of the user interface in administration and customer portals.

To upload a custom typeface file:

1. Click **More > Uplaod Font**.

   The Upload Font page appears.

2. Click **Browse** to upload a customized typeface file (zip file).

   The zip file contains four formats of custom font styles (EOT, SVG, WOFF, and WOFF2) and a CSS file. You must add all four font files to the CSS file. The zip filename should be same as the CSS filename.

3. Click **Upload**.

   A confirmation message **The font added** appears and the custom typeface file is saved in CSO.

   (Optional) To view the different formats of files to be uploaded to customize your font, click **Download Sample Font File**.

   The sample font file is downloaded to your local file system.

RELATED DOCUMENTATION

Apply or Modify a Theme | 53

2

CHAPTER

Managing E-Mail

Configuring SMTP Settings | **56**

Customizing E-mail Templates | **57**

Configuring SMTP Settings

Use this page to configure an SMTP e-mail server. The SMTP server is the local server that forwards your e-mail to the destination server. After you log in to the unified Administration or Customer portal for the first time, you must configure the SMTP settings for your deployment.

To configure SMTP settings:

1. Click **Administration > SMTP**.

   The SMTP page appears.

2. Specify the SMTP settings that you want to configure to user for the mail server. See Table 13 on page 56.

3. Click **Save**.

   The status of the save operation is displayed.

Table 13: SMTP Settings

Field	Description
SMTP Server	
Server Address	Enter the hostname for the SMTP server.
TLS	Enable Transport Layer Security (TLS) protocol to ensure that the e-mail messages are transmitted over an encrypted channel.
Port Number	Enter the port number for the SMTP server. Check with your e-mail service provider for the SMTP port number. By default, the port number is set to 587 when TLS is enabled and to 25 when TLS is not enabled. However, you can modify the port number.
SMTP Authentication	
SMTP Authentication	Enable this option if the e-mail server requires authentication before an e-mail can be sent. The **Username** and **Password** fields are displayed when you enable this option. Disable this option if you want to configure an unauthenticated e-mail server. The **From Name** and **From E-Mail Address** fields are displayed when you disable this option.

Table 13: SMTP Settings *(continued)*

Field	Description
User Name	Enter the username that you want to use for authentication.
Password	Enter the password that you want to use for authentication.
Confirm Password	Reenter the password for confirmation.
From Name	Enter your name. This name will appear as **from name** to the e-mail recipient.
From E-Mail Address	Enter your e-mail address in the user@domain format. This e-mail address will appear as the sender's e-mail address to the e-mail recipient.
Test SMTP Settings	
E-mail Address	Enter your e-mail address in the user@domain format.
Send Test E-mail	Enter the e-mail address and click **Send Test E-mail** to test the SMTP server connection. If the settings are correct, you will receive an e-mail, which confirms that the SMTP Server is working.

RELATED DOCUMENTATION

Authentication Methods Overview | 61

About the Authentication Page | 61

Customizing E-mail Templates

Contrail Service Orchestration (CSO) provides default e-mail templates that are used to send e-mails for the following operations:

- When a new user account is created.
- When a user's account is locked.
- When a user has forgotten the password.
- When a password is reset.
- When a new password is generated.

Use this page to customize an e-mail template as per your requirements.

To customize an e-mail template:

1. Select **Administration > Email Templates**.

   The Email Templates page appears.

2. Select an e-mail template and click the edit icon (pencil symbol) to modify the content of the template.

   The Edit Template page appears.

3. Modify the e-mail template for the following:
   - Add new context keywords.

     To insert a context keyword into e-mail template, place double curly braces around the keyword.

     Example:

     ```
     {{ user_name }}
     ```

     NOTE: You must not change the existing context keywords— user_first_name, user_last_name, user, and email.

   - Edit the title of the e-mail.

     The title field will be used in the subject of the e-mail

   - Address the user by their first name or last name in the e-mail.

     Examples:

     - ```
       Hi {{ user_first_name }},
       ```
     - ```
       Hi {{ user_last_name }},
       ```

   - Edit the body of the e-mail.
4. After you modify the template:
   - Click **Save** to save the changes.

     The modified template is used to send e-mail to the user. A message indicating the status of the operation is displayed.

   - Click **Cancel** to discard the changes.

The changes to the e-mail templates are discarded and you are returned to the E-mail Templates page.

- Click **Restore Default Content** to restore the e-mail template to default template.

  The e-mail template is restored to the default version that is generated by CSO.

3

CHAPTER

Managing Authentication

Authentication Methods Overview | **61**

About the Authentication Page | **61**

Editing the Authentication Method | **63**

Configuring a Single Sign-On Server | **66**

Edit and Delete SSO Servers | **69**

Authentication Methods Overview

Contrail Service Orchestration supports single sign-on (SSO) authentication for the unified portal.

You can authenticate and authorize users by using one of the following authentication methods:

- **Local**—User accounts are maintained locally in CSO, and users are authenticated and authorized by CSO.
- **Authentication by using an SSO server**—User accounts are maintained in the OpCo's SSO server, but authorization information is stored in CSO. Users are authenticated by using the credentials stored in the SSO server.
- **Authentication and authorization by using an SSO server**—User accounts and user roles are maintained in the OpCo's SSO server. Users are authenticated by the SSO server and authorized by CSO by using Security Assertion Markup Language (SAML) attributes.

When you log in to the unified Administration and Customer Portal, the login page is displayed. To log in to the unified Administration and Customer Portal, enter the username on the login page. If the username matches the username pattern configured for SSO, then you are redirected to the SSO page. If the username does not match the username pattern, you must enter the password.

For each SSO authentication method, a list of permitted roles must be provided to the SSO server. Only users with permitted roles in the SAML attribute are allowed to log in to CSO. Also, a mapping between the roles defined in CSO and the roles defined in the external SSO server (Identity Provider) must be provided.

RELATED DOCUMENTATION

About the Authentication Page | 61
Configuring a Single Sign-On Server | 66

About the Authentication Page

To access this page, click **Administration > Authentication**.

Use this page to configure the authentication method for OpCo and tenant users. You can also use this page to add, edit, and delete SSO servers, and modify the authentication method.

Tasks You Can Perform

You can perform the following tasks from this page:

- Enable or disable two-factor authentication at the global, OpCo, or tenant-level. See "Configuring Two-Factor Authentication" on page 41.
- Configure an SSO server. See "Configuring a Single Sign-On Server" on page 66.
- Edit and delete an SSO server. See "Edit and Delete SSO Servers" on page 69.

Field Descriptions

Table 14 on page 62 provides guidelines on using the fields on the Authentication page.

Table 14: Fields on the Authentication Page

Field	Description
Two-Factor Authentication	
Two-Factor Authentication	Enable the toggle button to enforce two-factor authentication for all users. By default, two-factor authentication is disabled for all users. Only an SP, OpCo, or tenant administrator can enable or disable two-factor authentication for all their users. • If you enable two-factor authentication, then individual users cannot disable it. • If two-factor authentication is disabled, then individual users can enable it from the Administration > My Profile page. • If you enable two-factor authentication initially and later disable it, existing users continue to have two-factor authentication enabled. Existing users can disable two-factor authentication in the My Profile page (**Administration > My Profile**). However, two-factor authentication is disabled for new users. New users can enable two-factor authentication in the My Profile page (**Administration > My Profile**).
Authentication Method	
Users	View the user's type. Example : SP Users or Tenant Users
Authentication Method	View the type of authentication method. Example: Local Authentication

Table 14: Fields on the Authentication Page *(continued)*

Field	Description
Owner	View the user (Global or OpCo) who configured the authentication method.
SSO Server	View the name of the SSO server.
Username Pattern	View the username pattern. Example: **@aaa-example.com*
Permitted Roles	Displays the permitted role names.
Single Sign-On (SSO) Servers	
SSO Server	View the name of the SSO server.
Description	View the description of SSO server.
Metadata URL	View the URL of the identity provider metadata. Example: https://aaa-example.com/saml/metadata/64000
Usage	View the information about whether the SSO server is used for authenticating SP users or tenant users. Example: SP Users

RELATED DOCUMENTATION

Authentication Methods Overview | 61
Configuring a Single Sign-On Server | 66

Editing the Authentication Method

Users with the SP administrator role can use the Authentication page to modify the authentication method for service provider and tenant users.

To modify the authentication method:

1. Select **Administration > Authentication**.

   The Authentication page appears.

2. Select the user type (SP User or Tenant User) for which you want to change the authentication method, click the edit icon.

   The Authentication Type page appears.

3. Select any one of the following authentication methods that you want to configure for the user.

   - Local Authentication
   - Authentication with SSO Server
   - Authentication and Authorization with SSO Server

   For more information about authentication methods, see "Authentication Methods Overview" on page 61.

4. If you select the **Authentication with SSO Server** or **Authentication and Authorization with SSO Server** method, then you must enter the configuration described in Table 15 on page 64.

   Table 15: Fields on the Authentication Type Page

Field	Description
SSO Server	Select the SSO server name from the list.
SSO Initiated By	Select the SSO initiation method. • **Service Provider (CSO)**—Select this method if SSO authentication is initiated by CSO. For example, when the user tries to use CSO application without authentication, the user is redirected to the SSO Server. After authentication with the SSO Server, the user is directed to CSO. • **Identity Provider (SSO Server)**—Select this method to authenticate users by using the identity provider. When you login to the identity provider, it provides a list of applications that are integrated with the identity provider and you can access any of the applications. For example, if you click on the CSO application, you are directed to CSO and you can access the CSO application.
If you select the **Service Provider (CSO)** method, then the following field is displayed:	

Table 15: Fields on the Authentication Type Page *(continued)*

Field	Description
Username Pattern	Enter a list of username patterns separated by a comma, space, or semicolon. For example, **@aaa-example.com*; *@xyz-example.com. **NOTE:** If the username matches the username pattern, the user is redirected to the SSO server to complete the authentication process. If the username does not match with any of the username patterns, then the local authentication is assumed.
When you select **Identity Provider (SSO Server)** method, the following fields are displayed:	
Direct CSO Login Message	Enter the message to display when a user tries to directly access CSO without being authenticated by the SSO server.
Logout Message	Enter the message to be displayed when the user logs out from CSO.
Tenant Identifier	Select the identifier to correlate the tenant Security Assertion Markup Language (SAML) attribute with the tenant. Whenever the tenant is onboarded into the system, the tenant is uniquely identified by any one of the following identifiers: • **Use Tenant Name**—Select this option to identify the tenants by using the tenant name. • **Use OSS Tenant ID**—Select this option to identify the tenants by using the tenant ID.
Permitted Roles and Mapping	Roles used in the SSO server (external system) are different from the roles used in CSO. Therefore, you must map the roles defined in CSO with the roles defined in the external SSO server (Identity Provider). To map the roles: 1. Click add icon (+). A new row appears under the header in the table. If you want to delete the row, click the delete icon (X). 2. Select the role from the **Role in CSO** column, and then enter one or more matching roles (separated by commas) in the **Mapped External Role** column. 3. Click **OK** to save the changes. If you want to cancel, The user role in CSO is matched with the role in the SSO server. You can also modify the permitted role and delete one or more permitted roles.

> **NOTE:** If you select the **Local Authentication** type, the **SSO Server**, **SSO Initiated By**, and **Username Pattern** fields are not displayed.

5. Click **Save** to save the changes. If you want to discard the changes, click **Cancel** instead.

RELATED DOCUMENTATION

About the Authentication Page | 61

Configuring a Single Sign-On Server | 66

Edit and Delete SSO Servers | 69

Configuring a Single Sign-On Server

Use this page to configure a single sign-on server (SSO) that is used for authenticating users. There are two entities involved during the SSO configuration:

- **SSO Server or Identity Provider**—An external server integrated with CSO.
- **OpCo**—Acts as an service provider and receives the SAML assertion sent by the SSO server in a response to a login request.

Both the identity provider and OpCo trust each other and configuration is required for both the entities. Two use cases are possible:

- **Identity provider is configured first before SSO server is added in CSO**—The identity provider is configured first. Then, at the OpCo level, you can add the SSO server in CSO for tenant users, and enter the server name and metadata URL.
- **IdP is configured after SSO server is added in CSO**—Enter the SSO server name and then click the **Next** button. CSO provides a list of URLs to be configured in the identity provider. After the identity provider is configured with the URLs, you can edit the SSO server name and enter the metadata URL.

> **NOTE:** For both the use cases, the metadata URL is required before you use the SSO server.

To configure an SSO server:

1. Select **Administration > Authentication**.

   The Authentication page appears.

2. Click the plus icon (+) in the Single Sign-On Server section.

   The Add Single Sign-On Server page appears.

3. Complete the configuration according to the guidelines Table 16 on page 67.

4. Click **Save** to save the changes. If you want to discard the changes, click **Cancel** instead.

5. After you configure both the SSO Server and CSO, click the **Test Login** button from the Authentication page.

   The SSO login page appears and shows the SAML attributes.

> **NOTE:** You must specify the metadata URL before you click the **Test Login** button. If you click the **Test Login** button without entering the metadata URL, an error message indicating that the metadata URL must be specified is displayed.

Table 16: Fields on the Single Sign-On Server Page

Field	Description
Basic Info	
SSO Server Name	Specify the name of the SSO server. You can use a string of alphanumeric characters, special characters such as the underscore (_) or the period (.), and spaces. The maximum length is 40 characters.
Description	Enter a meaningful description for the SSO server.
Metadata URL	Enter the URL from where the application metadata needs to be downloaded.
User Identification	Specify how a user is identified from the SAML assertion: • Name ID: The user is identified from the Name ID field that is present in the subject of the SAML assertion. • SAML attribute: The user is identified from the fixed value attribute.
SAML Settings	

Table 16: Fields on the Single Sign-On Server Page *(continued)*

Field	Description
SAML URLs	CSO displays the SAML URL settings. The administrator use this information to configure the IdP.
Single Sign-On URL	Displays the SAML Assertion Consumer Service (ACS) URL for the application. Example: https://*aaa-example.com*/ssol/*sso server name*/SAML2/POST
Audience URI (SP Entity ID)	Displays the service provider entity ID of the application. Example: https://*aaa-example.com*/Shibboleth
Metadata URL	Displays the metadata URL of the application. Example: https://*aaa-example.com*/saml/metadata/64000
Download Metadata	Click this option to download metadata from the application. The administrator can download the CSO metadata and use the metadata to configure the identity provider instead configuring individual identity provider fields at a time.
SAML Attributes	The identity provider needs to provide the SAML attributes if the authentication method is configured as **Authentication and Authorization with SSO Server**. **NOTE:** No SAML attributes are required if the authentication method is configured as **Authentication with SSO Server**.
tenant	This attribute is required when the Tenant User is authenticated. The value of this attribute should match with the tenant name used when the tenant was onboarded.
role	This attribute has four values. See Table 17 on page 68.

Table 17: Attribute Values and Roles

Attribute Value	Role
cloud-admin	SP Admin
cloud-operator	SP Operator
tenant-admin	Tenant Admin
tenant-operator	Tenant Operator

RELATED DOCUMENTATION

About the Authentication Page | 61
Edit and Delete SSO Servers | 69

Edit and Delete SSO Servers

IN THIS SECTION

Edit SSO Server Configuration | 69
Delete SSO Server Configurations | 70

From the **Administration** > **Authentication** page, you can edit the information of an SSO server, and delete one or more SSO servers.

Edit SSO Server Configuration

To edit the SSO server configuration:

1. Select **Administration > Authentication**.

   The Authentication page appears.

2. From the Single Sign-On (SSO) Servers section, select the check box of the SSO server name that you want to modify, and click the edit icon.

   The Edit Single Sign-On page appears. The options available on the Add Single Sign-On Server page are available for editing.

3. Update the configuration as needed.

4. Click **Next** to save the changes. If you want to discard your changes, click **Cancel** instead.

Delete SSO Server Configurations

Use the delete icon (X) at the top right corner of a page to delete one or more SSO servers.

To delete the SSO server configuration:

1. Select **Administration > Authentication**.

   The Authentication page appears.

2. Select the SSO server name that you want to delete and click the delete icon (X).

   The Confirm Delete page appears.

3. Click **Yes** to delete the SSO server or **No** to cancel the deletion.

   If you click **Yes**, then the SSO server is deleted. After an SSO server is deleted, you cannot use that SSO server for authenticate or authorize users.

RELATED DOCUMENTATION

About the Authentication Page | 61

Configuring a Single Sign-On Server | 66

4

CHAPTER

Managing Tenants

Tenant Overview | **73**

Full Mesh Topology Overview | **73**

Understanding Specific Route-based Routing Within the SD-WAN Overlay | **76**

About the Tenants Page | **77**

Adding a Single Tenant | **79**

Edit Tenant Parameters | **89**

Importing Data for Multiple Tenants | **91**

Allocating Network Services to a Tenant | **96**

Viewing the Create History of Imported Tenant Data | **97**

Delete a Tenant | **99**

Viewing the History of Deleted Tenant Data | **100**

Dynamic Mesh Tunnels Overview | **102**

Configuring Dynamic Mesh Tunnel Thresholds for all Tenants | **104**

Updating the Terms of Use | **105**

Tenant Overview

In Contrail Service Orchestration (CSO), a tenant is a logical representation of a customer. Tenants enable the separation and isolation of resources (such as sites) and traffic of different customers from one another.

If you are an SP administrator or an OpCo administrator you can add tenants (customer) in the Administration Portal and assign administrative users that represent the staff in the customer's organization and the geographical locations in the customer's network. You also use Administration Portal to allocate network service profiles to customers.

A tenant represents an enterprise customer who accesses virtualized network functions (VNFs) in a service provider's or an OpCo's cloud through a Layer 3 VPN. Typically an enterprise customer with many branches (sites) subscribe to the offerings provided by the service provider. Sites are provisioned within a tenant. One tenant cannot see the sites or assets of another tenant. The enterprise customer can view, configure, and manage tenant sites through the Customer Portal.

RELATED DOCUMENTATION

- Administration Portal Overview | 26
- About the Tenants Page | 77
- Adding a Single Tenant | 79
- Importing Data for Multiple Tenants | 91

Full Mesh Topology Overview

Contrail Service Orchestration (CSO) supports the full mesh topology on tenants in a software-defined WAN (SD-WAN) implementation. In a full mesh topology, all sites of a tenant are connected to one another. The sites are connected to one another through GRE and GRE_IPsec overlay tunnels. The default overlay tunnel encapsulation is GRE_IPsec.

In the full mesh topology, a WAN interface of one type is connected to a WAN interface of a different type if these WAN interfaces are associated with same mesh tags. A mesh tag is a label that you associate with a WAN link of a site. Mesh tags provide you the flexibility to establish overlay tunnels between WAN links of two different sites

NOTE: With mesh tags, you can connect two WAN links even if the link types (MPLS and Internet) are different.

The following requirements must be satisfied for connections between WAN interfaces:

- IP addresses of Internet WAN interfaces must be reachable on the Internet. Also, IP addresses must be preserved and change in IP addresses is not supported.
- WAN links that are associated with same mesh tags must be reachable on the Internet.

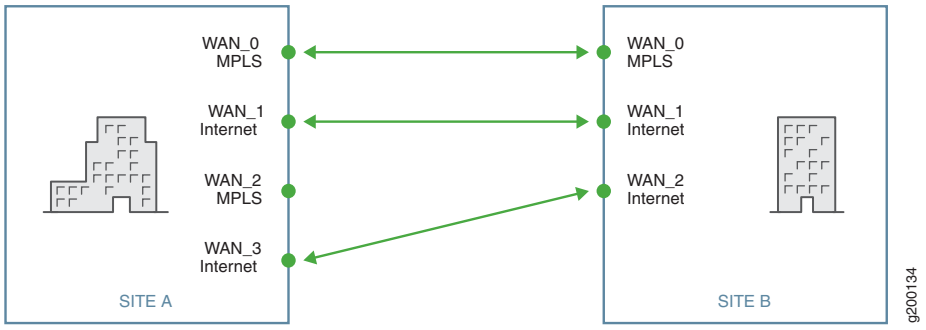
For more information about mesh tags, see *Mesh Tags Overview*.

The full mesh topology supports the following:

- Static policies and Application Quality of Experience (AppQoE)
- Dynamic mesh
- Mesh tags
- LAN segmentation
- Departments
- Multiple VPNs

CSO supports only sparse mode connections in full mesh topology. In sparse mode, a WAN interface of a specific type in a site is connected to only one other interface of the same type (see Figure 1 on page 74). This configuration reduces the number of overlay tunnels formed and is easy to maintain. However, sparse mode is susceptible to SD-WAN network performance deterioration due to connectivity disruptions because if connectivity on one tunnel is lost, then the respective connected WAN interfaces become unreachable.

Figure 1: Sparse Mode



Local Breakout in Full Mesh Topology

Local breakout is supported on all sites in the full mesh topology. Local breakout is the ability of a site to route Internet traffic directly from the site. A site can have multiple WAN interfaces, but only the WAN interfaces (up to a maximum of three) that are *not* enabled exclusively for local breakout traffic are chosen for connecting to the full mesh network. For instance, consider a site that has four WAN interfaces enabled. If WAN_1 on the site is enabled exclusively for local breakout traffic, then only WAN_0, WAN_2, and WAN_3 can be chosen for forming a full mesh.

WAN interfaces that are enabled exclusively for local breakout traffic cannot be used for non-Internet traffic and this makes those WAN interfaces essentially unusable in the full mesh topology. For WAN interfaces that are chosen to connect to the full mesh network, you do not need to provide overlay tunnel information while configuring the site; the overlay tunnel information is computed automatically.

CPE Devices Behind NAT in Full Mesh Topology

CSO supports site-to-site tunnels for WAN links of CPE devices behind NAT in full mesh topology. You can now provide private IP addresses for WAN links behind NAT and create the tunnels to hub or spoke sites. The support for CPE devices behind NAT in full mesh topology is applicable only for spoke devices. The OAM hubs, data hubs, and enterprise hubs or on-premise gateways require static public IP addresses for their WAN interfaces.

The supported NAT types are listed in Table 18 on page 75.

Table 18: CPE Behind NAT in Full Mesh Topology

WAN IP Address	NAT Type	Spoke-to-Hub Tunnel	Spoke-to-Spoke Tunnel
Public IP address	No NAT	Supported	Supported
Private IP address	Full cone NAT	Supported	Supported
Private IP address	Restricted NAT	Supported	Supported
Private IP address	Symmetric NAT	Supported	Not supported

RELATED DOCUMENTATION

SLA Profiles and SD-WAN Policies Overview | 348

About the Tenants Page | 77

Understanding Specific Route-based Routing Within the SD-WAN Overlay

CSO supports specific route-based routing (also known as longest prefix match or LPM) within the SD-WAN overlay routing domain, ensuring a more optimized route selection. The LPM feature ensures that traffic is forwarded on the specific routes learnt from remote devices (SD-WAN devices or non SD-WAN devices).

Here are a few points about how CSO supports a more optimized route selection with the help of LPM:

- CSO installs specific routes in the SLA VRF tables (default, default-reverse, Internet, and MPLS), ensuring that the traffic is forwarded on the shortest path using specific routes.
- CSO applies LPM to the traffic destinations that include provider hub IPVPN, enterprise hub data centers, and site-to-site traffic via enterprise hubs or provider hubs.
- The site-to-data center traffic uses specific routes from the SLA tables. It also uses the branch site's direct tunnel to the enterprise hub which hosts this data center. The traffic does not have to traverse an extra hop via the primary enterprise hub.
- The site-to-IPVPN traffic uses specific routes from the SLA tables. This traffic takes the provider hub route (tunnel) to reach IPVPN. The traffic uses an enterprise hub only when the provider hub is not reachable directly.
- As data forwarding is done using LPM, supernet and subnets can coexist within the SD-WAN department.
- CSO applies LPM to each department in case network segmentation is enabled. LPM is applied to the default VPN in case network segmentation is disabled.
- CSO depends on the default route only as a last resort.

As part of the LPM feature, CSO lets you configure a tenant to either route traffic through the user-selected primary and secondary hubs or prefer the shortest routes for traffic. To do this, you can use the Primary/Secondary Hub Affinity feature on the Tenant Properties tab of the Add Tenant page. See "Adding a Single Tenant" on page 79 for details.

CSO supports two hub affinity modes - enabled and disabled. By default, hub affinity is enabled. See Table 19 on page 77 to see how the hub affinity configuration influences route selection.

Table 19: Route Selection by SD-WAN CPEs Based on the Hub Affinity Mode

When Primary/Secondary Hub Affinity is Enabled	When Primary/Secondary Hub Affinity is Disabled
• Honors the user-selected primary and secondary hubs (enterprise hubs and provider hubs). • Ensures that traffic is forwarded over the primary hub as long as the primary hub is active. • Prefers enterprise hubs over provider hubs.	• Prefers the shortest path (the one with lesser hop count) to reach the remote destination. • Treats the user-selected primary and secondary hubs with the same preference. • Prefers the route via the enterprise hub when the cost of the routes via the enterprise hub and the provider hub is the same. • Prefers the enterprise hub with the lowest router-ID when the cost of routes via two enterprise hubs is the same. • Prefers the provider hub when the route via the enterprise hub is costlier or unavailable. • Prefers the provider hub with the lowest router-ID when the cost of routes via two provider hubs is the same. • Considers any non-parent enterprise hub (a third enterprise hub which a branch site device connects to via DVPN) for the traffic between the branch site and all other possible destinations.

About the Tenants Page

To access this page, click **Tenants**.

A tenant in Contrail Service Orchestration is a customer who can use one or more services (SD-WAN, or Security Services, which is also referred to as Next Gen firewall). You can use this page to add tenants, view tenant details, and delete tenants. You can add tenants by importing tenant-related data through a JSON file. See “Tenant Overview” on page 73.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a tenant. Click the details icon for the tenant, or you can select a tenant and click **More > Detail View**.
- Add a single tenant. See “Adding a Single Tenant” on page 79.
- Delete a tenant. See “Delete a Tenant” on page 99

- Import multiple tenants. See “Importing Data for Multiple Tenants” on page 91.
- Assign Network Services. See “Allocating Network Services to a Tenant” on page 96.
- View tenant create history. See “Viewing the Create History of Imported Tenant Data” on page 97.
- View tenant delete history. See “Viewing the History of Deleted Tenant Data” on page 100.

Field Descriptions

Table 20 on page 78 provides guidelines on using the fields on the Tenants page.

Table 20: Fields on the Tenants Page

Field	Description
Name	Name of the tenant. Click the name to view full information about a tenant.
Site Types	Displays one or more site capabilities (SD-WAN or Security Services) that the tenant can add.
Service Level	Displays the SD-WAN service level (**Advanced** or **Essential**) of the tenant.
State	Displays the tenant creation state.
Sites	Total number of sites that are available for the tenant.
Assigned Services	Number of services that are assigned to the tenant. To assign services to the tenant: 1. Click the Allocate Network Services link in Assigned Service column. The Allocate Network Services to *Tenant-Name* page appears. All network services that are available for the customer are listed. 2. Select the network services and click **Ok**. The network services are assigned to the tenant.
Activated Service Instances	Number of services that have been deployed by the administrator on a connection in the network.
Certificate Renewal	Displays the certificate renewal type (Auto or Manual).

Table 20: Fields on the Tenants Page *(continued)*

Field	Description
Administrator	Administrative user for the tenant.
Last Modified	Date and time when the tenant was last modified.

RELATED DOCUMENTATION

Importing Data for Multiple Tenants | 91

Adding a Single Tenant

You can use the Add Tenant page to add tenant data and other objects associated with a tenant, such as tenant user, network details, deployment scenario, service profiles, and custom properties. A single tenant can support one or more of the following services:

Begin by creating all the resources required for the network point of presence (POP).

The information listed on the Tenants page changes depending on the authentication mode configured:

- **Local Authentication**—You can add the administrative user information as the first step from the **Tenants** page.
- **Authentication and Authorization with SSO Server**—The **Admin User** information is not displayed on the **Tenants** page because users are not created in CSO and they are managed in the SAML identity provider. In addition, users are dynamically authorized to the CSO role based on the mapping rules configured in the SAML authentication.
- **Authentication with SSO Server**—When you create the administrative user, the login page does not require you to configure a password because the user is created in the SSO without the password and you can only enter the username.

To add a tenant:

1. Select **Tenants**.

   The Tenants page appears.

2. Click the add (**+**) icon.

   The Add Tenant page appears.

3. Add the tenant information by completing the configuration according to the guidelines provided in Table 21 on page 80.

> **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   A job to add the tenant is triggered and you are returned to the Tenants page. A confirmation message appears at the top of the page indicating that the job was created. You can click the link in the message to view the details of the job. (Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page. After the job completes successfully, the tenant that you added is displayed on the Tenants page.

   If the SMTP server is configured, an e-mail is sent to the tenant, which includes a URL to access Customer Portal. The URL is active for only 24 hours and is valid only for the first log in.

Table 21: Fields on the Add Tenant Page

Field	Description
Tenant Info	
Name	Enter a name for the tenant. You can use alphanumeric characters and hyphen (-); the maximum length is 32 characters. Example: test-tenant
Admin user	
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Username (Email)	Enter the e-mail address of the user. The e-mail address is used as the username for the user for logging in to CSO.

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Roles	Select one or more roles (both predefined and custom roles) that you want to assign to the tenant user. **NOTE:** In the **Available** column, all tenant scope roles are listed. Click the right arrow(>) to move the selected role or roles from the **Available** column to the **Selected** column. Note that you can use the search icon on the top right of each column to search for role names. To preview the access privileges assigned to a role, click the role name.
Password Policy	
Password Expiration Days	Specify the duration (in days) after which the password expires and must be changed. The range is from 1 through 365. The default value is 180 days. Click **Next** to continue.
Deployment Info	
Services for Tenant	Select one or more services for the tenant: • **SD-WAN**—Select this option if you want the tenant to add SD-WAN sites. SD-WAN sites can have up to 4 WAN links, and the tenant can define intent policies to intelligently route different applications through different WAN links. • **Security Services**—Select this option if you want the tenant to add a standalone firewall site for the CPE device. **NOTE:** The options listed in **Customer Portal > Resources > Site Management > Add** are filtered based on the service that you have selected for a tenant. For example, if you have selected only SD-WAN for a tenant, in **Customer portal > Resources > Sites Management > Add > Branch Site (Manual)**, only the SD-WAN capabilities (Secure SD-WAN Essentials or both Secure SD-WAN Essentials and Secure SD-WAN Advanced based on the SD-WAN service level chosen) are listed.

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Service Level	**NOTE:** This field appears only if you selected the **SD-WAN** in the Services for Tenant field. Choose an SD-WAN service type for the tenant. The following options are available: • **Essentials**—Provides the basic SD-WAN services (Secure SD-WAN Essentials service). This service 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 the web traffic over costly VPN or MPLS links. This service does not support multihoming, dynamic mesh tunnels, cloud breakout profiles, SLA-based steering profiles, pool based source NAT rules, IPv6, MAP-E, or underlay BGP. A tenant with the Essentials service level can create sites only with the Secure SD-WAN Essentials service. **NOTE:** 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. See "Edit Tenant Parameters" on page 89. • **Advanced**—Provides the complete SD-WAN services (Secure SD-WAN Advanced service). This service is ideal for enterprises with one or more data centers, requiring flexible topologies and dynamic application steering. You can establish site-to-site connectivity can be established 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. Click **Next** to continue.
Tenant Properties	
SSL Settings **NOTE:** This setting is applicable only to the SD-WAN deployment scenario.	

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Default SSL Proxy Profile	Click the toggle button to enable a default SSL proxy profile for the tenant. If you enable this option, the following items are created when a tenant is added: • A default root certificate with the certificate content specified (in the Root Certificate field) • A default SSL proxy profile • A default SSL proxy profile intent that references the default profile This option is disabled by default. **NOTE:** You use this option to create a tenant-wide default profile; enabling or disabling this option does *not* mean that SSL is enabled or disabled. If you enable this option, you must add a root certificate.
Root Certificate	You can add a root certificate (X.509 ASCII format) by importing the certificate content from a file or by pasting the certificate content: • To import the certificate content directly from a file: 1. Click **Browse**. The **File Upload** dialog box appears. 2. Select a file and click **Open**. The content of the certificate file is displayed in the Root Certificate field. • Copy the certificate content from a file and paste it in the text box. After the tenant is successfully added, a default root certificate, a default SSL proxy profile, and a default SSL proxy profile intent are created. **NOTE:** • The root certificate must contain both the certificate content and the private key. • For full-fledged certificate operations, such as certificates that need a passphrase, or that have RSA private keys, you must use the Certificates page (**Administration > Certificates**) to import the certificates and install on one or more sites.
VPN Authentication **NOTE:** This setting is applicable only to the SD-WAN (Advanced or Essential) deployment scenario.	

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Authentication Type	Select the VPN authentication method to establish a secure IPsec tunnel: • Preshared Key—Select this option if you want CSO to establish IPsec tunnels using keys. **NOTE:** Preshared Key is the default VPN authentication method. • PKI Certificate—Select this option if you want CSO to establish IPsec tunnels using public key infrastructure (PKI) certificates. Specify the following: ◦ CA Server URL—Specify the Certificate Authority (CA) Server URL. For example, http://*CA-Server-IP-Address*/certsrv/mscep/mscep.dll/pkiclient.exe. The CA server manages the life cycle of a certificate. The CA server also publishes revoked certificates to the certification revocation list (CRL) server. To obtain trusted CA certificates, CSO communicates with the CA server using the Simple Certificate Enrollment Protocol (SCEP). ◦ Password—Specify the password for the CA server. This field is optional. ◦ CRL Server URL—Specify the certificate revocation list (CRL) server URL. For example, http://*Revocation-List-Server-IP-Address*/certservices/abc.crl. CSO retrieves the list of revoked certificates from the CRL server. ◦ Auto Renew CA Certificates—Click the toggle button to enable automatic renewal of certificates. If you enable the Auto Renew toggle button, certificates are automatically renewed for all sites in the tenant. By default, the Auto Renew toggle button is disabled. If you disable the Auto Renew toggle button, certificates must be manually renewed. **NOTE:** If the certificate is expired before the renewal, CSO might not be able to reach the device. ◦ Renew before expiry—This field appears only if you enabled the automatic renewal of certificates. Select the period (3 days, 1 week, 2 weeks, or 1 month) before the expiration date when the certificates get automatically renewed. **NOTE:** The default value is 2 weeks. You can also change the duration in the VPN Authentication page in Customer Portal (**Administration > Certificate Management > VPN Authentication**) page.
Overlay Tunnel Encryption **NOTE:** This is applicable only to the SD-WAN (Advanced or Essential) deployment scenario.	

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Encryption Type	For security reasons, all data that passes through the VPN tunnel must be encrypted. Select the encryption type: • 3DES-CBC—Triple Data Encryption Standard with Cipher-Block Chaining (CBC) algorithm. • AES-128-CBC—128-bit Advanced Encryption Standard with CBC algorithm. • AES-128-GCM—128-bit Advanced Encryption Standard with Galois/Counter Mode (GCM) algorithm. • AES-256-CBC— 256-bit Advanced Encryption Standard with CBC algorithm. • AES-256-GCM—256-bit Advanced Encryption Standard with GCM algorithm. The default encryption type is AES-256-GCM.
Network Segmentation	
Network Segmentation	Click the toggle button to enable or disable network segmentation on the tenant. You enable network segmentation: • To create layer 3 VPNs per department. • Use overlapping IP addresses across departments. **NOTE:** CSO applies longest prefix match (LPM), also known as specific route-based routing, to each department in case network segmentation is enabled. LPM is applied to the default VPN in case network segmentation is disabled. See "Understanding Specific Route-based Routing Within the SD-WAN Overlay" on page 76 for the details.
Dynamic Mesh This setting is applicable only to Secure SD-WAN Advanced deployment scenarios. **NOTE:** Sites with the Secure SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.	
Threshold for Creating a Tunnel Set a threshold value, above which a tunnel is created between two sites.	

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Number of sessions	Specify the maximum number of sessions closed (for a time duration of 2 minutes) between two branch sites. The dynamic mesh tunnel is created between two branch sites if the number of sessions closed (for a time duration of 2 minutes) is greater than or equal to the value that you specified. The default threshold value (the number of sessions for 2 minutes) is 5. For example, if you specify the number of sessions as 5, dynamic mesh tunnels are created if the number of sessions closed between two branch sites in 2 minutes exceeds 5.
Threshold for Deleting a Tunnel Set a threshold value, below which a tunnel is deleted between two sites.	
Number of sessions	Specify the minimum number of sessions closed (for a time duration of 15 minutes) between two branch sites. The dynamic mesh tunnel is deleted between two branch sites if the number of sessions closed (for a time duration of 15 minutes) is lesser than or equal to the value that you specified. The default threshold value (the number of sessions for 15 minutes) is 2. For example, if you specify the number of sessions as 2, the dynamic mesh tunnels are deleted if the number of sessions closed is lesser than or equal to 2.
Max Dynamic Mesh Tunnels	
Max tunnels per CSO	Displays the maximum number of dynamic mesh tunnels that can be created in CSO. The total number of dynamic mesh tunnels that can be created by all tenants in CSO is limited to 125000. A major alarm is raised if the number of dynamic mesh tunnels created by all tenants reaches seventy percent of the maximum value. A critical alarm is raised if the number of dynamic mesh tunnels created by all tenants reaches ninety percent of the maximum value. To view alarms, see **Monitor > Alerts & Alarms > Alarms** in Administration Portal. For more information about alarms, see “About the Alarms Page” on page 454.

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Max tunnels per tenant	Specify the maximum number of dynamic mesh tunnels that the tenant can create. Range: 1 through 50,000. A major alarm is raised if the number of dynamic mesh tunnels created by all sites in a tenant reaches seventy percent of the maximum value. A critical alarm is raised if the number of dynamic mesh tunnels created by all sites in a tenant reaches ninety percent of the maximum value. To view alarms, see **Monitor > Alerts & Alarms > Alarms** in Customer Portal. For more information about alarms, see *About the Alarms Page*.
Dynamic Mesh	Click the toggle button to disable dynamic meshing between sites in the tenant. Dynamic meshing is enabled by default.
Cloud Breakout Settings **NOTE:** This setting is applicable only to Secure SD-WAN Advanced deployment scenarios.	
Customer Domain Name	Enter the domain name of the tenant. The domain name is used in cloud breakout profiles to generate the fully qualified domain name (FQDN). The cloud security providers use the FQDN to identify the IPsec tunnels. Example:test.gmail.com
Quality of service settings	
Class of Service	Click this toggle button to enable (default) or disable CSO from configuring QoS on the devices of a tenant. This setting is valid only for tenants with SD-WAN services. • Enable: CSO configures the class of service (CoS) parameters on an SD-WAN site (branch, cloud spoke, or enterprise hub site) when you deploy the SD-WAN policy for the site. The CoS parameters are derived from the application traffic type profile associated with the path-based steering profile, SLA-based steering profile, or breakout profile, which is referenced in an SD-WAN policy intent. • Disable: CSO does not configure CoS parameters for SD-WAN sites, which means that no CoS parameters are applied to SD-WAN traffic. If you want to apply CoS parameters on SD-WAN traffic, you must use configuration templates to configure and deploy CoS parameters on the SD-WAN sites. Therefore, unless you want to apply customized CoS parameters by using configuration templates, we recommend that you leave this setting enabled.
Advanced Settings (Optional)	

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Primary/Secondary Hub Affinity	By default, hub affinity is enabled. Enable the toggle button to configure the CPEs to prefer the user-selected primary and secondary hubs over other paths for the SD-WAN overlay traffic. Disable the toggle button to configure the CPEs to prefer the shortest routes over the user-selected primary and secondary hubs for the SD-WAN overlay traffic. For more details, see "Understanding Specific Route-based Routing Within the SD-WAN Overlay" on page 76.
Tenant-Owned Public IP Pool	You can add one or more public IPv4 subnets that are part of the tenant's pool of public IPv4 addresses. The tenant IP pool addresses are assumed to be public IP addresses and represent public LAN subnets in SD-WAN branch sites. To add an IPv4 subnet: 1. Click the add (+) icon. An editable row appears inline in the table. 2. In the Addresses field, enter a valid, public IPv4 prefix. **NOTE:** Ensure that the IP addresses configured for a tenant are unique. 3. Click √ (check mark) to save your changes. The prefix that you entered is displayed in the table. You can enter more IPv4 subnets by following the preceding procedure. You can also modify subnets that you entered by selecting a row and clicking the edit (pencil) icon.
Tenant-specific Attributes	If you have set up a third-party provider edge (PE) device by using software other than CSO, then configure settings on that router by specifying custom parameters and its corresponding values.
Name	Specify any information about the site that you want to pass to a third-party router. Example: Location
Value	Specify a value for the information about the site that you want to pass to a third-party device. Example: Boston Click **Next** to continue.

Table 21: Fields on the Add Tenant Page *(continued)*

Field	Description
Summary	You can review the configuration in the Summary tab and modify the settings, if required. You can also download the settings that you configure as a JavaScript Object Notation (JSON) file by clicking the **Download as JSON** link at the bottom of the page.

RELATED DOCUMENTATION

Tenant Overview | 73

Edit Tenant Parameters

You, as an SP administrator or OpCo administrator, can modify the parameters configured for a tenant from the Tenants page.

To modify the parameters configured for a tenant:

1. Select **Tenants**.

   The Tenants page appears.

2. Select the tenant whose parameters you want to modify and click the **Edit** icon (pencil).

   The Edit Tenant page appears, displaying the same fields that are presented when you add a tenant.

3. Modify the tenant parameters as needed. For more information on these parameters, see "Adding a Single Tenant" on page 79.

4. Click **Save** to save the changes or click **Cancel** to discard the changes.

   If you click Save, the changes that you made for the tenant are saved.

   Subsequently, a tenant edit job is triggered and a confirmation message, indicating that a tenant edit job is created successfully, appears on the Tenant Settings page.

5. (Optional) You can click the job name in the message to view details of the job (including job status, start date and time, and end date and time) on the **Update tenant settings Details** page. Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

If the job is completed successfully, a confirmation message appears on top of the Tenants page.

Table 22 on page 90 describes the tenant parameters that you can modify.

Table 22: Tenant parameters

Tenant Capability	Tenant Parameters
Tenant Info	
Basic Information	
Name	You cannot modify the name of the tenant.
Password Policy	
Password Expiration Days	The settings are applicable to all new users and users whose password has expired.
Deployment Info	
Services for Tenant	You can add or remove one or more services for the tenant. **NOTE:** The changes are applied to newly-added sites only.
Service Level	**NOTE:** This field appears only if you have selected the **SD-WAN** in the Services for Tenant field. This field is read-only if the tenant is using the Secure SD-WAN Advanced service. However, if the tenant is using the Secure SD-WAN Essentials service, you can upgrade the service level to Advanced by selecting the **Advanced** option.
Tenant Properties	

Table 22: Tenant parameters ***(continued)***

Tenant Capability	Tenant Parameters
Tenant with SD-WAN capability	You can modify the following parameters only before SD-WAN sites are added by the tenant: • SSL Settings • VPN authentication **NOTE:** If **PKI Certificate** is configured as the authentication type during tenant onboarding, you can modify the PKI properties (CA Server URL, Password, CRL Server, and Auto Renew) even after SD-WAN sites are added by the tenant. • Overlay Tunnel Encryption • Network Segmentation You can modify the following parameters even after SD-WAN sites are added by the tenant: • Dynamic Mesh > Threshold for Creating a Tunnel and Threshold for Deleting a Tunnel • Cloud Breakout Settings • Tenant-Specific Attributes
Tenant with Security Services	Tenant-Specific Attributes

Importing Data for Multiple Tenants

IN THIS SECTION

- Creating a Tenant Data File | **92**
- Importing Tenant Data | **95**

You can use the Import Tenants page to import tenant data and other objects associated with the tenant, such as administrative users, sites, and topology. You can start by downloading a JSON template and using it to customize the data file that you want to import.

Creating a Tenant Data File

To create a tenant data file:

1. On the Tenants page, click **Import Tenants > Import**.

   The Import Tenants page appears.

2. Click **Download Sample JSON** to download a sample JavaScript Object Notation (JSON) template.

   The sample tenant template file is downloaded to your system.

3. On the Import Tenants page, click **Cancel**.

4. Open the template file.

5. Save the template file to your computer with an appropriate name.

6. Customize the file with your tenant data, using Table 23 on page 92 as a reference.

7. Save the customized tenant data file.

You can add tenants using the customized tenant data file.

Table 23: Tenant Configuration Fields

Field	Description
tenant_name	Specify a unique name for the tenant. CSO uses the unique name for internal communications.
tenant_display_name	Specify the display name for the tenant to be displayed on the GUI interfaces. You can only use alphanumeric characters and hyphens; the maximum length allowed is 32 characters.
password_expiration_radio	Specify the duration (in days) after which the password expires and must be changed.
tenant_admin	

Table 23: Tenant Configuration Fields *(continued)*

Field	Description
admin_user_name	Specify a unique name for the tenant administrator. Example: admin-tenant-a
first_name	Enter the first name of the tenant.
last_name	Enter the second name of the tenant.
password_expiration_interval	Specify the duration (in days) after which the password expires and must be changed. The range is from 1 through 365.
topology_type	Specify the topology type (SD-WAN)
default_ssl_proxy_profile	Specify whether you want to enable or disable SSL proxy profile for the tenant
properties	If you have set up a third-party provider edge (PE) device by using software other than Contrail Service Orchestration, then configure settings on that router by specifying custom parameters and its corresponding values. Specify information (name and value) about the site that you want to pass to a third-party router.
vpn	Specify the VPN authentication method to establish a secure IPsec tunnel.
departments	Specify if you want to enable network segmentation on the tenant.
managed_wan_topology	
network_name	Specify a unique name for the customer Layer 3 VPN network. You can use an unlimited number of alphanumeric characters, including symbols. Example: vcpe-tenant-a-l3vpn
router_info (cloud_site_info)	
router_name	Specify the router name that connects to the tenant site.
route_target	Specify the route target of the transit network for the tenant. Example: 8888:889

Table 23: Tenant Configuration Fields *(continued)*

Field	Description
right_network_name	Specify the name of the transit network for the tenant. Example: internet, corp-vpn-right
subnet	Specify the subnet of the transit network for the tenant. Example: 10.154.0.0/24
route_target (internet-info)	Specify the route target of the site virtual network. Example: 8888:887
subnet (internet-info)	Specify the IP address of the subnet that connects the site to the Internet. Example: 10.155.0.0/24
pop_info (cloud_site_info)	
pop_name	Specify the name of the POP that manages the site. You can use an unlimited number of alphanumeric characters, including symbols. Example: pne-pop10
route_target	Specify the route target of the transit network for the tenant. Example: 8828:889
right_network_name	Specify the name of the transit network for the tenant. Example: corp-vpn-right
subnet	Specify the subnet of the transit network for the tenant. Example: 10.151.0.0/24
route_target (internet-info)	Specify the route target of the site virtual network. Example: 8888:887
subnet (internet-info)	Specify the IP address of the subnet that connects the site to the Internet. Example: 10.155.0.0/24
pop_info (data_center_site_info)	

Table 23: Tenant Configuration Fields *(continued)*

Field	Description
pop_name	Specify the name of the POP. You can use an unlimited number of alphanumeric characters, including symbols. Example: pne-pop10
route_target	Specify the route target for the corporate data center network. Example: 65412:772
subnet	Specify the subnet of the corporate data center network. Example: 10.155.0.0/24
route_target (internet-info)	Specify the route target for the Internet network. Example: 8888:887
subnet (internet-info)	Specify the subnet IPv4 address for the Internet network. Example: 10.155.0.0/24

Importing Tenant Data

To import tenant data:

1. Click **Tenants > All Tenants > Import Tenants**.

   The Import Tenants page is displayed.

2. Click **Browse** and navigate to the directory where the tenant file is located.

3. Select the tenant file and click **Open**.

4. Click **Import**.

   The status of the import operation is displayed. You can click **View Details** for more information about the import operation. If the import operation state is successful, then proceed to Step 4 or verify the tenant file format.

5. Click **OK**.

The new tenants are displayed on the Tenants page. You can click any tenant to view more information about the tenant.

RELATED DOCUMENTATION

Viewing the Create History of Imported Tenant Data | 97

Allocating Network Services to a Tenant

Use the Tenants page to assign the network services to a tenant. Network services are created and saved in Network Service Designer. When setting up a tenant with Administration Portal, you must import the network services and assign them to customers. After the allocation, tenants can see and activate the network services in Customer Portal.

Before You Begin

To assign network services:

1. Click **Tenants**.

   The Tenants page appears.

2. Select a customer and click **Allocate Network Services**.

   The Allocate Network Services to *Tenant-Name* page appears. All network services that are available for the customer are listed.

3. Select the network services and click **Ok**.

   The network services are assigned to the tenant.

RELATED DOCUMENTATION

About the Tenants Page | 77

Viewing the Create History of Imported Tenant Data

You can use the Create History page to view the imported tenant data, status of the import operation, and log details.

To view the create history of imported tenant data:

1. Click **Tenants > Import Tenants > Create History**.

   The Create History page is displayed. Table 24 on page 97 describes the fields on the Import History page.

2. Click the task name.

   The Create Tenants Task page appears. Table 25 on page 98 describes the fields on the Import Tenants Task page.

3. Click the task ID on the Job Status page to view the job details, such as whether this job succeeded or failed.

   Table 26 on page 98 describes the fields on the Job Status page for imported tenant data.

Table 24: Fields on the Import History Page

Field	Description
In progress	View the number of import tasks that are in progress.
Success	View the number of import tasks that succeeded.
Failure	View the number of import tasks that have failed.
Name	View the name of the task.
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.
Status	View the status of the task to know whether the task succeeded or failed.
Log	View the import logs. Click a log to access more detailed information about the imported log.

Table 25: Fields on the Import Tenants Task Page

Field	Description
Success	View the number of times the import operations succeeded for a tenant.
Failure	View the number of times the import operations failed for a tenant.
Task ID	View the ID created for the task. Click the task ID to view the import log details corresponding to a tenant.
Status	View the status of the task to know whether the task succeeded or failed.

Table 26: Fields on the Job Status Page for Imported Tenant Data

Field	Description
Name	View the name of the task.
User	View the name of the user who imported the task.
State	View the status of the task to know whether the task succeeded or failed.
Actual Start Time	View the start date and time of the task.
End Time	View the end date and time of the task.

RELATED DOCUMENTATION

Importing Data for Multiple Tenants | 91

Delete a Tenant

Users with the SP (Service Provider) Administrator or OpCo (Operating Company) Administrator role can delete a tenant and its associated sites.

> **NOTE:** Before triggering the deletion of a tenant, ensure that you delete the allocated network services and deployed policies for all the associated sites.

To delete a tenant:

1. Select **Tenants**.

   The Tenants page appears.

2. Select the tenant that you want to delete.

   > **NOTE:**
   > - You can delete only one tenant at a time.
   > - When a tenant is deleted, the sites, users, devices, and all other data associated with the tenant are deleted.

3. Click the delete (trash can) icon.

   The Confirm Delete dialog box appears.

4. Click **Yes**.

   The Confirm dialog box appears indicating that the sites associated with the tenant will also be deleted.

5. Click **Yes**.

   A job to delete the tenant is triggered and you are returned to the Tenants page.

   A confirmation message appears (with the job link) at the top of the page indicating that the job was created. You can click the job link to view the status of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor** > **Jobs**) page.

   After the job completes successfully, the tenant is removed on the Tenants page.

RELATED DOCUMENTATION

Viewing the History of Deleted Tenant Data | 100

About the Tenants Page | 77

Viewing the History of Deleted Tenant Data

You can use the Delete History page to view the deleted tenant data, status of the delete operation, and log details.

To view the history of deleted tenant data:

1. Click **Tenants > Import Tenants > Delete History**.

   The Delete History page is displayed. Table 27 on page 100 describes the fields on the Delete History page.

2. Click the task name.

   The Delete Tenants Tasks page appears. Table 28 on page 101 describes the fields on the Delete Tenants Tasks page.

3. Click the task ID in the Job Status page to view the job details, such as whether this job succeeded or failed.

   Table 29 on page 101 describes the fields on the Job Status page for deleted tenant data.

Table 27: Fields on the Delete History Page

Field	Description
In progress	View the number of delete tasks that are in progress.
Success	View the number of delete tasks that succeeded.
Failure	View the number of delete tasks that failed.
Name	View the name of the task.
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.

Table 27: Fields on the Delete History Page *(continued)*

Field	Description
Status	View the status of the task to know whether the task succeeded or failed.
Log	View the delete logs. Click a log to access more detailed information about deleted logs.

Table 28: Fields on the Delete Tenants Tasks Page

Field	Description
Success	View the number of delete operations that succeeded for a tenant.
Failure	View the number delete operations that failed for a tenant.
Task ID	View the ID created for the task. Click the task ID to view the delete log details corresponding to a tenant.
Status	View the status of the task to know whether the task succeeded or failed.

Table 29: Fields on the Job Status Page for Deleted Tenant Data

Field	Description
Name	View the name of the task.
User	View the name of the user who deleted the task.
State	View the status of the task to know whether the task succeeded or failed.
Actual Start Time	View the start date and time of the task.
End Time	View the end date and time of the task.

RELATED DOCUMENTATION

Importing Data for Multiple Tenants | 91

Viewing the Create History of Imported Tenant Data | 97

Dynamic Mesh Tunnels Overview

In releases earlier than CSO 4.1.0, all the overlay tunnels for the site are established between branch sites during the Zero Touch Provisioning (ZTP) process.

However, starting with CSO Release 4.1.0, during ZTP, only the following static tunnels are established:

- Between a branch site and the corresponding enterprise hub (primary enterprise hub or secondary enterprise hub)
- Between a branch site and the provider hub (primary provider hub or secondary provider hub)
- Between two enterprise hubs

Therefore, the communication between two branch sites (with the Secure SD-WAN Advanced service) is established only through the enterprise hub or the provider hub.

For sites with the Secure SD-WAN Advanced service, CSO dynamically creates or deletes a mesh tunnel (also called DVPN tunnel) between two branch sites directly so that the traffic does not go through an enterprise hub or a provider hub, if:

- The number of sessions closed between two branch sites crosses the configured threshold value, and
- The WAN links of branch sites have matching mesh tags. For more information, see *Mesh Tags Overview*.

> **NOTE:** The dynamic mesh feature is applicable only for Secure SD-WAN Advanced sites (Full mesh).
>
> Sites with the Secure SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites. However, an OpCo administrator or a tenant administrator can create a static tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

The SP administrator, OpCo administrator, or tenant administrator can modify the default threshold value on the following pages:

- SP administrator or OpCo administrator:
  - **Administration > Dynamic Mesh** page of Administration Portal
  - The Add Tenant page
- Tenant administrator:
  - The **Administration > Tenant Settings** page (Dynamic Mesh section) of Customer Portal (global level)
  - The Add Branch Site page

- The Add Enterprise Hub page

The threshold value that you specify at site-level takes precedence over the tenant-level and global-level threshold values.

That is, the threshold value that you specify on the Add Tenant page overrides the threshold value that you specified on the Dynamic Mesh page of Administration Portal.

Similarly, the threshold value that you specify in the Add Site page overrides the threshold value that you specified on the Dynamic Mesh page and Add Tenant page.

> **NOTE:** Changes that OpCo and SP administrators make at global level do not apply to existing tenants. The changes are applied only to tenants added after the changes have been made at the global level.

RELATED DOCUMENTATION

Configuring Dynamic Mesh Tunnel Thresholds for all Tenants | **104**

Configuring Dynamic Mesh Tunnel Thresholds for all Tenants

CSO dynamically creates or deletes a mesh tunnel (that does not pass through an enterprise hub or a provider hub) between two branch sites, if:

- The number of sessions closed between two branch sites crosses the threshold value.
- The WAN links of the two branch sites have matching mesh tags.

For more information on dynamic mesh tunnels, see "Dynamic Mesh Tunnels Overview" on page 102.

NOTE:

- Changes made to the dynamic mesh threshold values are not applicable to existing tenants. Changes are applicable only to tenants that are added after the threshold values are modified.
- You can also modify the threshold values while adding a tenant. The threshold values that you specify on the Add Tenant page (for a specific tenant) override the threshold value previously configured for all tenants.
- Sites with the Secure SD-WAN Essentials service do not support creation or deletion of dynamic mesh tunnels based on a user-defined threshold for the number of sessions closed between two branch sites.

To modify dynamic mesh threshold values for all tenants:

1. Select **Administration** > **Dynamic Mesh**.

   The Dynamic Mesh page appears.

2. Complete the configuration according to the guidelines in Table 30 on page 105.

   NOTE: Fields marked with * are mandatory.

3. Click **Save**.

   A confirmation message appears indicating that the threshold values are saved and you are returned to the Dynamic Mesh page.

Table 30: Fields on the Dynamic Mesh Page

Field	Description
Threshold for Creating a Tunnel	
Number of Sessions	For creating dynamic mesh tunnels, specify the number of sessions closed (for a duration of 2 minutes) between two branch sites. If the number of sessions closed (for a duration of 2 minutes) is greater than or equal to the value that you specified, a dynamic mesh tunnel is created between two branch sites. The default threshold value (the number of sessions closed for 2 minutes) is 5. For example, if you specify the number of sessions closed as 10, dynamic mesh tunnels are created if the number of sessions closed between two branch sites in 2 minutes is greater than or equal to 10.
Threshold for Deleting a Tunnel	
Number of Sessions	For deleting dynamic mesh tunnels, specify the number of sessions closed (for a duration of 15 minutes) between two branch sites. If the number of sessions closed (for a duration of 15 minutes) is lesser than or equal to the value that you specified, a dynamic mesh tunnel is deleted between two branch sites. The default threshold value (the number of sessions for 15 minutes) is 2. For example, if you specify the number of sessions closed as 5, dynamic mesh tunnels are deleted if the number of sessions closed between two branch sites in 15 minutes is lesser than or equal to 5.

RELATED DOCUMENTATION

Dynamic Mesh Tunnels Overview | 102

Updating the Terms of Use

When you create a CSO account for a tenant, an e-mail (with the subject line CSO Account Created) is sent. This e-mail contains a URL that allows the tenant to log in to Customer Portal. The URL is active for only 24 hours and is valid only for the first log in.

When the tenant logs in to Customer Portal for the first time, the tenant must read and agree to the terms of use document.

The terms of use document is a policy document (pdf format) that is hosted on Juniper Networks site.

In this page you can specify the URL from which an OpCo admin or a tenant can view or download the Terms of Use document. If there is an update to the Terms of Use document, you can specify the date from which you want the terms of use document to be effective.

To update the information related to the Terms of Use document:

1. Select **Administration** > **Terms of Use**.

   The Terms of Use page appears.

2. Update the fields according to the guidelines in Table 31 on page 106.

   NOTE: Fields marked with * are mandatory.

3. Click **Save** to save the changes.

   A confirmation message appears indicating that the URL and the effective date that you have specified are saved.

Table 31: Fields on the Terms of Use Page

Field	Description
Document URL	Specify the URL from which the tenant can view or download the Terms of Use document. For example, https://www.juniper.net/assets/us/en/local/pdf/legal/*Document-Name*.pdf
Effective date	If there is an update to the Terms of Use document, you can schedule a date to notify tenants about the change. Select the date from which the Terms of Use document is effective. The format is, YYYY-MM-DD. On the specified date, the Terms of Use page pops up in Customer Portal. The Terms of Use page includes the link to the updated document. By selecting the check box in the Terms of Use page the tenant agrees to the terms and conditions mentioned in the updated document.

RELATED DOCUMENTATION

Accessing Administration Portal | 33

5
CHAPTER

Managing Operating Companies

Operating Companies Overview | **108**

About the Operating Companies Page | **115**

Creating Operating Companies | **116**

Editing and Deleting Operating Companies | **119**

Operating Companies Overview

IN THIS SECTION

- OpCo Hierarchy Management | 108
- OpCo Authentication and Authorization | 109
- Access Privileges for Global SP, OpCo, and Tenant Users | 110
- Benefits of Operating Companies | 115

Contrail Service Orchestration (CSO) supports operating companies in a service provider environment. An operating company (OpCo) is a region-specific service provider that can create and manage its own tenants and provide services to them—thus an OpCo is a subset of the global service provider and functions as a service provider for its own tenants.

A global service provider can create one or more operating companies and share resources (cloud hub devices, device templates, and so on) with the operating companies. The global service provider manages its own tenants as well as the operating companies.

For example, the Global SP administrator can create operating companies such as OpCo_Spain, OpCo_Italy, and OpCo_France under the global service provider V1_Global and share the resources with these operating companies.

Tenants managed by one OpCo are isolated from tenants of another OpCo—that is, resources from one OpCo cannot be shared with other operating companies.

> **NOTE:** When an SP administrator creates one or more operating companies under the service provider, the service provider is called a global service provider and the SP administrator is called the Global SP administrator.

This topic contains the following sections:

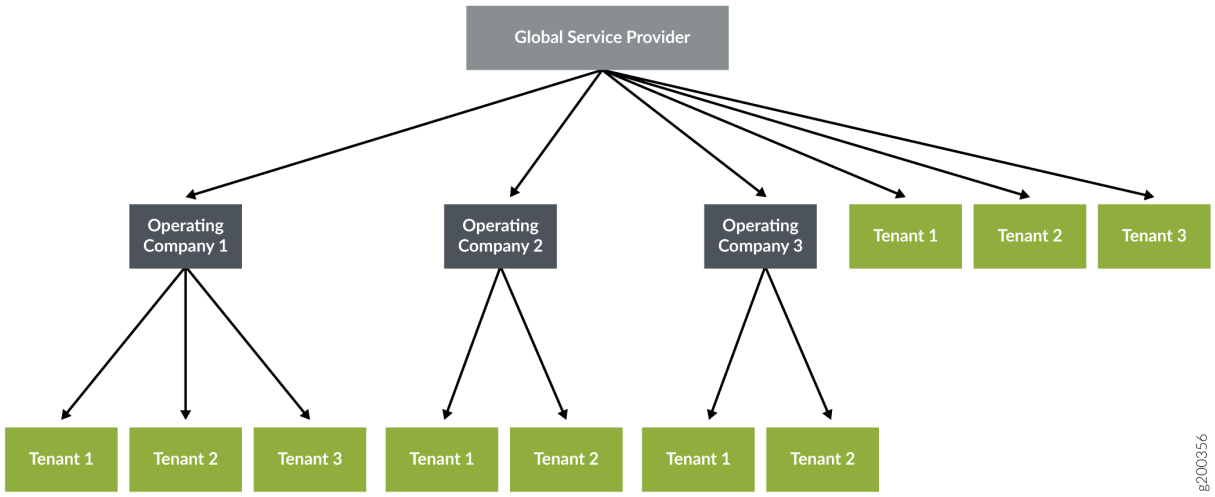
OpCo Hierarchy Management

The CSO multitenant hierarchy has the following levels:

- **Global service provider**—Contains one or more operating companies and its tenants, manages resources at the service provider level, and shares common resources with operating companies and tenants. The Global SP administrator has the required access privileges to view and access resources across operating companies.
- **Operating company**—A region-specific service provider that can manage its tenants and provide services to them. Tenants managed by one OpCo are isolated from tenants of another OpCo. A global service provider share resources (cloud hub devices, device templates, and so on) with the operating companies and their tenants.
- **Tenant**—A tenant uses the resources that the global service provider or the tenant's OpCo shares with it.

Figure 2 on page 109 shows the relationship between the global service provider, operating companies, and tenants. A global service provider can have one or more operating companies and tenants, and each OpCo can be assigned one or more tenants.

Figure 2: OpCo Hierarchy Management



OpCo Authentication and Authorization

A newly created OpCo can use either the same authentication method used by the global service provider or its own SSO server to authenticate its users. If the OpCo uses its own SSO server, the SSO server details need to be added in the Authentication (**Administration > Authentication**) page. For more information about configuring a SSO server, see "Configuring a Single Sign-On Server" on page 66.

The following authentication methods are available for OpCo users:

- Local authentication

- Authentication using an SSO server
- Authentication and authorization using an SSO server

For more information about authentication methods, see "Authentication Methods Overview" on page 61.

Access Privileges for Global SP, OpCo, and Tenant Users

Global SP, OpCo, and tenant users can perform tasks based on the access privileges assigned to these roles.

- An OpCo administrator, Global SP administrator, tenant administrator, or users with administrator role privileges can can perform an administrator's tasks.
- Global SP users cannot access operating companies and tenants automatically. An OpCo administrator, a tenant administrator, or users with administrator role privileges need to provide the required access privileges to the Global SP users. Therefore, global users can view and access operating companies and tenants.
- An OpCo administrator, tenant administrator, or users with the administrator role privileges can add global SP users to the OpCo or to the tenant. Therefore, global SP users can perform tasks specific to an OpCo or a tenant by switching the scope to a specific OpCo or tenant.

For more information about roles, see "Role-Based Access Control Overview" on page 399.

Table 32 on page 110 shows the access privileges of Global SP, OpCo, and Tenant Users.

Table 32: Access Privileges for Global SP, OpCo, and Tenant Users.

Main Menu	Submenu	Access Privileges
Dashboard—Display widgets for both global SP and an OpCo users when they log in to CSO. However, for OpCo users, the following information is filtered based on OpCo tenants.		
	Tenant Sites – Total Alerts	Global SP users can view alerts across all tenants. OpCo users can view alerts across their tenants.
	POPs – Capacity Used	Global SP users can create and manage all POPs and share the POPs with operating companies. Global SP and OpCo users can view POPs usage (CPU, Memory, and Storage).
	Cloud Services: POP Resources Used	Global SP and OpCo users can view POPs usage (CPU, Memory, and Storage).
	Top 5 POPs with Alerts	Global SP and OpCo users can view POPs alerts. However, OpCo users can only view POP alerts across their tenants.

Table 32: Access Privileges for Global SP, OpCo, and Tenant Users. *(continued)*

Main Menu	Submenu	Access Privileges
	Top 5 Tenants with Alerts	Global SP users can view alerts across all tenants. OpCo users can only view alerts across their tenants.
	Top 5 Sites with Alerts	Global SP users can view alerts across their tenant sites. OpCo users can only view alerts across their tenant sites.
Monitor—Displays a geographical map of all POPs and alerts associated with each POP. Global SP users can create and manage all POPs and share the POPs with operating companies. Both Global SP and OpCo users can view POPs and their associated alerts. However, tenants can view only the alerts of their sites.		
	Alerts	Alerts are generated for a tenant's site or device and the alerts are shared with its tenant's OpCo and global service provider. The tenant user can only view tenant-specific alerts and the OpCo users can view alerts of the OpCo's tenants. Global SP users can view all alerts across all tenants.
	Alert Definition – SD-WAN Alert	Global SP users can create SD-WAN alert definitions. OpCo users and tenants can view SD-WAN alert definitions.
	Alert Definition – Security Alert	Tenants can create security alert definitions. OpCo and Global SP users can view security alert definitions.
	Alarms	Alarms are generated for a specific tenant and shared with an OpCo's tenant and Global SP users. Global SP users can view alarms across all tenants and the OpCo users can view alarms specific to their tenants. Global SP users can view alarms specific to global devices (for example, cloud hub devices).
	Tenants SLA Performance	SLA performance is measured for each tenant. Global SP users can view the SLA performance of all tenants. OpCo users can view the SLA performance of their tenants.
	Jobs – All	Global SP users can view and edit the scheduled jobs across all tenants. OpCo users can view and edit scheduled jobs of the OpCo's tenants. Tenants can view and edit their scheduled jobs.
	Jobs – Scheduled	Global SP users can view scheduled jobs across all tenants. OpCo users can view scheduled jobs specific to their tenants.

Table 32: Access Privileges for Global SP, OpCo, and Tenant Users. *(continued)*

Main Menu	Submenu	Access Privileges
Resources—Global SP and OpCo users can create and manage POPs, tenant devices, cloud hub devices, device profiles, and device images. POPs and cloud hub devices are shared globally. Both Global SP and OpCo users can view all POPs and cloud hub devices.		
	POP	Global SP users can create POPs and share the POPs with all operating companies and their tenants. Operating companies and tenants of global service provider have read-only access to POPs.
	Tenant Devices	Tenants own tenant devices and share the devices with the tenant's OpCo and global service provider.
	Cloud Hub Devices	Global SP users can create and manage all cloud hub devices and share the devices with operating companies and tenants. Operating companies and tenants have read-only access to cloud hub devices.
	Virtual Route Reflector (VRR)	The VRR is created during CSO deployment and is available to all operating companies and tenants. A virtual route reflector (VRR) resides on a virtual machine (VM) on each regional microservices server. During the CSO installation, a VRR is installed on the regional servers. The VRR has a fixed configuration that you cannot modify. Use of a VRR enhances scaling of the BGP network with low cost and removes the need for hardware-based route reflectors that require space in a data center and ongoing maintenance. **NOTE:** VRR is not a UI element.
	Device Profiles	Device profiles can be managed by: • Global SP—Global SP users can create, modify, and share device profiles with operating companies and tenants. Operating companies and tenants have read-only access to the global service provider's device profiles. • Operating companies—OpCo users can create, modify, and share device profiles with the OpCo's tenants. The global SP users have read-only access to the OpCo's device profiles.
	Images	Global SP users can upload all device images, and the images are available to all operating companies and tenants associated with global service provider and operating companies.

Table 32: Access Privileges for Global SP, OpCo, and Tenant Users. ***(continued)***

Main Menu	Submenu	Access Privileges
Configuration—Global SP and OpCo users can create and manage application traffic types, application SLA profiles, shared objects, and network services and share them with other operating companies.		
	Application Traffic Type Profiles	Global SP users can create and manage application traffic type profiles. Operating companies and tenants have read-only access to application traffic type profiles.
	Application SLA Profiles	Application SLA profiles can be managed by: • Global SP—Global SP users can create application SLA profiles. Operating companies and tenants have read-only access to application SLA profiles. • Operating companies—OpCo users can create SLA application profiles. Global SP users and OpCo tenants have read-only access to SLA application profiles. • Tenants—Both global service provider and OpCo tenants can create SLA application profiles. Global SP and operating companies have read-only access to their tenants SLA application profiles.
	Shared Objects	Global SP users can create and manage shared objects. Operating companies and tenants have read-only access to the shared objects of the global service provider.
	Network Services (VNF and NSD)	Global SP users can create and manage network services and share them with operating companies and tenants.
Tenants—Global SP and OpCo users can create and manage tenants for the global service provider and operating companies.		
	Global Tenants	Global SP users can create and manage their tenants. However, if the global service provider user has privilege to access an OpCo, then the user can switch to OpCo scope and manage OpCo tenants.
	Operating companies	Operating companies can be managed only by the Global SP users. OpCo users are not allowed to create operating companies.
	OpCo Tenants	OpCo users can create and manage their tenants. The Global SP user has read-only access to the OpCo's tenants.
Administration—Global SP and OpCo users can create and manage users, and manage application databases, licenses, and preferences. Both Global SP and OpCo users can configure authentication methods and SMTP settings, and customize e-mail templates for their tenants.		

Table 32: Access Privileges for Global SP, OpCo, and Tenant Users. *(continued)*

Main Menu	Submenu	Access Privileges
	Users	Users can be managed by: • Global SP—Global SP users can create and manage users for their scope (service provider, tenant, and OpCo). • OpCo—OpCo users are created with appropriate access privileges by switching the scope to an OpCo.
	Authentication	Authentication methods can be configured at: • Global SP—Global SP users can configure an authentication method for service provider and tenant users. • Operating companies—OpCo users can use the same authentication method used by the global service provider or use their SSO server for their tenant users.
	Licenses	Global SP users can upload and manage licenses. OpCo and tenant users can upload their licenses.
	Signature Database	Global SP users can manage and share application signature database with all operating companies and tenants.
	SMTP	SMTP settings can be configured for: • Global SP—Global SP users can configure SMTP settings to send e-mails to their users (service provider, tenant, and OpCo) and tenants. • Operating companies—OpCo users can configure their SMTP settings to send e-mails to their users (both service provider and tenant) and tenants.
	Preferences (Portal Customization)	Global SP users can create and manage themes for all operating companies and tenants. Operating companies can use the same theme used by the global service provider. Only the Global SP users can view and modify the theme settings.
	E-mail Templates	Global SP users can customize e-mail messages. OpCo users can create their e-mail templates for their tenants.

Benefits of Operating Companies

- An OpCo relieves the global service provider of the responsibility of tenant management for a specified region. For example, the OpCo can look after a country-specific regulatory, billing, or operational need for the global service provider.
- With the creation and configuration of operating companies, the Global SP administrator needs to define only a single solution across various regions and countries, and yet enable the operating companies to manage their assigned sets of tenants.
- Each OpCo can use a shared CSO cloud-hosted solution instead of using its own CSO installation. OpCo administrators can access a centrally deployed CSO instance, and local resources, and offer SD-WAN services to their tenants.

About the Operating Companies Page

To access this page, click **Tenants > Operating Companies (OpCos)** in Administration Portal.

Use this page to view and manage operating companies of a Global SP. You can add, edit, and delete operating companies. Each operating company can have its own set of tenants.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an operating company. See "Creating Operating Companies" on page 116.
- Edit or delete an operating company. See "Editing and Deleting Operating Companies" on page 119.

Field Descriptions

Table 33 on page 115 describes fields on the Operating Companies page.

Table 33: Fields on the Operating Companies Page

Field	Description
OpCo Name	Name of the operating company.

Table 33: Fields on the Operating Companies Page *(continued)*

Field	Description
Authentication Method: OpCo users	A authentication method that the operating company uses to authenticate its users.
Authentication Method: OpCo Tenant users	A authentication method that the operating company uses to authenticate its OpCo tenant users.
Administrator	Name of the administrator that created the operating company.

RELATED DOCUMENTATION

- Operating Companies Overview | **108**
- Creating Operating Companies | **116**
- Editing and Deleting Operating Companies | **119**

Creating Operating Companies

Use the Operating Companies (OpCos) page to create operating companies. The Global SP administrator or users with Create OpCo privilege can create one or more operating companies.

> **NOTE:** Only users with the OpCo administrator role can create its tenants. However, they cannot create further operating companies.

To create an operating company:

1. Select **Tenants > Operating Companies**.

   The Operating Companies (OpCos) page appears, displaying the details of the available operating companies.

2. Click the add icon (+) to create a new operating company.

   The Create Operating Companies (OpCos) page appears.

3. Complete the configuration according to the guidelines provided in Table 34 on page 117.

4. Click **OK**.

   A new operating company is created and listed on the Operating Companies (OpCos) page.

Table 34: Fields on the Create Operating Company Page

Field	Description
Name	Enter a unique name for the operating company. The name can contain alphanumeric characters, underscore, period, and space. The maximum length is 15 characters.
Portal URLs	
Admin Portal	Enter the URL of the Administration portal. End users can use this URL to access the administration portal.
Tenant Portal	Enter the URL of the Customer Portal. End users can use this URL to access the customer portal.
Authentication Method	
OpCo Users	Select the authentication method to authenticate OpCo users. The default method is local authentication. • **Same as Global**—Select this option to use the authentication method which is used by the Global SP. • **Allow OpCo to decide**—Select this option to use OpCo's own authentication method.
OpCo Tenant Users	Select the authentication method to authenticate OpCo's tenant users. The default method is local authentication. • **Same as Global**—Select this option to use the authentication method which is used by the Global SP. • **Allow OpCo to decide**—Select this option to use OpCo's own authentication method.
Admin User	
First Name	Enter the first name of the administrative user.
Last Name	Enter the last name of the administrative user.
Username (Email)	Enter the e-mail ID of the administrative user. The e-mail ID is the username for the administrative user.

Table 34: Fields on the Create Operating Company Page *(continued)*

Field	Description
Role	Select one or more roles (both predefined and custom roles) that you want to assign to the OpCo user. You can assign both service provider and tenant roles to OpCo users. Click the greater-than icon (>) to move the selected role or roles from the **Available** column to the **Selected** column. You can use the search icon on the top right of each column to search for role names. The following are the predefined roles for OpCo users: • **OpCo Admin**—Users with the OpCo Admin role have full access to the OpCo's Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with OpCo Admin, OpCo Operator, and custom roles. They can onboard tenants and add the first tenant user during the OpCo's tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant. • **OpCo Operator**—Users with the OpCo Operator role have read-only access to the OpCo's Customer Portal UI and APIs.
Password Policy	
Password Expiration Days	Specify the duration (in days) after which the password expires and must be changed. The range is from 1 through 365. The default value is 180 days.
MAP-E Network Settings	
MAP-E for Tenants	Click the toggle button to enable the OpCo's tenants to configure the Mapping of Address and Port with Encapsulation (MAP-E) functionality for their branch sites with NFX150 as the CPE. MAP-E supports transporting IPv4 packets across an IPv6 network by using IPv4-in-IPv6 encapsulation. If you enable this toggle button, you must select a manufacturer code to be associated with the OpCo user. **NOTE:** MAP-E is compliant only with the Japan Network Enabler (JPNE) standards.
Manufacturer Code	From the list of manufacturer codes assigned to Juniper Networks, select a manufacturer code to be associated with the OpCo user. If a tenant belonging to the OpCo enables MAP-E for a branch site with NFX150 as the CPE device, the device uses this manufacturer code to obtain the MAP-E rules from the MAP-E rule server.

RELATED DOCUMENTATION

Operating Companies Overview | 108
About the Operating Companies Page | 115
Editing and Deleting Operating Companies | 119

Editing and Deleting Operating Companies

IN THIS SECTION

Editing Operating Companies | 119
Deleting Operating Companies | 120

You can edit and delete operating companies from the Operating Companies (OpCos) page. This topic has the following sections:

Editing Operating Companies

To modify the parameters of an operating company.

NOTE: You cannot modify the operating company name.

1. Select **Tenants > Operating Companies**.

   The Operating Companies (OpCos) page appears, displaying the details of the available operating companies.

2. Select the operating company name that you want to edit and click the edit icon (represented by the pencil graphic on the page).

   The Edit Operating Company(OpCo) page appears.

3. Modify the admin and tenant portal URLs as needed.

4. Click **OK** to save your changes.

   A confirmation message appears, indicating the status of the edit operation.

Deleting Operating Companies

To delete an operating company:

> **NOTE:** You cannot delete an OpCo if any tenant is associated with an OpCo.

1. Select **Tenants > Operating Companies**.

   The Operating Companies (OpCos) page appears, displaying the details of the available operating companies.

2. Select the operating company that you want to delete and then click the delete icon (X) from the top right corner of the page.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected operating company.

   A confirmation message appears, indicating the status of the delete operation. If you do not want to delete, click **Cancel** instead.

RELATED DOCUMENTATION

About the Operating Companies Page | 115

Creating Operating Companies | 116

6
CHAPTER

Managing Resources

About the POPs Page | **124**

Creating a Single POP | **125**

Importing Data for Multiple POPs | **127**

Viewing the History of POP Data Imports | **131**

Viewing the History of POP Data Deletions | **133**

View the History of Device Data Deletions | **135**

Manually Importing Provider Hub Sites | **137**

About the Tenant Devices Page | **138**

About the Provider Hub Devices Page | **140**

Add a Provider Hub Device | **144**

Edit Provider Hub Site Parameters | **153**

Manage a Provider Hub Device | **156**

Upgrade a Provider Hub Device | **158**

Delete a Provider Hub Site | **159**

Perform Return Material Authorization (RMA) for a Provider Hub Device | **160**

Grant Return Material Authorization (RMA) for a Provider Hub Device | **162**

Generate Device RSI for Provider Hub Devices | **164**

Managing a Tenant Device | **165**

Device Redundancy Support Overview | **167**

Viewing the History of Tenant Device Activation Logs | **170**

Secure OAM Network Overview | **172**

Secure OAM Network Redundancy Overview | **174**

Rebooting Tenant Devices and Provider Hub Devices | **178**

Identifying Connectivity Issues by Using Ping | **180**

Identifying Connectivity Issues by Using Traceroute | **184**

Remotely Accessing a Device CLI | **186**

Device Template Overview | **188**

Multi-Service Shared Bearer Overview | **192**

About the Device Template Page | **194**

Cloning a Device Template | **199**

Importing a Device Template | **200**

Configuring Template Settings in a Device Template | **202**

Updating Stage-2 Configuration Template in a Device Template | **224**

Configuring Stage-2 Initial Configuration in a Device Template | **229**

Modifying a Device Template Description | **232**

Deleting a Device Template | **232**

Configuration Templates Overview | **233**

Configuration Templates Workflow | **234**

About the Configuration Templates Page | **236**

Predefined Configuration Templates | **239**

Edit, Clone, and Delete Configuration Templates | **243**

Deploy Configuration Templates to Devices | **246**

Undeploy a Configuration Template from a Device | **251**

Dissociate a Configuration Template from a Device | **253**

Preview and Render Configuration Templates | **254**

Import Configuration Templates | **255**

Export a Configuration Template | **257**

Assign Configuration Templates to Device Templates | **258**

Add Configuration Templates | **261**

Jinja Syntax and Examples for Configuration Templates | **271**

View the Configuration Deployed on Devices | **283**

APN Overview | **285**

Configuring APN Settings on CPE Devices | **286**

Device Images Overview | **289**

About the Device Images Page | **290**

Staging an Image | **292**

Deploying Device Images to Devices | **294**

Uploading a Device Image | **296**

Deleting Device Images | **298**

Network Services Overview | **299**

About the Network Services Page | **300**

About the Service Overview Page | **302**

About the Service Instances Page | **304**

Allocating a Service to Tenants | **305**

Removing a Service from Tenants | **306**

About the POPs Page

To access this page, select **Resources > POPs**.

Use the POPs page to view the list of available POPs in your network . You can also view and manage each POP in your network.

Tasks You Can Perform

- View details of a POP. Hover over the POP name and click the Detailed View icon or click **More > Detail View**.

  The Detail pane for the selected POP appears on the right side of the POPs page, displaying information such as the sites connected to the POPs and alarms on the POP.

  Click the close icon (X) to close the pane.

- Show or hide columns that contain details of the POP. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.

- Search for a POP. Click the Search icon in the top right corner of the page to search for a POP.

  You can enter partial text or full text of the keyword in the text box and press Enter.

  The search results are displayed on the same page.

- Create a POP. See “Creating a Single POP” on page 125.

- Import data for multiple POPs. See “Importing Data for Multiple POPs” on page 127.

- View the history of POP data imports. See “Viewing the History of POP Data Imports” on page 131.

- View the history of POP data deletions. See “Viewing the History of POP Data Deletions” on page 133.

- Delete a POP. Click the Delete icon (trash can) to delete a POP.

- Manage resources for a POP. Click a POP from the list of available POPs.

  The<*Pop-name* > page appears. You can view and manage resources for the POP from the tabs that appear.

> **NOTE:** From CSO Release 5.0.0 onward, virtualized infrastructure manager (VIM) and element management system (EMS) are not supported as resources for POPs.

Field Descriptions

Table 35 on page 125 describes the fields on the POPs page.

Table 35: Fields on the POPs Page

Field	Description
Name	Name of the POP. Example: AWS
Location	Location of the POP. Example: Sunnyvale, CA
Routers	Number of routers provisioned in the POP. Example: 1
Tenants	List of tenants in the POP. Example: Softbank, ATT, and Juniper
Sites	Number of tenant sites in the POP. Example: 4
Region	Region selected to manage services in the POP. Example: Regional (default)

RELATED DOCUMENTATION

Creating a Single POP | 125

Creating a Single POP

IN THIS SECTION

- Adding Information About the POP | 126

You can use the POPs page to create a network point of presence (POP) and its associated resources.

Creating a single POP involves adding several types of objects. The sections in this topic describe how to add each type of object to a POP in Administration Portal. You must finish the steps in each section to create the objects that you need for a single POP and to save the POP successfully.

Adding Information About the POP

To add a single POP and to add basic information to the POP:

1. Click **Resources > POPs**.

   The POPs page appears.

2. Click the plus icon (+) .

   The Add POP page appears.

3. Complete the configuration settings according to the guidelines provided in Table 36 on page 126.

4. (Optional) Click **Download as JSON** to save a JSON file of the POP configuration settings that you configured.

5. Click **OK** to save the POP configuration. If you want to discard your changes, click **Cancel** instead.

   A confirmation message appears at the top of the page indicating that the job was created. You can click the link in the message to view the details of the job.

Table 36: Fields on the Add POP page

Field	Description
Region	Regions are used to group services for various business reasons such as location, proximity, service distribution and load. The default region is selected and cannot be modified. Example: regional **NOTE:** The administrator must not delete the region name.
Name	Enter the name of the POP. You can use an unlimited number of alphanumeric characters, including special characters. Example: north-east.

Table 36: Fields on the Add POP page *(continued)*

Field	Description
Street Address	Enter the street address. You can use an unlimited number of alphanumeric characters, including special characters. Example: 1133 Innovation Way
City	Enter the name of the city. You can use an unlimited number of alphanumeric characters, including special characters. Example: Sunnyvale
State/Province	Enter the name of the state. You can use an unlimited number of alphanumeric characters, including special characters. Example: California
ZIP/Postal Code	Enter the zip code or postal code for the country. You can use an unlimited number of alphanumeric characters, including special characters. Example: 94089
Country	Select the name of the country. Example: USA

RELATED DOCUMENTATION

About the POPs Page | **124**

About the Routers Page

Importing Data for Multiple POPs

IN THIS SECTION

Customizing a POP Data File | **128**

Uploading a POP Data File | **130**

You can use the Import POPs page to import a POP and its associated resources, such as a provider edge device for the POP, a virtualized infrastructure manager (VIM), a container for management network for the VIM, and an element management system (EMS).

Customizing a POP Data File

To customize a POP data file:

1. Select **Resources > POPs**.
2. Click **Import POPs > Import**.

   The Import POPs page appears.
3. Click the **Download Sample JSON** link to open and save the sample JSON data file.

   The sample file opens at the bottom of the page.
4. Save the file to your computer with an appropriate name.

   Example: sample-pop-data.json

   NOTE: You need to retain the file format as .json to successfully upload the POP details to the Administration Portal.
5. Customize the sample JSON file using the guidelines in Table 37 on page 128.
6. Save the customized file.

Table 37: Fields on the POPs Page

Field	Description
POP Information	
dc_name	Specify the name of the region for this POP. Example: regional **NOTE:** Administrator should not delete the region name.

Table 37: Fields on the POPs Page *(continued)*

Field	Description
name	Specify the name of the POP. You can use an unlimited number of alphanumeric characters, including special characters. Example: pne-pop10
street	Specify the street address. Example: 1133 Innovation Way
city	Specify the name of the city. Example: Sunnyvale.
state	Specify the name of the state. Example: CA
zip_code	Specify the zip code or postal code for the state. Example: 94089.
country	Specify the name of the country. Example: USA
Device Information	
name	Specify the name of the device. You can use any number of alphanumeric characters, including special characters. Example: pnf-import123
device_ip	Specify the management IP address of the device. Example: 192.0.2.15.
pne_package	Specify the name of the package providing metadata and configuration templates needed to program a PNE device for service chain attachments in the case of a vCSO solution. You must specify the PNE package only for a data center gateway device. Do not use the SRX Series package for the PE router or the SDN gateway.
assigned_device_profile	Select the name of the configuration image for the SDN gateway or the PE router.

Table 37: Fields on the POPs Page *(continued)*

Field	Description
username	Specify the username of the device administrator for logging into the device. Example: root
password	Specify the password for logging into the device. Example: pwd123

Uploading a POP Data File

You can use the Administration Portal to import POP data to support tenant services.

To upload a POP data file:

1. Select **Resources > POPs**.
2. Click **Import POPs > Import**.

   The Import POPs page appears.
3. Click **Browse** and navigate to the directory containing the POP data file.
4. Select the file and click **Open**.
5. Click **Import**. If you want to discard the import process, click **Cancel** instead.

   A success message is displayed indicating that the job was uploaded successfully.

SEE ALSO

Creating a Single POP | 125

Viewing the History of POP Data Imports | 131

Viewing the History of POP Data Deletions | 133

Viewing the History of POP Data Imports

You can use the Import History page to view the imported POP data. You can also view the details of the imported logs and their status.

To import your POP data, see “Importing Data for Multiple POPs” on page 127.

To view the history of imported POP data:

1. Click **Resources > POPs > Import POPs > Import History**.

   The Import History page is displayed. Table 38 on page 131 describes the fields on the Import History page.

2. Click a task name.

   The Import POPs Tasks page appears. Table 39 on page 132 describes the fields on the Import Task page.

3. Click the Task ID.

   The Job Status page appears. Table 40 on page 132 describes the fields on the Job Status page.

4. Click **OK** to return to the previous page.

Table 38: Fields on the Import History Page

Field	Description
In progress	View the number of import tasks that are in progress.
Success	View the number of import tasks that are successful.
Failure	View the number of import tasks that have failed.
Name	View the name of the task. Example: import_pop_csp.topology_service.import_pop_28c93be6325f4e87a440be096c7e4b58
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.

Table 38: Fields on the Import History Page *(continued)*

Field	Description
Status	View the status of the task to know whether the task succeeded or failed.
Log	View the import logs. Click a log to access more detailed information about the imported log.

Table 39: Fields on the Import POPs Tasks Page

Field	Description
Task ID	View the ID created for the task.
Status	View the status of the task to know whether the task succeeded or failed.

Table 40: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who imported the task.
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

RELATED DOCUMENTATION

Importing Data for Multiple POPs | 127

Viewing the History of POP Data Deletions | 133

Viewing the History of POP Data Deletions

You can use the Delete History page to view the deleted POP data, status of the delete operation, and log details.

To view the history of deleted POP data:

1. Click **Resources > POPs > Import POPs > Delete History**.

   The Delete History page is displayed. Table 41 on page 133 describes the fields on the Delete History page.

2. Click a task name.

   The Delete POPs Tasks page appears. Table 42 on page 134 describes the fields on the Delete Task page.

3. Click the Task ID.

   The Job Status page appears. Table 43 on page 134 describes the fields on the Job Status page.

4. Click **OK** to return to the previous page.

Table 41: Fields on the Delete History Page

Field	Description
Name	View the name of the task.
In progress	View the number of delete tasks that are in progress.
Success	View the number of delete tasks that are successful.
Failure	View the number of delete tasks that have failed.
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.
Status	View the status of the task to know whether the task is succeeded or failed.
Log	View the import logs. Click on a log to access more detailed information about the deleted log.

Table 42: Fields on the Delete POPs Tasks Page

Field	Description
Success	View the number of times the delete operations has been successful for a POP.
Failure	View the number of times the delete operations has failed for a POP.
Task ID	View the ID created for the task. Click on the task ID to view the delete log details corresponding to a POP.
Status	View the status of the task to know whether the task succeeded or failed.

Table 43: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who deleted the task.
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

RELATED DOCUMENTATION

Importing Data for Multiple POPs | 127

Viewing the History of POP Data Imports | 131

View the History of Device Data Deletions

You can use the Delete History page to view the deleted device data, status of the delete operation, and log details.

NOTE: This topic is applicable only to users with the SP Administrator role.

To view the history of deleted device data:

1. Click **Resources > POPs > *POP Name* > Routers > More > Delete History**.

   The Delete History page is displayed. Table 44 on page 135 describes the fields on the Delete History page.

2. Click a task name.

   The Delete Device Tasks page appears. Table 45 on page 136 describes the fields on the Delete Task page.

3. Click the Task ID.

   The Job Status page appears. Table 46 on page 136 describes the fields on the Job Status page.

4. Click **OK** to return to the previous page.

Table 44: Fields on the Delete History Page

Field	Description
Name	View the name of the task.
In progress	View the number of delete tasks that are in progress.
Success	View the number of delete tasks that are successful.
Failure	View the number of delete tasks that have failed.
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.
Status	View the status of the task to know whether the task succeeded or failed.

Table 44: Fields on the Delete History Page *(continued)*

Field	Description
Log	View the import logs. Click a log to access more detailed information about the deleted log.

Table 45: Fields on the Delete Device Tasks Page

Field	Description
Success	View the number of times the delete operations succeeded for a device.
Failure	View the number of times the delete operations failed for a device.
Task ID	View the ID created for the task. Click the task ID to view the delete log details corresponding to a device.
Status	View the status of the task to know whether the task succeeded or failed.

Table 46: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who deleted the task.
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

RELATED DOCUMENTATION

Creating Devices

Configuring Devices

Manually Importing Provider Hub Sites

A provider hub site represents an automation endpoint that is part of a data center or POP that is owned by the service provider. The provider hub site is connected to multiple spoke sites using the overlay connections. Provider hubs sites are logical entities in a multi-tenant device (provider hub device). Users with the OpCo Administrator role can add a provider hub site from the **Sites** page.

To manually import a provider hub site:

1. Select **Resources > Site Management**.

   The Sites page appears.

2. Click **Add** and select **Add Provider Hub**.

   The **Add Provider Hub for *OpCo-Name*** page appears.

3. Complete the configuration settings according to the guidelines provided in Table 47 on page 137.

   NOTE: Fields marked with * are mandatory.

4. Click **OK**.

   The newly created provider hub site is displayed on the **Sites** page.

Table 47: Fields on the Add Provider Hub for OpCo-Name Page

Field	Description
Configuration	
Service POP	Select the name of the point of presence (POP) for the site. A network POP is a location at which a service provider instantiates a network function, such as a virtualized network function (VNF).
Hub Device Name	Select the provider hub device for the OpCo.

RELATED DOCUMENTATION

About the Sites Page

About the Tenant Devices Page

To access this page, click **Resources > Tenant Devices**.

You can use the Tenant Devices page to view the list of available CPE devices in the OpCo network. You can also view information about each CPE device in the network.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the history of tenant device activation logs. See "Viewing the History of Tenant Device Activation Logs" on page 170.
- Reboot a CPE device. See "Rebooting Tenant Devices and Provider Hub Devices" on page 178.
- Push licenses to devices. Select the devices and click **Push License**.

  The Push License page appears displaying the list of licenses uploaded in CSO. Select the license(s) which you want to push to the selected devices. Click **Push Licenses** to push the licenses to the selected devices. To cancel the action, click **Cancel**.

  See "Pushing a License to Devices" on page 386.
- View Stage-1 configuration. Click **Resources > Tenant Devices > *Device-Name* > Stage 1 Config** to view the stage-1 configuration for the device.
- View the device audit logs. Click **Resources > Tenant Devices > *Device-Name* > Device Audit Logs** to view the audit logs for the device.
- View details about a CPE device. Click the details icon that appears when you hover over the name of a device or click **More > Details**.
- Deleting a CPE—Select the CPE device that you want to delete and click the delete icon.
- Show or hide columns about the CPE—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a CPE device—Click the Search icon in the top right corner of the page to search for a CPE device. You can enter partial text or full text of the keyword in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

Table 48 on page 139 describes the fields on the Tenant Devices page.

Table 48: Fields on the Tenant Devices Page

Field	Description
Device Name	Displays the name of the device. Example: sunny-NFX-250
Tenant	Displays the name of the tenant. Example: tenant-blue
Site Name	Displays the name of the tenant site. Example: site-blue-white
Location	Displays the name of the location. Example: San Jose, CA
Status Message	Displays the latest status message. Example: IPsec provision success
WAN Links	Displays the number of WAN links. Example: 2
POP Name	Displays the name of the POP. Example: pop_blue
Management Status	Displays the management status of the CPE devices deployed in the cloud. • Expected—Regional server has activation details for the CPE device, but CPE device has not yet established a connection with the server. • Active—CPE device has downloaded images, but is not yet configured. • Provisioned—IPsec tunnel on NFX250 device is operational. • Provision Failed—CPE device failed when the vSRX was not instantiated properly.

Table 48: Fields on the Tenant Devices Page ***(continued)***

Field	Description
Model	Displays the name of the device model. Example: NFX
Active Services	Displays the number of services that are activated for the device. Example: 3
Image Name	Displays the name of the device image file. Example: install_nfx_fmpm_agent_1_0.sh
OS Version	Displays the Junos OS Release version. Example: 15.1X49-D40
Serial Number	Displays the serial number of the device. Example: DD0416AA0117

RELATED DOCUMENTATION

Viewing the History of Tenant Device Activation Logs | 170

About the Provider Hub Devices Page

To access this page, select **Resources > Provider Hub Devices**.

Use the Provider Hub Devices page to view the list of provider hub devices that are owned by the administrator in the OpCo network. You can add or delete a provider hub with DATA_ONLY capability. You can also view detailed information about each provider hub device in the network.

CSO uses the provider hub devices as SD-WAN hubs to setup tunnels and provision site-to-site or site-to-hub traffic. All other configurations such as Internet breakout, hub meshing, and so on must be configured manually on the device.

Tasks You Can Perform

You can perform the following tasks from the Provider Hub Devices page:

- Add a provider hub device with DATA_ONLY capability. See “Add a Provider Hub Device” on page 144.
- View details of a provider hub device—Hover over the device name and click the Detailed View icon or click **More > Detail View**.

  The Detailed View pane appears on the right side of the Provider Hub Devices page, displaying information (such as hardware and software) about the provider hub device.

  Click the close icon (X) to close the pane.
- Edit provider hub site parameters. See “Edit Provider Hub Site Parameters” on page 153.
- Upgrade the provider hub device. See “Upgrade a Provider Hub Device” on page 158.
- Perform Return Material Authorization (RMA) to replace a device that is faulty or not reachable. From Administration Portal, you can perform RMA for provider hub devices. See “Perform Return Material Authorization (RMA) for a Provider Hub Device” on page 160 for details.
- Delete a provider hub device with DATA_ONLY capability—Select the hub device that you want to delete and click the delete icon.
- Show or hide columns that contain details of the provider hub device—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a provider hub device—Click the Search icon in the top right corner of the page to search for a particular provider hub device.

  You can enter partial text or full text of the keyword in the text box and press Enter.

  The search results are displayed on the same page.
- Filter the available devices on the page based on the specified criteria—Select the filter icon at the top right corner of the table to apply a filter. For example, you can filter information based on the management status or site name. The table displays only the data that fits the filtering criteria.

  Click the Clear All icon to remove the applied filter.

Field Descriptions

- Table 49 on page 142 describes the fields on the Provider Hub Devices page.

Table 49: Fields on the Provider Hub Devices Page

Field	Description
Device Name	Name of a provider hub device. Example: srx-provider-hub
Tenant	Name of the tenant. Example: tenant-blue
Site Name	Name of the tenant site. Example: site-blue-white
Location	Name of the location. Example: San Jose, CA
Status Message	Latest status message. Example: IPsec provision success
WAN Links	Number of WAN links for a device. Example: 2
POP Name	Name of the POP. Example: pop_blue
Capabilities	Type of capability configured for the provider hub device. Example: OAM

Table 49: Fields on the Provider Hub Devices Page *(continued)*

Field	Description
Management Status	Management status of the provider hub devices deployed in the cloud: • **Expected**—The regional server has activation details for the device, but the device has not yet established a connection with the server. Click **Activate** to activate the provider hub device. If the activation process is successful, then the management status changes to **Provisioned**. • **Active**—Provider hub device is yet to be configured. • **Provisioned**—Provider hub device is ready to be used. • **Provision** Failed—Provider hub device is not yet ready to be used.
Authentication Type	Authentication method used for the device—Preshared Key (PSK) or Public Key Infrastructure (PKI).
Version	CSO version in which the provider hub device was added.
Model	Name of the device model. Example: SRX
OS Version	Junos OS Release version. Example: 15.1X49-D40
Serial Number	Serial number of the device. Example: DD0416AA0117

RELATED DOCUMENTATION

About the Tenant Devices Page | 138

Add a Provider Hub Device

Users with the SP (service provider) Administrator role or an OpCo (operating company) Administrator role can add provider hub devices with different capabilities as indicated in Table 50 on page 144.

Table 50: Provider Hub Capabilities and Roles

Capability	Description	Added By (Role)
OAM_ONLY	Transmits only OAM traffic. IPsec OAM tunnels are configured between a spoke site and the provider hub.	SP Administrator
DATA_ONLY	Transmits only data traffic. IPsec data tunnels are configured between a spoke site and the provider hub with data capability. IPsec OAM tunnels are not configured between the spoke site and the provider hub.	SP Administrator OpCo Administrator
OAM AND DATA	Transmits both data and OAM traffic. Both IPsec OAM and data tunnels are configured between a spoke site and the provider hub.	SP Administrator OpCo Administrator

You can add an SRX Series services gateway or a vSRX instance as a provider hub with DATA_ONLY capability in a hub-and-spoke topology or full mesh topology.

> **NOTE:** Because specifying a POP is mandatory for adding a provider hub, the SP Administrator or OpCo Administrator must add a POP. For more information, see "Creating a Single POP" on page 125.

In SD-WAN deployments, there is a provision to add a provider hub and activate it later. While the provider hub can be added by an SP or an OpCo administrator, it can be activated by another SP or OpCo administrator. The second user must enter either the serial number and the activation code, or only the serial number when manually activating the device later.

To add a provider hub device:

1. Select **Resources > Provider Hub Devices**.

   The Provider Hub Devices page appears.

2. Click the add icon **(+)**.

   The Add Provider Hub Device page appears.

3. Complete the configuration according to the guidelines provided in Table 51 on page 146.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. (Optional) Review the configuration in the Summary tab and modify the settings, if required.

5. Click **OK**.

   - If you entered a serial number during activation and automatic activation is enabled, the Site Activation Progress page appears. The site activation process proceeds through the tasks explained in *Troubleshooting Site Activation Issues*.

     Click **OK** to close the Site Activation Progress page.

   - If you did not enter a serial number and the automatic activation is disabled, you are returned to the Provider Hub Devices page. CSO triggers a job and displays a confirmation message with a job link. Click the link to view the status of the job. After the job is finished, CSO displays a confirmation message with a job link. The status of the site changes to CREATED.

     You must manually activate the device to finish the activation process.

     NOTE: The following procedure is applicable if zero touch provisioning (ZTP) is set true in the device template. If ZTP is disabled in the device template, you must copy the stage-1 configuration and commit it on the device for CSO to proceed with the activation.

     To manually activate the provider hub:

     a. Select the provider hub device that has to be activated.

     b. Click **Activate Device** button in the Provider Hub Devices page.

        The **Activate Site** page appears.

     c. Enter the serial number(s) of the device and the activation code. Click **OK**.

        The **Site Activation Progress** page appears displaying the progress of steps executed for activating the provider hub. On successful activation of the device, the Site Status changes from **Created** to **Provisioned**.

After the device is successfully activated, you can start using the provider hub in your network.

Table 51: Fields on the Add Provider Hub Device Page

Field	Description
Site Name	Enter the name of the provider hub device. You can use alphanumeric characters, including special character(-). The maximum length is 32 characters. Example: provider-hub-1
Device Host Name	The device host name is auto-generated and uses the format *tenant-name.host-name*. You cannot change the *tenant-name* part in the device host name. Use alphanumeric characters and hyphen (-); the maximum length allowed is 32 characters.
Management Region	Displays the regional server with which the device communicates. The management region name is populated based on the information from the device template. Example: regional
POP	Select the POP where the hub device needs to be added. Example: pop_blue
Site Capability	Select the site capability of the provider hub device: • **OAM_ONLY** (Available only for SP Administrator users) • **DATA_ONLY** • **OAM AND DATA** CSO establishes a secure OAM tunnel between the provider hub with DATA_ONLY capability and a provider hub with OAM_ONLY or OAM AND DATA capability).
Authentication Type	Select the IPsec tunnel authentication method—Preshared Key (PSK) or Public Key Infrastructure (PKI).
Advanced Configuration	

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
Domain Name Server	Specify one or more IPv4 or IPv6, or both IPv4 and IPv6 addresses of the DNS server. To specify more than one DNS server address, type the address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone of the site.
Click **Next** to continue.	
Device Template	
Device Template	The device template that is currently supported for provider hub devices is SRX as SD-WAN Hub. Based on the device series that you select, the supported device templates (containing information for configuring devices) are listed. Select a device template.
Device Information	
Serial Number	Enter the serial number of the provider hub device. Serial numbers are case-sensitive. If you do not enter the serial number, the provider hub is added but not activated. See "Step-by-Step Procedure" on page 145 to manually activate the provider hub later.
Auto Activate	Click the toggle button to enable or disable automatic activation of the provider hub device. The device template that you select determines whether this option is enabled or disabled by default.

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
Device Root Password	The default root password is fetched from the ENC_ROOT_PASSWORD field in the services template. You can retain the password or change it by entering a password in plain-text format. The password is encrypted and stored on the device.
Activation Code	If you disabled automatic activation, enter the activation code used while adding the site to manually activate the device. See "Step-by-Step Procedure" on page 145 to manually activate the device later. The activation code is an authentication code created when adding the device and shared with the user who later activates the provider hub device. This is to ensure that only an authorized user activates a provider hub that was added earlier.
Boot image	Select the boot image from the drop-down list if you want to upgrade the image for the provider hub device. The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when CSO starts the ZTP process. If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while creating a site.
Management Connectivity	The fields in this section are displayed based on the capability that you select for the provider hub device.
Loopback IP Prefix	By default, CSO assigns the IPv4 address prefix for the loopback interface on the device. If you prefer to use a specific loopback address, you can enter an IPv4 address prefix for the loopback interface on the provider hub device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network.

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
OAM Interface	Select an interface on the provider hub device to connect to the CSO. The interface is used only for OAM connectivity. The interface names are listed based on the configuration in the selected device template.
OAM VLAN	Enter an OAM VLAN ID for in-band management of the hub device. If you specify an OAM VLAN ID, then in-band OAM traffic reaches the device through the selected OAM interface.
OAM IP Prefix	Enter an IPv4 address prefix for the OAM interface in the provider hub device. The prefix must be unique across the entire management network.
OAM Gateway	Enter the IP address of the next-hop through which the connectivity to CSO is established.
EBGP Peer AS	Enter the autonomous system (AS) number of the external BGP (EBGP) peer.
WAN Links	
WAN_0 *WAN-Interface-Name*	This field is enabled by default. Enter parameters related to WAN_0. Fields marked with an asterisk (*) must be configured to proceed.
Local Interface	Displays the interface name configured in the device template. You cannot modify this field.
Link Type	Select the underlay network type (MPLS or Internet) of the WAN link.
Public IP Address	For Internet links, enter the public IPv4 address for the link. This IP address should be provided only if the static IP prefix is private and 1:1 NAT is configured.
VLAN ID	Enter the VLAN ID that is associated with the data link.

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
Underlay Address Families	
IPv4	Click the toggle button to enable or disable IPv4 address assignment for the WAN link. By default, IPv4 address assignment is enabled for the WAN link. The WAN link requires an IPv4 address to connect to an IPv4 network.
Address Assignment Method	Displays the address assignment method used for the WAN link (STATIC). You cannot modify this field.
Static IP Prefix	Enter the IPv4 address prefix of the WAN link.
Gateway IP Address	Enter the gateway IPv4 address of the default route.
IPv6	Click the toggle button to enable or disable IPv6 address assignment for the WAN link. By default, IPv6 address assignment is disabled for the WAN link. The WAN link requires an IPv6 address to connect to an IPv6 network.
Address Assignment Method	Displays the address assignment method used for the WAN link (STATIC). You cannot modify this field.
Static IP Prefix	Enter the IPv6 address prefix of the WAN link.
Gateway IP Address	Enter the gateway IPv6 address of the default route.
WAN_1 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for WAN_0 *WAN-Interface-Name* for an explanation of the fields.

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
WAN_2 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for WAN_0 *WAN-Interface-Name* for an explanation of the fields
WAN_3 WAN-Interface-Name	Click the toggle button to enable or disable the WAN link. When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for WAN_0 *WAN-Interface-Name* for an explanation of the fields
Click **Next** to continue.	
Configuration Templates (Optional)	

Table 51: Fields on the Add Provider Hub Device Page *(continued)*

Field	Description
Configuration Templates List	Select one or more configuration templates from the list. This list is filtered based on the device that you select. Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators. **NOTE:** You must set the parameters of the configuration templates that you have selected before you move to the LAN section. To set the parameters for the selected configuration templates: 1. After you select one or more configuration templates, click **Set Parameters**. The **Device Configurations** page appears. This page consists of two tabs—Configure and Summary 2. In the Configure tab fill in the attributes for each of the configuration templates. (Optional) View the CLI commands in the Summary tab. 3. Click **Save**. You have added and set the parameters for the configuration templates that are part of the site template that you are creating.

RELATED DOCUMENTATION

About the Provider Hub Devices Page | 140

Edit Provider Hub Site Parameters

The Edit Provider Hub page enables the Service Provider (SP) or Operating Company (OpCo) Administrator users to modify the parameters of a provider hub site with DATA_ONLY capability and the following management status:

- Configuration-Failed
- Partially-Provisioned
- Provisioned

> **NOTE:**
> - You cannot edit provider hub sites with OAM_ONLY or OAM_AND_DATA capability because such modifications can impact the connectivity of the entire network.
> - To edit a provisioned or a partially-provisioned provider hub site, the Operational Status must be UP.
> - SP and OpCo Administrator users can only edit the parameters of provider hub sites that they added.

You can add or delete WAN links, or modify the site parameters without affecting the connectivity between the provider hub site and Contrail Service Orchestration (CSO).

When a WAN link is added to a provider hub site, CSO creates secure OAM tunnels and enables the monitoring of the new WAN link.

> **NOTE:** Before you delete a WAN link on a provider hub site, ensure that:
> - At least one Operations, Administration, and Maintenance (OAM) WAN link is enabled for the site.
> - There are no spoke or enterprise hub sites connected to the WAN link.

When you delete a WAN link from the provider hub site, the associated secure OAM tunnels are also deleted.

What should you do if adding or deleting a WAN link fails?

When the addition or deletion of a WAN link fails, PARTIALLY DEPLOYED is displayed next to the WAN link name.

You can do one of the following:

- Retry the specific edit site job to execute the failed tasks from the Jobs page (**Monitor** > **Jobs**). For more information, see *Retrying a Failed Job on Devices*.
- Redeploy the WAN link by clicking the **Re-Deploy WAN Link** toggle button and updating the WAN link parameters, which first deletes the WAN link and then adds it again.
- Leave the WAN link as is and redeploy the WAN link later.

To edit the parameters configured for a provider hub site:

1. Select **Resources > Provider Hub Devices**.

   The Provider Hub Devices page appears.

2. Select the provider hub site whose parameters you want to modify and click the **Edit** icon (pencil).

   The Edit Provider Hub page appears.

3. Modify the provider hub site parameters as described in Table 52 on page 155.

4. (Optional) Review the configuration in the Summary tab and modify the settings, if required.

5. Do one of the following:
   - Click **Finish** to save the changes that you made to the provider hub site.
   - Click **Previous** to make changes in the previous page.
   - Click **Cancel** to discard the changes. A dialog box appears asking for your confirmation. Click **Yes**. The changes you made are lost and you are returned to the Provider Hub Devices page.

   If you click Finish, an Edit Site job is triggered and a job link appears on the Provider Hub Devices page.

   You can click the job link to view details of the job (including job status, start date and time, and end date and time). Alternatively, you can view the status of the job on the Jobs page.

   After the job completes successfully, a confirmation message appears on top of the Provider Hub Devices page.

   NOTE: The following operations take several minutes (greater than 15 minutes) based on the number of sites connected to the provider hub:

   - Deleting a WAN link.
   - Editing the Link Type, Address Assignment Method, or VLAN ID of a WAN link.
   - Re-deploying a partially deployed WAN link.

Table 52: Editable Fields for a Provider Hub Site

Editable Parameters	Description
General **NOTE:** • To edit the WAN parameters of a provider hub site, ensure that the site version is 5.3.0 or higher. If the site version is of an earlier release, you must upgrade the site. For more information, see "Upgrade a Provider Hub Device" on page 158. • For provider hub sites with 5.2.0 or earlier site versions, only advanced configuration fields are editable. You can find the version of a provider hub site in the Version column on the Provider Hub Devices page.	
Site Name	Edit the name of the site. You can only use alphanumeric numbers and hyphen. The site name must be unique and name length must not exceed 32 characters.
Device Host Name	Edit the device host name for the site. You can only use alphanumeric numbers and hyphen. The device host name must be unique and name length must not exceed 32 characters. Format: *<tenant_name>.<site_name>*. For example, TenantA.Orange. **NOTE:** The tenant name is always added as a prefix for the device host name. The tenant name part in the device host name cannot be edited.
Advanced Configuration	Edit the Domain Name Server (DNS) IP address (IPv4 or IPv6, or both), NTP Server IP address, and the selected Timezone.
WAN You can do one of the following: • Edit the WAN parameters (specified below) of an existing WAN link. • Add a new WAN link by clicking the toggle button next to the WAN link name and specifying the WAN parameters. For more information on WAN link parameters, see Table 51 on page 146. • Delete an existing WAN link by clicking the enabled toggle button next to the WAN link name.	
Re-Deploy WAN Link	For partially deployed WAN links, click the toggle button to enable editing the WAN parameters.
Link Type	Edit the link type by selecting **MPLS** or **Internet**.

Table 52: Editable Fields for a Provider Hub Site *(continued)*

Editable Parameters	Description
Address Assignment	STATIC is the only option for assigning an IP address to the WAN link. You can edit the **Static IP Prefix** and **Gateway IP** address of the site.
Data VLAN ID	Edit the VLAN ID. Range: 0 through 4049 (4050 to 4094 is reserved by CSO).
Underlay Address Families	Click either IPv4 or IPv6, or both IPv4 and IPv6 toggle buttons to enable either IPv4 or IPv6, or both IPv4 and IPv6 address assignment respectively, for the WAN link. You can also edit the **Static IP Prefix** and **Gateway IP** address for the WAN link.

RELATED DOCUMENTATION

About the Sites Page

About the Provider Hub Devices Page | **140**

Manage a Provider Hub Device

Users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can use the ***Device-Name*** page (**Resources > Provider Hub Devices > *Device-Name***) to view details of and manage a provider hub device.

To manage a provider hub device:

- Click the **Overview** tab to perform the following operations:
  - View the geographical location of the device at the tenant site.
  - View the aggregate throughput of the device.
  - View the recent alerts for the device.
  - View the details of the device, such as serial number, management IP address, OS version, device template, tenant name, site name, and site location.
  - View WAN link throughput over time: Displays a line chart of WAN interface utilization as throughput (in bps) over time for each underlay WAN link. Different color lines represent the input and output rate for each WAN link. You can select them by hovering over the input/output rate list on the right

side of the widget. Every three minutes the bandwidth usage information is collected for each WAN link and the rate is displayed respectively on the graph.

You can view the utilization statistics for a particular time range by selecting any one of the following values from the **Time Span** list:

- Last 15 min
- Last 30 min
- Last 1 hour
- Last 8 hour
- Last 1 day
- Last 1 week
- Last 1 month

> **NOTE:** You must upgrade the site to CSO Release 6.0.0 to view this widget. For more information, "Upgrade a Provider Hub Device" on page 158.

- Click the **Configuration Template** tab to perform the following operations:
  - Save a configuration template, for the device, in the database.
  - Deploy a configuration template to the device.
  - Undeploy a configuration template from the device.

    Undeploying a configuration template removes the configuration pushed to the device when the configuration template was deployed.
  - Dissociate a configuration template from the device.

    Dissociating a configuration template removes only the references to the configuration template from the device but does not remove the configuration pushed to the device.
  - Roll back a configuration template for the device.
  - View the deployment history of the configuration template for the device.

RELATED DOCUMENTATION

About the Provider Hub Devices Page | 140

Upgrade a Provider Hub Device

A provider hub is a multitenant device that can be upgraded by Service Provider (SP) Administrators or Operating Company (OpCo) Administrators. We recommend that you upgrade provider hubs when a new CSO version is released so that, the device functionality can be updated. To find out if an upgrade is required, check the provider hub version (displayed in the **Version** field of the Provider Hub Devices page) against the CSO version (displayed in the About panel that you can access through the Help (?) menu). If the version of a provider hub device is not the same as the CSO version, then the provider hub device needs to be upgraded. Provider hub devices of any version can be upgraded to the latest CSO version.

Users with the Service Provider (SP) Administrator or Operating Company (OpCo) Administrator roles can upgrade provider hub devices that they previously added.

To upgrade a provider hub device:

1. In Administration Portal, select **Resources > Provider Hub Devices**.

   The Provider Hub Device page appears.

2. Select a provider hub device, and click **More > Upgrade**.

   > **NOTE:** You can upgrade only one provider hub device at a time.

   An Upgrade Provider Hub Device: *Device-Name* dialog box appears and CSO analyzes if an upgrade job is required.

3. Click **OK** when the job analysis dialog box shows 100 percent.

   The Upgrade Provider Hub Device: *Device-Name* page appears displaying the following information:

   - Impact of the upgrading the provider hub device, such as upgrade of software image of the physical device (device image), changes in configuration or network services.

     > **NOTE:** When you upgrade provider hub devices in CSO, the Junos OS in the device is also upgraded to the recommended version.

   - Impacted sites in each tenant.
   - Estimated time needed to upgrade the provider hub device.

4. From the **Upgrade Time** field, select one of the following:

   - **Run now** to start the upgrade for the provider hub device immediately.

- **Schedule at a later time** to schedule an upgrade and enter the date and time at which to schedule the upgrade.

5. Click **Upgrade**.

CSO triggers an upgrade job and displays a confirmation message with a job ID link. You are returned to the Provider Hub Devices page. You can click the link in the message to view the details of the job. Alternatively, you can check the status of the job on the Jobs (**Monitor > Jobs**) page.

When the provider hub device is upgraded successfully, the version number of the provider hub device matches the CSO version and the management status is set to **Provisioned**.

Delete a Provider Hub Site

You can delete a provider hub site from the Provider Hub Devices page (**Resources > Provider Hub Devices**) in Administration Portal.

The following are applicable when you want to delete a provider hub:site.

- You can delete only one provider hub at a time.
- You cannot delete a provider hub site that is associated with a cloud or on-premises spoke site. You must first delete the spoke sites associated with the provider hub site and then delete the provider hub site.

To delete a provider hub site:

1. Click **Resources > Provider Hub Devices**.

   The Provider Hub Devices page appears.

2. Select the device that you want to delete and click the delete (trash can) icon.

3. Select one of the following options:

   - **Load Recovery Configuration**—Use this option to back up any custom configuration on the device that is present on the device when you trigger site deletion. CSO restores the custom configuration when you reinstall the device.
   - **Zeorize the device**—Use this option to reset the device to the factory default configuration.

NOTE: When you zeroize the device, you will lose custom configurations on the device.

4. Click **OK**.

   CSO triggers a job to delete the provider hub site. After the job completes successfully, a message appears on top of the Provider Hub Devices page indicating that the provider hub site is deleted.

NOTE:

- The time taken to delete a site is dependant on the device template attached to the site.
- If the delete site operation is unsuccessful, you cannot add a new site that uses the same site name as the site that you attempted to delete.

RELATED DOCUMENTATION

About the Site Management Page

Contrail Service Orchestration Monitoring and Troubleshooting Guide

Perform Return Material Authorization (RMA) for a Provider Hub Device

Sometimes, due to hardware failure, a device managed by Contrail Service Orchestration (CSO) needs to be returned to the vendor for repair or replacement. In such situations, as a Service Provider (SP) Administrator or Operating Company (OpCo) Administrator with the RMA privilege, you can perform Return Material Authorization (RMA) for the faulty device.

The RMA process includes actions to:

1. Back up the configuration of the faulty device.
2. Recall the faulty device and replace it with a new or restored device.
3. Push the required configuration to the new or restored device.
4. Activate the new or restored device in order for CSO to recognize and manage the device.

NOTE:

- When you request RMA for a provider hub device associated with a site that has a version earlier than the CSO version, the site version is not upgraded to the CSO version as part of the device activation and zero touch provisioning (ZTP) process of the replacement device that is performed after RMA.

To perform RMA for a faulty provider hub device:

1. Select **Resources** > **Provider Hub Devices**.

   The **Provider Hub Devices** page appears.

2. Select the faulty device and click **More** > **Initiate RMA**.

   A confirmation page appears requesting for confirmation to initiate the RMA process for the device.

   NOTE:

   - The **Initiate RMA** option is enabled only for a device with the management status **PROVISIONED**.

3. Click **Yes** to confirm RMA for the device.

   You are returned to the Provider Hub Devices page where a confirmation message appears, indicating that the RMA process is initiated.

4. After the management status of the device changes to **RMA**, raise a device replacement request. This process is performed outside of CSO.

5. After you receive the new device, click **More** > **Grant RMA**.

   The Grant RMA for Device page appears. Provide details of the new device on this page. See “Grant Return Material Authorization (RMA) for a Provider Hub Device” on page 162 for details.

   NOTE:

   - The **Grant RMA** option is enabled only for a device with the management status **RMA**.

6. To complete the RMA process and start using the new device, the device must be activated.

   - If you enabled the Auto-activate toggle button on the Grant RMA for Device page, the device is activated automatically and its **Management Status** changes to **PROVISIONED**.

- If you disabled the Auto-activate toggle button on the Grant RMA for Device page, you must manually activate the new device after the grant RMA job completes successfully.

  To manually activate the new device:

  a. On the Provider Hub Devices page, select the new device and click **Activate Device**.

     The Activate Device page appears.

  b. Enter the activation code for the device and click **Next**.

     The progress of device activation is displayed.

     After the device is activated, its **Management Status** changes to **PROVISIONED**.

The RMA process is now complete. You can start using the new device.

RELATED DOCUMENTATION

Grant Return Material Authorization (RMA) for a Provider Hub Device | 162

Grant Return Material Authorization (RMA) for a Provider Hub Device

As a Service Provider (SP) Administrator or Operating Company (OpCo) Administrator with the RMA privilege, you can grant RMA for a device that is in the RMA state.

When you grant RMA, the device-related configuration is backed up to the CSO database, the existing device is recalled, and the new device is added to the network.

Before you grant RMA for a device, ensure that:

- You have received a new device to replace the faulty device.
- You have the serial number and activation code for the new device.

To grant RMA for a provider hub device:

1. Select **Resources** > **Provider Hub Devices**.

   The **Provider Hub Devices** page appears.

2. Select the faulty device for which you initiated RMA and click **More** > **Grant RMA**.

The **Grant RMA for Device** page appears.

> **NOTE:** The **Grant RMA** option is enabled only for a device with the **Management Status RMA**.

3. Complete the configuration according to the guidelines provided in Table 53 on page 163.

4. Click **OK** to perform the grant RMA process.

   You are returned to the Provider Hub Devices page where a confirmation message appears indicating that a Grant RMA job is created.

5. (Optional) Click the job link in the message to view the progress of the job. Alternatively, view the progress of this job on the Jobs (**Monitor** > **Jobs**) page.

   This job might take around 15 minutes to complete.

After the job is completed successfully, the management status of the device on the Devices page changes to **Expected**. In addition, the status of the site on the Sites page (**Resources > Site Management**), where the device for which you performed Grant RMA is installed, changes to **Expected**.

To complete the RMA process and start using the new device, the device must be activated. See step 6 in "Perform Return Material Authorization (RMA) for a Provider Hub Device" on page 160 for details.

Table 53 on page 163 provides information about the fields on the **Grant RMA for Device** page.

Table 53: Fields on the Grant RMA for Device Page

Field	Description
Customer Name	Displays the name of the tenant whose sites are connected to the provider hub.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with a new device through the Grant RMA process.
Auto Activate	Click the toggle button to enable (default) or disable automatic activation of the new device.
Activation Code	If you disabled automatic activation, enter the activation code for the new device. You receive the activation code (Example: 545454) from the service provider, outside of CSO.

Table 53: Fields on the Grant RMA for Device Page *(continued)*

Field	Description
Serial Number	Enter the serial number of the new device. The serial number is case-sensitive. Example: DD2316AF0177
Boot Image	From the list, select the same boot image as the faulty device. If you select a different boot image for the new device, the grant RMA process may not complete successfully.

Generate Device RSI for Provider Hub Devices

Starting from Release 6.0.0, CSO provides the option to generate the RSI (request support information) file for provider hub devices. Before you contact the customer support team, you must generate an RSI file for the device. The RSI file contains system data that can be analyzed to troubleshoot and debug any issue.

Only the SP administrator, OpCo administrator, or tenant administrator can generate the device RSI. Users with custom roles can generate RSI files, if the device RSI action is enabled for that role.

To generate the RSI log, the operational status of the device must be UP.

To collect the device RSI:

1. Select **Resources > Provider Hub Devices**.

   The Provider Hub Devices page appears.

2. Select a device from the list of devices displayed and click **More > Device RSI**. You can generate the device log for only one device at a time.

   An alert message that prompts you to confirm the operation appears.

3. Click **Yes**.

   A message indicating that the request system information job is triggered is displayed. You can click the link in the message to view the progress of the job. Alternatively, you can view the progress on the Jobs (**Monitor >Jobs**) page.

   If the job is completed successfully, a confirmation message appears. This job might take up to 35 minutes to complete depending on the device type.

You can download the log file from the Jobs page. To download the device log, click the **[Download Logs]** link next to the job name. The log file is saved in a compressed (.gz) format with the **rsi_*site-name*_JUNOS** filename. Extract the file to view the details.

> **NOTE:** CSO retains only one version of the log file. Each time you generate a log file, the previous version is overwritten.

Managing a Tenant Device

You can use the Tenant Devices page to view and manage a single customer premises equipment (CPE) device at the tenant site. To access this page, click **Resources > Tenant Devices > *Device-Name***.

You can perform the following operations on the **Overview** tab:

- View the geographical location of the device at the tenant site.
- View the aggregate throughput of the device.
- View the recent alerts for the device.
- View the details of the device, such as serial number, management IP address, OS version, device template, tenant name, site name, site location, operational status, and management status of the device.
- View the recent alarms (critical, major, and minor) for the device.
- View the details of licenses, such as the license name, description, and the time when the license was pushed to the device.

You can perform the following operations on the **Configuration Template** tab:

> **NOTE:** The **Configuration** tab that was available in earlier releases for stage-2 template-based configuration is renamed as **Configuration Template**.

- Save the configuration template for the device.
- Deploy the configuration template for the device.
- Undeploy the configuration template for the device.

  Undeploying a configuration template removes the configuration pushed to the device when the configuration template was deployed.

- Dissociate the configuration template for the device.

  Dissociating a configuration template removes only the references to the configuration template from the device but does not remove the configuration pushed to the device.

- Rollback to the previous configuration template for the device.
- View the deployment history of the configuration template for the device.

You can also perform the following operations on the **Configuration** tab.

- Click **Physical Interfaces** tab to view and manage the physical interfaces for the device.
- Click **Security Zone** tab to view and manage the security zones for the device.
- Click **Routing Instance** tab to view and manage the routing instances for the device.

RELATED DOCUMENTATION

About the Tenant Devices Page | 138

Device Redundancy Support Overview

Contrail Service Orchestration (CSO) supports spoke redundancy for large enterprise SD-WAN branch sites. To protect an SD-WAN site against device or link failures, you can configure the site with two CEP devices that can function as primary and secondary devices. . If the primary device fails, the secondary device takes over the traffic processing.

> **NOTE:** You must use the same device model for both primary and secondary devices and the devices must have the same version of Junos OS installed.

The following SD-WAN features are not supported for device redundancy:

- LTE WAN backup link
- Service chaining

> **NOTE:** Device redundancy is supported only for SD-WAN deployments.

Prerequisites for using SRX Series Devices for Device Redundancy

The prerequisites to configure an SD-WAN site with dual CPE SRX Series devices are as follows:

- For SRX Series, you need to form the cluster manually by connecting two SRX Series devices together using a pair of the same type of Ethernet connections. To create an SRX cluster, see Chassis Cluster Feature Guide for SRX Series Devices.
- Log in to any one of the SRX Series devices, copy the **Stage-1** configuration from the **Sites** page and paste it into the console screen and commit the configuration.

Supported Connection Plans

The following connection plans are supported for device redundancy:

- Dual NFX250 as SD-WAN CPEs—Supports NFX Series devices as CPE devices in an SD-WAN site.
- Dual SRX as SD-WAN CPEs—Supports SRX Series devices as dual CPE devices in an SD-WAN site.

- Dual SRX4x00 as SD-WAN CPEs—Supports SRX 4100 and SRX4200 devices as dual CPE devices in an SD-WAN site.

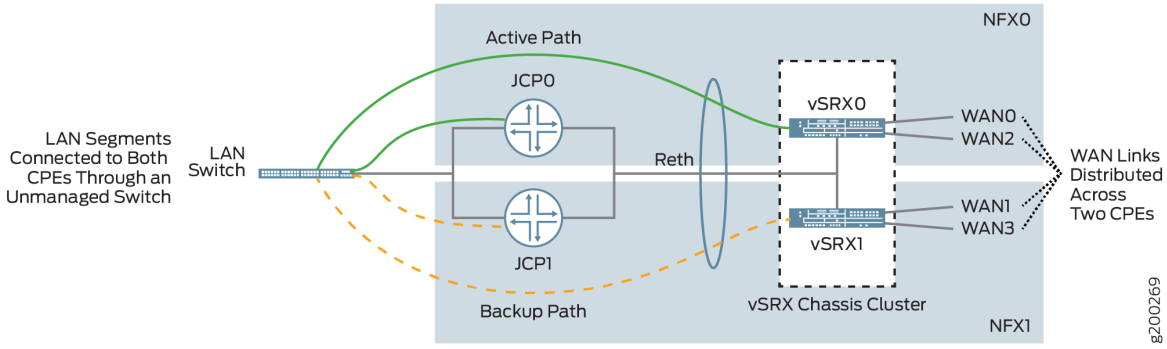
Create and Configure an SD-WAN Site

You can create and configure an SD-WAN site with dual CPE devices and the two devices back up each other, with one node acting as the primary device and the other as the secondary device. The workflow to add and configure a site with dual CPE devices is similar to the single CPE device. For more information about creating and configuring a site with dual CPE devices, see *Add a Branch Site with SD-WAN Capability*, *Manage a Site*, and *Edit Branch and Enterprise Hub Site Parameters*.

Dual CPE Devices Logical Topology for NFX Network Services Platform

Figure 3 on page 168 shows the logical topology of the NFX Series dual CPE devices.

Figure 3: Dual CPE Device Topology - NFX Network Services Platform



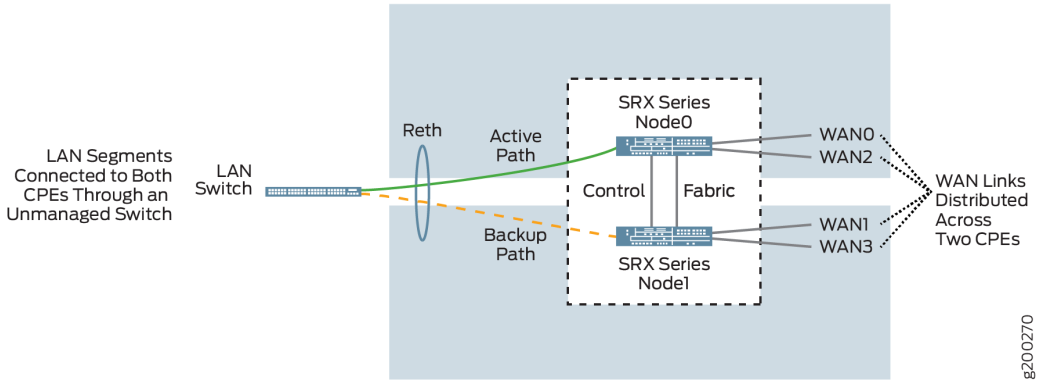
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

The Junos Control Plane (JCP) component acts as a switch, controls the front panel ports, and sends the traffic which arrives from the LAN or WAN to the NFX Series devices. On the LAN, the active/backup mechanism is used and if the primary device fails, the secondary device takes over processing of traffic. On the WAN, the active/active mechanism is used and all four WAN links are active and distributed across two NFX Series devices.

Dual CPE Devices Logical Topology for SRX Series Gateway Devices

Figure 4 on page 169 shows the logical topology of the SRX Series dual CPE devices.

Figure 4: Dual CPE Device Topology - SRX Series Devices



You can form a cluster using two SRX devices. A chassis cluster is formed between these nodes and performs as a single logical router. On the LAN, the active/backup mechanism is used and if the primary device fails, the secondary device takes over traffic processing. On the WAN, the active/active mechanism is used and all four WAN links are active and distributed across two SRX Series device.

> **NOTE:** On SRX 4100 and SRX4200 devices, out of the eight 1-Gigabit Ethernet/10-Gigabit Ethernet, a maximum of two ports are used for WAN links, and the remaining ports are used for LAN connectivity. The HA ports are used only for forming the cluster.

RELATED DOCUMENTATION

About the Device Template Page | 194

Viewing the History of Tenant Device Activation Logs

You can use the Activation Logs page to view the history of device activation logs. You can also view the details of the activation logs and their status.

To view the tenant device activation logs:

1. Click **Resources > Tenant Devices**.

   The Tenant Devices page appears, which list all devices.

2. Select a device and click **More > Activation Logs**.

   The Activation Logs page is displayed. Table 54 on page 170 describes the fields on the Activation Logs page.

3. Click a task name.

   The ZTP Logs page appears. Table 55 on page 171 describes the fields on the ZTP Logs page.

4. Click the Task Name.

   The Job Status page appears. Table 56 on page 171 describes the fields on the Job Status page.

5. Click **OK** to return to the previous page.

Table 54: Fields on the ZTP History Page

Field	Description
In progress	View the number of activated tasks that are in progress.
Success	View the number of activated tasks that are successful.
Failure	View the number of activated tasks that have failed.
Name	View the name of the task. Example: csp.tssm_ztp-Juniper-site-17-NFX-250-8052cc9451914be28c7c98fb64fd0db3
Start Date	View the start date and time of the task.
End Date	View the end date and time of the task.

Table 54: Fields on the ZTP History Page *(continued)*

Field	Description
Status	View the status of the task to know whether the task succeeded or failed.
Log	View the import logs. Click a log to access more detailed information about the imported log.

Table 55: Fields on the ZTP Logs Page

Field	Description
Task Name	View the ID created for the task. Example: install-license-to-device
Status	View the status of the task to know whether the task succeeded or failed.

Table 56: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who activated the task.
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

RELATED DOCUMENTATION

About the Tenant Devices Page | 138

Secure OAM Network Overview

IN THIS SECTION

- Topology of a Secure OAM Network | 172
- Workflow for Establishing a Secure OAM Network | 173
- Benefits of Secure OAM Network | 174

The management and control plane traffic between a customer premises equipment (CPE) device associated with an SD-WAN branch site and Contrail Service Orchestration (CSO) consists of the following:

- SSH and HTTPS sessions between the CPE device and CSO.
- BGP session between the CPE device and a virtual route reflector (VRR).
- System log traffic between the CPE device and CSO.

This traffic must be carried across the network through a secure and redundant communication channel. To provide such a secure and redundant communication channel, you must configure a secure Operation, Administration, and Maintenance (OAM) network between the SD-WAN branch sites and CSO.

This topic provides an overview of the secure OAM network, explains the workflow for configuring a secure OAM network, and benefits of a secure OAM network in an SD-WAN deployment.

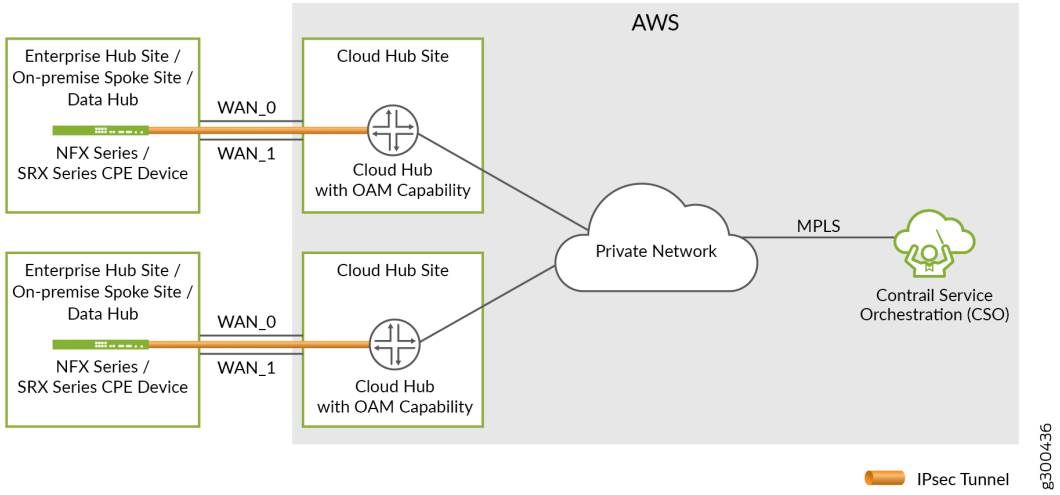
Topology of a Secure OAM Network

CSO uses the provider hub devices as SD-WAN hubs to set up IPsec tunnels and provision site-to-site or site-to-hub traffic. The provider hub acts as a concentrator for terminating the IPsec tunnels from SD-WAN branch sites. The provider hub device is located in the service provider's point of presence (POP). A provider hub device can be a SRX Series services gateway, or a vSRX instance. In CSO Release 5.0, provider hub devices are owned and managed by the Juniper Network team that hosts the cloud-based CSO.

NOTE: In CSO Release 5.0, the OAM hub is instantiated within the CSO. You do not need a provider hub for OAM network.

Figure 5 on page 173 shows the connections between the SD-WAN branch site, provider hub, and CSO.

Figure 5: Secure OAM Network



The secure OAM network is built using a dedicated IPsec tunnel (overlay connection) that is established between the CPE device associated with the SD-WAN branch site and a provider hub with OAM capability. The provider hub is connected to CSO through a secure private network (underlay connection) that is owned by the service provider.

Because the loopback IP address of the CPE device is used for OAM communication, it is fixed and unique across the entire deployment, and is always reachable from CSO over the IPsec tunnel. Even if the WAN interfaces are behind NAT and are assigned private IP addresses (by using DHCP), the OAM connectivity between the SD-WAN branch site and the provider hub is not impacted. The IPsec tunnel can still be established over the Internet WAN link including the LTE access type.

The secure OAM network is supported on both hub-and-spoke and full-mesh topologies.

Workflow for Establishing a Secure OAM Network

Use the following workflow to establish a secure OAM network between the SD-WAN branch site and the provider hub. As the provider hub is located in the service provider's POP, it has a private and secure connectivity to CSO.

To establish a secure OAM network between SD-WAN sites and the provider hub:

1. Log in to Customer Portal, and add a provider hub site. Associate the provider hub site with one of the available provider hub devices.

2. In Customer Portal, add a branch site for the CPE device in SD-WAN deployment.

3. When you create the site, specify the IP address prefix for the site and select at least one WAN link for OAM traffic. The WAN link with the **Use for OAM traffic** option enabled is used to set up the secure OAM tunnel to the provider hub device.

   > **NOTE:** For an NFX250 CPE device, specify at least one WAN link with traffic type as OAM and Data. If device redundancy is enabled, then specify one WAN link for each CPE device with the traffic type as OAM and Data.

   The CPE device is detected and activated. The Zero Touch Provisioning (ZTP) process is triggered over the secure OAM tunnel and the device is moved to provisioned state. The management and control plane traffic is carried across the secure OAM tunnel.

Benefits of Secure OAM Network

- IPsec tunnel redundancy—The secure OAM network supports a maximum of two IPsec tunnels between each SD-WAN branch site and the provider hub, thus providing redundancy and ensuring that OAM traffic is not lost even in the case of a WAN link failure.
- Hub device redundancy—In case of multihoming at the branch sites, each CPE device at the site is connected to two provider hubs, and the IPsec tunnels are established from the SD-WAN branch site to both the primary and secondary provider hub devices. This hub device redundancy ensures that the OAM traffic is not lost even if a hub fails.

  > **NOTE:** Sites with SD-WAN Essentials service do not support multihoming.

Secure OAM Network Redundancy Overview

IN THIS SECTION

- Logical Topology | **175**
- BGP Configuration | **176**
- Adding and configuring provider hub devices | **176**

- Adding and configuring a branch spoke site | 177
- Failure Detection and Recovery | 177
- Benefits of Secure OAM Network Redundancy | 177

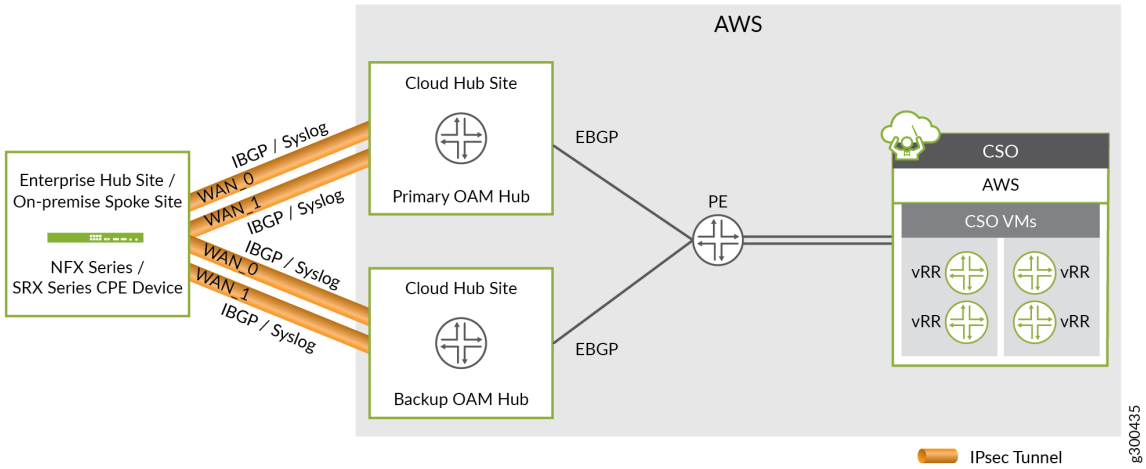
Contrail Service Orchestration (CSO) supports secure Operation, Administration, and Maintenance (OAM) network redundancy for provider hub devices in an SD-WAN deployment. You can configure two provider hub devices to act as the primary and secondary OAM hub devices and protect the site against device and link failures (WAN link between the CPE and the provider hub). If a fault or an outage occurs at the OpCo's OAM network beyond the primary OAM hub, the OAM connectivity is automatically restored through the secondary OAM hub without any user intervention.

The following sections explain the topology and benefits of secure OAM network redundancy in an SD-WAN deployment.

Logical Topology

Figure 6 on page 175 shows the topology for secure OAM network redundancy.

Figure 6: Secure OAM Network Redundancy



The CPE device at the branch site is connected to two provider hub devices that are configured as OAM hubs. The OAM hub devices are in turn connected to the OAM gateway router. During Zero Touch Provisioning (ZTP), two separate IPsec tunnels are established from the CPE device to the primary and

secondary OAM hub devices. The CPE device has a static route (loopback lo0.1) to both the OAM hubs through the IPsec tunnels.

BGP Configuration

When the provider hub device is onboarded, the BGP sessions are established. During the BGP sessions, the OAM hub device advertises the CSO subnet to the CPE device and the CPE device advertises the OAM subnet to the OAM hub device.

BGP supports primary and backup OAM hub by using local preference(hub-primary-select option) on the CPE device at the branch site. The CPE device decides whether the OAM hub is primary or secondary based on the hub-primary-select option. If the primary OAM hub fails or losses the CSO routes from the OAM gateway, then the secondary OAM hub is used. The CPE device advertises the OAM subnet to the OAM hubs. The OAM hubs, in turn, advertises the OAM subnet to the OAM gateway router.

> **NOTE:** In case the SINGLE_SSH feature is enabled in the device template, then only one IP address (loopback ip) is advertised. In case the SINGLE_SSH feature is disabled in the device template, then the OAM subnet is advertised.

The details of the BGP session that is established during ZTP are as follows:

- External BGP (eBGP) session is established between the OAM hub device and the OAM gateway router. During the eBGP session, the OAM gateway router advertises the CSO route reachability (CSO prefix and VRR prefixes) to both primary and secondary OAM hubs.
- Internal BGP (iBGP) session is established between the CPE device at the branch site and the OAM hub device. During this session the OAM hub device advertises the learned CSO route to the CPE device at the branch site. The CPE device learns routes from both primary and secondary OAM hub devices, and configures the primary OAM hub device with a higher preference and the backup OAM hub device with a lower preference.

Adding and configuring provider hub devices

The workflow to add and configure provider hub devices to support redundant secure OAM network is similar to adding a single provider hub device. For more information about adding and configuring a provider hub device, see *Add Provider Hub Sites in SD-WAN Deployments*.

NOTE: While adding the first provider hub device in any deployment, ensure that the capability of the device is set to **DATA and OAM**.

Adding and configuring a branch spoke site

The workflow to configure a branch site to support redundant secure OAM network is similar to adding a single branch site. For more information about adding and configuring a branch site, see *Add a Branch Site with SD-WAN Capability*.

NOTE:

- In real time-optimized deployments, you must enable the **Connect to Hubs** feature to establish secure OAM IPsec tunnels.
- On NFX250 devices, you must enable the traffic type as **OAM_AND_DATA** for at least one WAN link.

Failure Detection and Recovery

In case of network failure at the OpCo's OAM network behind the primary OAM hub, the route to primary OAM hub breaks and as a result, the primary OAM hub loses the route. The route from primary OAM hub to spoke for CSO breaks. As a result, the spoke obtains the route from the secondary OAM hub. The OAM traffic then moves from primary OAM hub to secondary OAM hub.

When the primary OAM hub is active, the BGP session is established and the primary OAM hub receives the route and propogates the route to the spoke. Because the primary OAM hub is configured with a higher preference in the spoke device, when the spoke receives the traffic from primary OAM hub, the OAM traffic will switches back to primary OAM hub.

Benefits of Secure OAM Network Redundancy

Hub device redundancy—In case of multihoming at the spoke sites, each CPE device at the site is connected to two provider hubs devices, which function as primary and secondary provider hub devices. Two separate

IPsec tunnels are established from the SD-WAN site to both primary and secondary provider hub devices. This hub device redundancy ensures that the OAM traffic is not lost even if a hub fails.

RELATED DOCUMENTATION

Secure OAM Network Overview | 172

Rebooting Tenant Devices and Provider Hub Devices

IN THIS SECTION

Rebooting a Tenant Device | 178
Rebooting a Provider Hub Device | 179

You can reboot tenant devices and provider hub devices by using CSO.

You need to reboot a tenant device or provider hub device if the device is down or if you want to fix operational errors in the device.

Rebooting a Tenant Device

To reboot a tenant device:

CAUTION: If you reboot a tenant device, deployments that are in progress are stopped.

1. Select **Resources > Tenant Devices**.

   The Tenant Devices page appears.

2. Select the tenant device that you want to reboot and select **More > Reboot**.

The Reboot Device page appears, displaying the message **Reboot Device will stop deployments in progress. Continue with reboot?**.

3. Click **Yes** to reboot the device.

   A device reboot job is triggered and the message **Device Reboot job is created** appears on the Tenant Devices page.

   You can click the Device Reboot link in the message to view the device reboot logs (including job status, start date and time, end date and time) on the Device Reboot Details page. Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

   The Status Message column on the Tenant Devices page displays the status as **Reboot in-progress**.

   - If the device is rebooted successfully, the Status Message column displays the status as **Reboot Succeeded**.
   - If the device reboot fails, the Status Message column displays the status as **Reboot Failed**.

     A device reboot may fail because of various reasons such as the reboot time exceeding the timeout value that is set by CSO, or when the device is unreachable.

     You can log in to the device CLI and check the logs to identify the reason for reboot failure

Rebooting a Provider Hub Device

To reboot a provider hub device:

CAUTION: If you reboot a provider hub device, deployments that are in progress are stopped.

1. Select **Resources > Provider Hub Devices**.

   The Provider Hub Devices page appears.

2. Select the Provider hub device that you want to reboot and select **More > Reboot**.

   The Reboot Device page appears, displaying the message **Reboot Device will stop deployments in progress. Continue with reboot?**.

3. Click **Yes** to reboot the device.

   A device reboot job is triggered and the message **Device Reboot job is created** appears on the Provider Hub Devices page.

You can click the Device Reboot link in the message to view the device reboot logs (including job status, start date and time, end date and time) on the Device Reboot Details page. Alternatively, you can view the status of the job on the Jobs (**Monitor > Jobs**) page.

The Status Message column on the Provider Hub Devices page displays the status as **Reboot in-progress**.

- If the device is rebooted successfully, the Status Message column displays the status as **Reboot Succeeded**.
- If the device reboot fails, the Status Message column displays the status as **Reboot Failed**.

  A device reboot may fail because of various reasons such as the reboot time exceeding the timeout value that is set by CSO, or when the device is unreachable.

  You can log in to the device CLI and check the logs to identify the reason for reboot failure

RELATED DOCUMENTATION

About the Provider Hub Devices Page | **140**

About the Tenant Devices Page | **138**

Identifying Connectivity Issues by Using Ping

You can use Contrail Service Orchestration (CSO) to perform a ping operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to a remote host for identifying issues in connectivity with the remote host.

When you ping a remote host from a device, an Internet Control Message Protocol (ICMP) packet is sent to the remote host. By analyzing the results of the ping operation, you can identify the possible device connectivity issues between the remote host and the device.

NOTE: In Contrail Service Orchestration (CSO) Release 6.1, the following devices support ping:

- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform the ping operation:

1. Do one of the following:
   - To initiate a ping from a provider hub device, select **Resources** > **Provider Hub Devices**.

     The :Provider Hub Devices page appears.
   - To initiate a ping from a tenant device, select **Resources** > **Tenant Devices**.

     The Tenant Devices page appears.
2. Select a device from the list of devices displayed and click **More** > **Ping**.

   The Ping page appears.

   > **NOTE:** You can initiate a ping from a device only when its operational status (in CSO) is Up.

3. Complete the configuration according to the guidelines provided in Table 57 on page 181.

   > **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. Click **Ping** to initiate the ping request.

   A job is created and a Ping Progress page appears. After the host sends the ping packets, the Ping Result page appears. If the ping operation is successful, the Ping Result page displays the parameters specified in Table 58 on page 183.

   If the ping operation fails, the Ping Result page displays an appropriate error message (such as **No response** or **No route to host**), indicating that there is an issue in the connectivity to the remote host.

Table 57: Fields on the Ping page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Ping Request Packets	Enter the number of ping request packets to be sent to the remote host. Default: 5. Range: 1 through 300.
Advanced	

Table 57: Fields on the Ping page *(continued)*

Field	Description
Source Interface	Select the source interface on the device through which you want to send the ping request to the remote host. If you do not select a source interface, ping requests are sent on all interfaces. To clear the selected interface, click **Clear All** and select another interface.
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops along the path to the remote host.
Rapid Ping	Click the toggle button to enable or disable (default) sending ping requests rapidly. If you enable this option, the device sends a minimum of 100 ping request packets per second or sends a packet as soon as a response to the previous packet is received, whichever is greater. • If the source device does not receive a response for 500 ms, timeout is considered. • If the source device receives a response within 500 ms, the next ping request packet is sent immediately. **NOTE:** The ping results are displayed in a single consolidated message instead of individual messages for each ping request packet sent.
Packet Fragmentation	Click the toggle button to enable or disable (default) the fragmenting of ping request packets. If packet fragmentation is disabled, ping packets with the maximum transmission unit (MTU) greater than 1500 bytes are dropped.
Packet Size (bytes)	Enter the size (in bytes) of the ping request packet. Default: 56 bytes. Range: • 1 through 1,472 bytes, if packet fragmentation is disabled. • 1 through 65,468 bytes, if packet fragmentation is enabled.
Wait Time (seconds)	Enter the time (in seconds) for which the source device waits for a response to the ping request packet. The source device considers the remote host as not reachable after the wait time elapses. Default: 10 seconds. Range: 0 through 600 seconds.

Table 57: Fields on the Ping page *(continued)*

Field	Description
Incoming Interface	Click the toggle button to include or exclude (default) information (on the Ping Result page) about the interface on the source device that receives the ping responses..
Routing Instance	Select a specific routing instance that the ping request packets can use to reach the remote host. The ping result displays the information about the connectivity between the source device and the remote host based on the selected routing instance. To clear the selected routing instance, click **Clear All** and select another routing instance.

Table 58: Fields on the Ping Result page

Field	Description
Packet Loss	Displays the percentage of ping packets sent for which the source device did not receive a response.
Round Trip Time Taken (in µs)	Displays the following information about the duration (in microseconds) between the time when the device sends the ping request and the time when the device receives a response from the remote host. Displays the following: • Minimum: The minimum time taken to receive a response for a ping request packet. • Maximum: The maximum time taken to receive a response for a ping request packet. • Average: The average time taken to receive a response for all the ping request packets sent in a ping operation. • Standard Deviation: The variation of the round trip time from the mean round trip time.
Details	
Sequence	Sequence number of all the ping request packets.
Result	Result of the ping request packets—Success or Failure.
Incoming Interface	Interface on the source device on which the responses are received for the ping requests. This data appears if you have enabled the Incoming Interface option on the Ping page.
Time Taken	Time taken (in microseconds) to receive response to a ping request packet.

Identifying Connectivity Issues by Using Traceroute

You can use Contrail Service Orchestration (CSO) to perform a traceroute operation from a device (provider hub, tenant device, CPE device, enterprise hubs, or next-generation firewall device) to the remote host. Traceroute helps you view the path that a packet travels to reach the remote host. The result is useful in identifying the point of network failure in the path between the source device and remote host.

> **NOTE:** In Contrail Service Orchestration (CSO) Release 6.1, the following devices support traceroute:
>
> - NFX Series: NFX150, NFX250
> - SRX Series: SRX300, SRX320, SRX340, SRX345, SRX380, SRX1500, SRX4100, SRX4200, SRX4600
> - vSRX

To perform traceroute operation:

1. Do one of the following:
   - To initiate traceroute from a provider hub device, select **Resources** > **Provider Hub Devices**.

     The Provider Hub Devices page appears.
   - To initiate traceroute from a tenant device, select **Resources** > **Tenant Devices**.

     The Tenant Devices page appears.
2. Select a device from the list of devices displayed and click **More** > **Traceroute**.

   The Traceroute page appears.
3. Complete the configuration according to the guidelines provided in Table 59 on page 185.

   > **NOTE:** Fields marked with an asterisk (*) are mandatory.
4. Click **Traceroute** to initiate the traceroute operation.

   A job is created and a traceroute progress page appears. If the traceroute operation is successful, the Traceroute Result page displays the traceroute parameters specified in Table 60 on page 186.

   If the traceroute operation fails, the Traceroute Result page displays an appropriate error message (such as **No response** or **No route to host**).

Table 59: Fields on the Traceroute page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Maximum Hops	Specify the maximum number of network devices that a packet can pass through to reach the remote host. Default: 30. Range: 1 through 255. If the number of hops to reach the remote host exceeds the set value, the traceroute packet is dropped.
Advanced	
Source Interface	Select a source interface on the device from which you want to send the packets to the remote host. Click **Clear All** to remove the selected interface and select another interface.
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops in the path to the remote host.
Wait Time (seconds)	Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout. Default: 10 seconds. Range: 0 through 86,399 seconds.
Routing Instance	Select a routing instance that the traceroute request packets can use to reach the remote host. The trace result displays the route information based on the configured routing instance type. To clear the selected routing instance, click **Clear All** and select another routing instance.

Table 60 on page 186 lists the parameters on the Traceroute Result page when the traceroute operation is successful.

Table 60: Fields on the Traceroute Result page

Field	Description
Hop	Hostname or IPv4 address of the network devices that the packet passed through to reach the remote host.
Time Taken by Packet 1 Time Taken by Packet 2 Time Taken by Packet 3	Duration (in microseconds) between the time from when the source device sends a packet, and the time it received a response from the hops and the remote host.

Remotely Accessing a Device CLI

You can use the Devices page to remotely access the CLI of a CPE device and run **show** operational commands.

> **NOTE:** As an OpCo administrator, you can remotely access a device CLI only if you have the tenant administrator role assigned to you.
>
> As a tenant administrator, you can remotely access the device CLI from the Devices page on the Customer Portal.

To access this page:

1. Select **Resources > Devices**.

   The Devices page appears.

2. Select a device from the Devices List.

   > **NOTE:** You can only select a device whose operational status is marked **Up**.

3. Click **More > Remote Console**.

   The Remote Console for *Device-Name* page appears.

> **NOTE:** For dual SRX Series devices, the **Remote Console** option is enabled only at the cluster level and disabled at the member level.
>
> For dual NFX250 devices, the **Remote Console** option is enabled at the individual member level and disabled at the cluster level.

4. Select one of the following options:
   - **Read only access** (default option)—Allows you to automatically log in to the device through the Remote Terminal browser window, without entering a username and password. If the connection is established successfully, the operational mode CLI prompt appears in the browser window. You can run only operational commands in this mode.
   - **Full access with Junos device login credentials**—Allows you to log in to the device using the Junos login credentials. If the connection is established successfully, the configuration mode CLI prompt appears in the browser window. You can run both configuration and operational commands in this mode.
5. Close the Remote Terminal browser window to disconnect from the device.

   The session times out if the session remains idle for more than 15 minutes (default) and you are automatically logged out of the device. The **Remote console connection was closed. Please close this window and open the remote console again** message appears in the browser window.

   You must close the idle terminal window before opening a new terminal window.

   CSO generates an audit log each time a user accesses the device CLI. The logs provide information about the user, the date and time of access, and type of access (read-only or read-write). Use the Audit Logs page (**Administration > Audit Logs**) to view the remote console audit logs.

RELATED DOCUMENTATION

About the Provider Hub Devices Page | 140

About the Tenant Devices Page | 138

Device Template Overview

IN THIS SECTION

- Platform | 189
- SD-WAN CPE | 189
- Secure Internet CPE | 190
- Managed Internet CPE | 191

A device template contains configuration and provision settings for a physical device, such as a CPE device or a router, which you manage through Contrail Service Orchestration (CSO). The CSO installation includes several default device templates for CPE devices and other physical devices. You can either use a default CPE device template as is if the template suits your specific topology requirements or customize the default CPE device template to meet your specific requirements. You can also create your own device templates and upload that to CSO. The CPE device templates are specific to the type of device and topology of the solution. The device templates for non-CPE devices are fixed and you cannot customize them. You must assign a device template to each CPE device at the site. You assign a device template to a device in CSO when you add a point of presence (POP). In some cases, you might want all CPE devices to use the same values, through device templates, you have the options to provide the values.

> **NOTE:** In CSO Release 5.0, device templates are owned and managed by the Juniper Networks team that manages the cloud installation of CSO. If you need to modify device templates, talk to your Juniper Networks representative.

The CPE device templates contain three types of information:

- Template settings information—It prepares the device for remote activation, connects the device to the peer router, and establishes an IPsec tunnel with the router.
- Stage-2 configuration template information—It specifies the additional settings that you or your customer can configure for the device. For example, you can enable configuration of LAN and firewall policies. You create these configuration templates in Configuration Designer and provide implementation details in the device template.
- Stage-2 initial configuration information—It provides the actual values for the stage-2 configuration templates. In general, your customers perform this configuration through the Customer Portal.

The CPE device templates support four deployment models: Platform, SD-WAN CPE, Secure Internet CPE, and Managed Internet CPE.

Platform

Starting in Release CSO 6.0.0, CSO uses platform-specific templates (SRX Platform, NFX150 Platform, or Dual SRX platform) to onboard a device. These platform templates contain the basic configuration settings required for CSO to activate and manage the device.

SD-WAN CPE

You can use the **NFX 150 as SDWAN CPE**, **NFX 250 as SDWAN CPE**, **Dual NFX 250 as SDWAN CPE**, **SRX as SDWAN CPE**, **SRX-1500 as SDWAN CPE**, **SRX-4x00 as SDWAN CPE**, **Dual SRX as SDWAN CPE**, **Dual SRX 1500 as SDWAN CPE**, or **Dual SRX 4x00 as SDWAN CPE** device template for a CPE device in an SD-WAN deployment.

Figure 7 on page 189 shows the topology for an SD-WAN CPE deployment model.

Figure 7: SD-WAN CPE

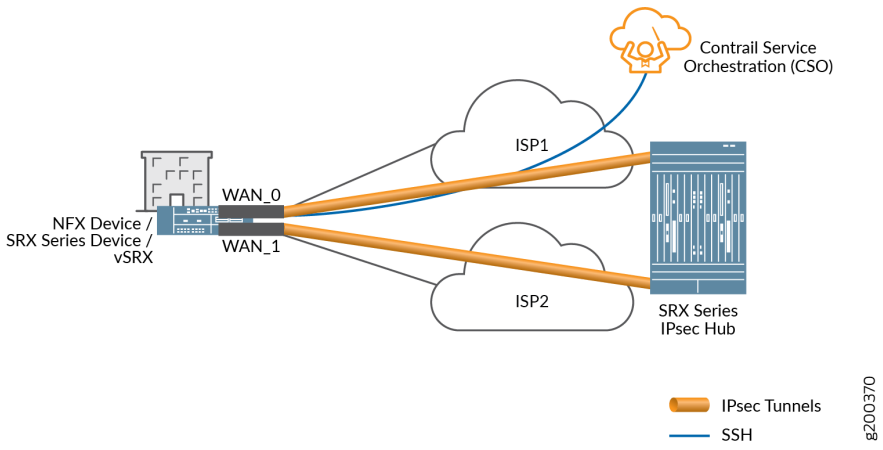


Table 61 on page 190 lists the connectivity details for an SD-WAN CPE.

Table 61: Connectivity Details for SD-WAN CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	MPLS, Internet	ge-1/0/1 (NFX150 ge-0/0/10 (NFX250) ge-0/0/0 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM
WAN_1	MPLS, Internet	ge-1/0/2 (NFX150) ge-0/0/11 (NFX250) ge-0/0/1 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM
WAN_2	MPLS, Internet	ge-1/0/3 (NFX150) (NFX1250) ge-0/0/2 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM
WAN_3	MPLS, Internet	ge-1/0/4 (NFX150) (NFX250) ge-0/0/3 (SRX) xe-0/0/0 (SRX4x00)	Static, DHCP	IPsec	Data, OAM

Secure Internet CPE

You can use the **NFX 150 as Secure Internet CPE** or **NFX 250 as Secure Internet CPE** device template to provide a secure Internet connection through the CPE device.

Figure 8 on page 191 shows the topology for a secure Internet CPE deployment model.

Figure 8: Secure Internet CPE

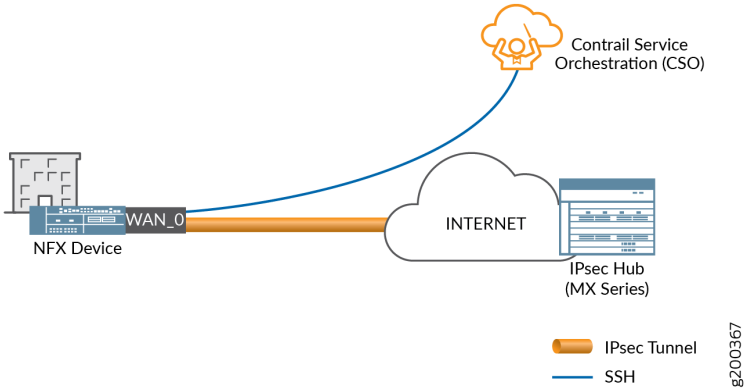


Table 62 on page 191 lists the connectivity details for secure Internet CPE.

Table 62: Connectivity Details for Secure Internet CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	Internet	ge-1/0/1 (NFX150) ge-0/0/8 (NFX250)	DHCP	IPsec	Data, OAM

Managed Internet CPE

You can use the **NFX Managed Internet CPE** or **SRX Managed Internet CPE** device template to provide a managed Internet connection through the CPE device.

Figure 9 on page 191 shows the topology for a managed Internet CPE deployment model.

Figure 9: Managed Internet CPE

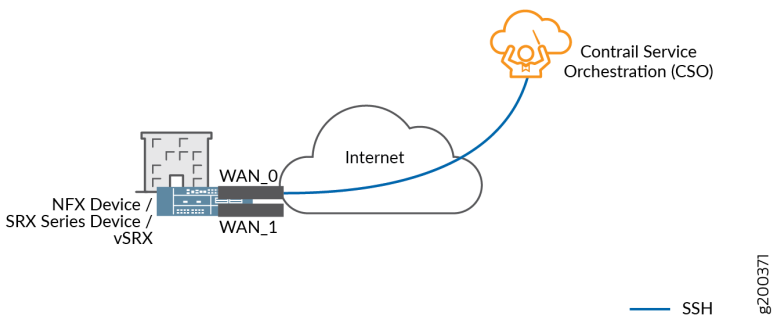


Table 63 on page 192 lists the connectivity details for a managed Internet CPE deployment model.

Table 63: Connectivity details for Managed Internet CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	Internet	ge-1/0/1 (NFX150) ge-0/0/8 (NFX250)	DHCP	—	Data, OAM

RELATED DOCUMENTATION

About the Device Template Page | 194

Multi-Service Shared Bearer Overview

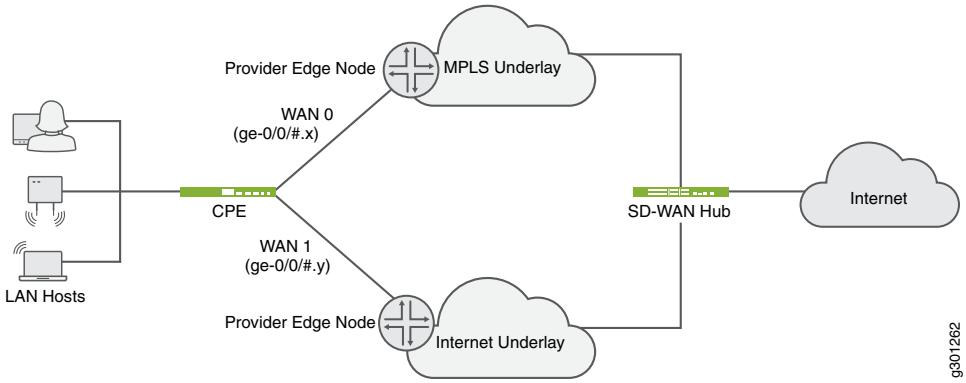
IN THIS SECTION

- Benefits of Shared Bearer | 194

Contrail Service Orchestration (CSO) supports the provisioning of more than one service on the same physical (bearer) interface for WAN links associated with on-premise SD-WAN spoke sites and enterprise hub sites. In previous CSO releases, each WAN link had to be configured as a separate physical interface. However, from CSO Release 5.1.0 (for on-premise spoke sites) and CSO Release 5.1.1 (for enterprise hub sites), WAN links can be configured as logical interfaces on the same physical interface. Therefore, the *same* physical interface can be used to carry Internet and MPLS traffic with VLAN separation. The shared bearer (physical interface) supports both full-mesh and hub-and-spoke topologies.

Figure 10 on page 193 shows an example of a shared bearer topology. There are two WAN links on the CPE device (WAN 0 and WAN 1), which are connected to two PE devices, one on an MPLS network and the other on an Internet network.

Figure 10: Example of Multi-Service Shared Bearer Topology



In this example, WAN 0 uses the logical interface ge-0/0/#.*x*, and WAN 1 uses the logical interface ge-0/0/#.*y*.

Here, ge-0/0/# represents the physical interface, where # represents the port, and *x* and *y* represent the logical unit numbers of the physical interface ge-0/0/#. For example, if the physical interface is ge-0/0/3, then the logical interfaces can be ge-0/0/3.10 and ge-0/0/3.11.

Therefore, WAN 0 and WAN 1 share the same physical interface, but are on two separate logical interfaces with VLAN separation.

> **NOTE:** The interface names might differ based on the device model and the WAN interface configured in the device template.

When the same physical interface is used for multiple WAN links:

- CSO supports class of service (CoS) provisioning of the shaping rate at the logical interface level. In previous releases, CoS provisioning of the shaping rate was supported only at the physical interface level. Shaping rate controls the maximum rate at which traffic is allowed to be transmitted on an interface.
- CSO supports flexible (mixed) tagging with simultaneous tagged and untagged WAN links for single CPE devices. However, when there are multiple logical interfaces on the same physical interface, there can be only one untagged logical interface and the rest of the interfaces must be tagged. The support for simultaneous tagged and untagged logical interfaces on same physical interface is not available on dual CPE devices. Table 64 on page 194 displays the VLAN tagging support for single and dual CPE devices.

To enable the configuration of WAN links as logical interfaces in enterprise hub and on-premise SD-WAN spoke sites, the administrator users must modify the device template and configure the WAN ports as logical interfaces. See “Configuring Template Settings in a Device Template” on page 202.

Table 64: Support for VLAN Tagging for Single and Dual CPE Devices

Type of CPE	VLAN Tag	Unique Physical Interface for Each WAN Link	Same Physical Interface for More Than One WAN Link
Single CPE	Untagged	Supported	Supported. However, only one WAN link can be untagged.
Single CPE	Tagged	Supported	Supported
Dual CPE	Untagged	Supported	Not supported
Dual CPE	Tagged	Supported	Supported

Benefits of Shared Bearer

- Reduces operational complexity by allowing multiple services to be configured on the same physical interface.

RELATED DOCUMENTATION

About the Device Template Page | 194

About the Device Template Page

IN THIS SECTION

- Tasks You Can Perform | 195
- Field Descriptions | 195
- Supported Device Templates | 196

To access this page, click **Resources > Templates > Device Templates**.

Use this page to view and manage device templates.

Tasks You Can Perform

You can perform the following tasks from this page:

- Clone a device template. See "Cloning a Device Template" on page 199.
- Import a device template from a file. See "Importing a Device Template" on page 200.
- Configure device template settings. See "Configuring Template Settings in a Device Template" on page 202.
- Update stage-2 configuration template. See "Updating Stage-2 Configuration Template in a Device Template" on page 224.
- Configure stage-2 initial configuration. See "Configuring Stage-2 Initial Configuration in a Device Template" on page 229.
- Modify a device template description. See "Modifying a Device Template Description" on page 232.
- Delete a device template. See "Deleting a Device Template" on page 232.
- View details of a device template—Hover over the device template name and Click the Detailed View icon or click **More > Detail View**.

  The detailed view pane for the selected device template appears on the right side of the Device Templates page, displaying details such as the target family and tenants.

  Click the close icon (X) to close the pane.
- Show or hide columns displayed on the page—Click the **Show Hide columns** icon in the top right corner of the table and select the columns that you want to view on the page.
- Search for a specific device template—Click the Search icon in the top right corner of the table and enter the search text in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

Table 65 on page 195 describes the fields on the Device Templates page.

Table 65: Fields on the Device Templates Page

Field	Description
Name	Name of the device template

Table 65: Fields on the Device Templates Page *(continued)*

Field	Description
Description	Description of the device template. Example: NFX250 device deployed as a CPE device with SD-WAN capability.
Version	CSO version of the device template.
Build	CSO build name of the device template.
Assigned to	Number of tenant sites using the device template. Example: 2 Tenants (2 Sites)
Workflows	Number of workflows used in the device template. Example: 7
Target Family	Name of the device family for which the device template is created. Example: juniper-srx
Owner	Name of the owner (*OpCo Name* or default-project) who created the device template.
Last Updated	Date and time when the device template was last updated. Example: 05/23/2017 06:22

Supported Device Templates

Table 66 on page 196 describes the list of supported device templates.

Table 66: List of Supported Device Templates

No.	Device Template Name	Device Template Description
3	NFX250 as Managed Internet CPE	Device template for an NFX250 device acting as a CPE for a managed Internet service. This device template supports managed Internet Service with one Gigabit Ethernet WAN link.

Table 66: List of Supported Device Templates *(continued)*

No.	Device Template Name	Device Template Description
4	NFX250 as SD-WAN CPE	Device template for an NFX250 device acting as a CPE in an SD-WAN deployment with hub-and-spoke topology. This device template supports SD-WAN deployment with up to four WAN links.
5	Dual NFX250 as SD-WAN CPEs	Device template for NFX250 devices in device redundancy mode in an SD-WAN deployment. This device template supports device redundancy in SD-WAN deployment with up to four WAN links.
6	NFX150 as Managed Internet CPE	Device template for an NFX150 device as CPE for managed Internet service. This device template supports managed Internet Service with one Gigabit Ethernet WAN link.
8	NFX150 as SD-WAN CPE	Device template for an NFX150 device as CPE in an SD-WAN deployment with hub-and-spoke topology. This device template supports up to four WAN links.
9	SRX as SD-WAN CPE	Device template for an SRX Series Services Gateway acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology. This device template supports SD-WAN deployment with up to four WAN links.
10	SRX as SDWAN Hub	Device template for an SRX Series Services Gateway acting as a hub device in an SD-WAN deployment with hub-and-spoke topology. This device template supports SD-WAN deployment with up to four WAN links.
11	Dual SRX as SD-WAN CPEs	Device template for SRX Series Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment. This device template supports SD-WAN deployment with up to four WAN links.

Table 66: List of Supported Device Templates *(continued)*

No.	Device Template Name	Device Template Description
12	vSRX as SD-WAN spoke in AWS	Device template for a vSRX instance acting as spoke in AWS for SD-WAN deployment. This device template supports SD-WAN deployment with up to four WAN links.
13	SRX-4x00 as SD-WAN CPE	Device template for an SRX 4000 line Services Gateways acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology. This device template supports SD-WAN deployment with up to four WAN links.
14	Dual SRX4x00 as SD-WAN CPEs	Device template for SRX 4000 line Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment. This device template supports SD-WAN deployment with up to four WAN links.
15	SRX_Standalone_Pre_Staged_NonZTP	Device template for pre-staged SRX Services Gateways acting as a Standalone CPE device without ZTP.
16	SRX_Standalone_Pre_Staged_ZTP	Device template for pre-staged SRX Services Gateways acting as a Standalone CPE device with ZTP.

RELATED DOCUMENTATION

Device Template Overview | 188

Cloning a Device Template

Cloning a device template is useful when you want to create a device template that is similar to an existing one but with small differences. You can clone a device template by using either of the methods mentioned below:

To clone a device template:

1. Select **Resources > Templates > Device Templates**.

   The Device Template page appears.

2. Select the device template that you want to clone, and click **Clone**.

   The Clone Template page appears.

3. Specify an appropriate name for your new device template. For example, SRX as SD-WAN CPE.

4. Click **Ok**.

   The cloned device template appears on the Device Template page. You can now edit the new device template and customize the configurations as needed.

   NOTE: You can create only one clone of a platform template. If a cloned platform template is present, then CSO uses this template to onboard the device.

You can also clone the device template by performing the following procedure:

1. Select **Resources > Templates > Device Templates**.

   The Device Template page appears.

2. Select the device template that you want to clone, and then select **Edit Device Template > Template Settings**.

   The Template Settings page appears.

3. Modify the configurations as required and click **Save As**.

   The Create Device template page appears.

4. Specify an appropriate name for your new device template. For example, SRX as SD-WAN CPE.

5. Click **Ok**.

   The cloned device template appears on the Device Template page. You can now edit the new device template and customize the configurations as needed.

RELATED DOCUMENTATION

Importing a Device Template | **200**

Importing a Device Template

IN THIS SECTION

- Creating a Device Template File | **201**
- Importing a Device Template File | **201**

Use the Device Templates page (**Resources > Templates > Device Templates**) to import a device template in JSON format for the customer.

NOTE: You must create a device template file before you can import a device template

Creating a Device Template File

To create a file of device information:

1. Select **Resources > Templates > Device Templates > Import Device Template**.

   The Import Device Template page appears.

2. Click the **Download Sample JSON** link to open and save the sample JSON data file.

   The sample file opens at the bottom of the page.

3. Save the template file with an appropriate name to your computer.

   NOTE: You must retain the file format as .json to successfully upload the device template details to the Administration Portal.

4. Customize the sample JSON file according to the deployment.

5. Save the customized file.

Importing a Device Template File

Device templates are used to configure devices on a tenant site and these templates must be assigned to the device before you activate the device.

NOTE: A device template data file is required before your import device templates.

To import device template configuration:

1. Select **Resources > Templates > Device Templates > Import Device Template**.

   The Import Device Template page appears.

2. Click **Browse** and navigate to the directory containing the device template configuration JSON file.

3. Select the file and click **Open**.

4. Click **Import Device Templates**. If you want to discard the import process, click **Cancel** instead.

   The Device Templates Import Completed page appears with the details of the successful import.

5. Click **OK** to complete the import process.

   The imported device template is displayed on the Device Template page.

Configuring Template Settings in a Device Template

To configure the device template settings:

> **NOTE:** This topic is applicable only to users with an SP Administrator role.

1. Select **Resources > Templates > Device Templates**.

   The Device Templates page appears.

2. Select the device template for which you want to configure the settings and then select **Edit Device Template > Template Settings**.

   The Template Settings page appears.

3. Complete the configuration settings according to the guidelines in Table 67 on page 203.

   For platform-specific templates, see Table 70 on page 222 and Table 71 on page 223.

4. Click **Save**.

   The changes that you made to the device template are saved and you are returned to the Device Templates page. After you modify a device template and use that device template to add a site, the

modified parameters are used in the site addition workflow. The device template modifications do not take effect on existing sites.

Table 67: Fields on the Template Settings Page for All Device Templates

Field Name	Description	Applicable To (Device Templates)
SSH Settings		
Prevent root login via SSH?	Specify whether root login (to the device) by using SSH should be allowed or not.	NFX250 NFX150 SRX4100 SRX4200
Restrict SSH access to be from CSO only	Specify whether SSH access to the device should be restricted only to Contrail Service Orchestration (CSO) or not.	NFX250 NFX150 SRX4100 SRX4200
Max number of SSH connections allowed at any time	Enter the maximum number of SSH connections allowed at any time. Range: 1 through 250.	NFX250 NFX150 SRX4100 SRX4200
Max number of SSH connections allowed per minute	Enter the maximum number of SSH connections allowed per minute. Range: 1 through 250.	NFX250 NFX150 SRX4100 SRX4200
Max number of sessions per SSH connection	Enter the maximum number of sessions allowed per SSH connection. Range: 1 through 250.	NFX250 NFX150 SRX4100 SRX4200

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
Policer Settings		
Bandwidth limit for ICMP traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Internet Control Message Protocol (ICMP) traffic towards the device.	NFX250
Burst-size limit for ICMP traffic towards the device	Enter the burst-size limit, in bytes, for ICMP traffic towards the device.	NFX250
Bandwidth limit for trace-route traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for traceroute traffic towards the device.	NFX250
Burst-size limit for trace-route traffic towards the device	Enter the burst-size limit, in bytes, for traceroute traffic towards the device.	NFX250
Bandwidth limit for DHCP traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Dynamic Host Configuration Protocol (DHCP) traffic towards the device.	NFX250
Burst-size limit for DHCP traffic towards the device	Enter the burst-size limit, in bytes, for DHCP traffic towards the device.	NFX250
Bandwidth limit for DNS traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Domain Name System (DNS) traffic towards the device.	NFX250
Burst-size limit for DNS traffic towards the device	Enter the burst-size limit, in bytes, for (DNS) traffic towards the device.	NFX250
Log Rotation Settings		
Max size (MB) for log files	Enter the maximum size, in megabytes (MB), of the log files stored on the device.	NFX250
Max number of log files	Enter the maximum number of log files to be stored on the device at any time.	NFX250
Customer Parameters		

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
S2_MODEL_HUGEPAGE_COUNT	Enter the number of 1-GB huge pages usable by the virtualized network functions (VNFs) (on an NFX250-S2 device with a total memory of 32 GB.	NFX250
Dual_VF_ENABLED	Click the toggle button to configure two WAN links on the same physical port. If you enable this toggle button, map two virtual ports (WAN ports) to the same physical port (heth port) in the WAN Ports grid.	NFX150
ADSL_VPI	Enter the Virtual Path Identifier (VPI) setting to connect to the asymmetric digital subscriber line (ADSL) service provider.	NFX150 NFX250 SRX320 SRX340 SRX345 SRX380
ADSL_ENCAP	Enter the encapsulation that is used to connect to the ADSL service provider.	NFX150 NFX250 SRX320 SRX340 SRX345 SRX380
VNF_OAM_TRANSLATED_PORT_START	Enter the first port number that can be used to expose (by using port translation) a VNF Operation, Administration, and Maintenance (OAM) port on the gateway router OAM interface or the WAN interface. This setting is used in cases where the VNF does not have its own OAM IP address from the in-band OAM network.	NFX250

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
ADSL_VCI	Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider.	NFX150 NFX250 SRX320 SRX340 SRX345 SRX380
AUTO_INSTALL_LICENSE_TO_DEVICE	Specify whether licenses should be automatically installed on the device during the ZTP workflow or not.	NFX250
AUTO_INSTALL_DEFAULT_TRUSTED_CERTS_TO_DEVICE	Specify whether the Junos OS default trusted certificates should be installed on the device during the ZTP workflow or not.	NFX250
NO_LOCAL_FAVOR_ECMP	Use this parameter to control the behavior of local-breakout traffic in a dual CPE cluster. The overlay traffic continues to load-balance across nodes as usual and doesn't have any dependency on this parameter. By default, this parameter is disabled. When disabled, Local-Breakout traffic will egress from the active link of the node on which the traffic has arrived. The local-breakout traffic will load-balance within this node and not across nodes. You can enable this parameter to load balance equal-cost multi path (ECMP) traffic across active-active links on both the nodes of a dual CPE cluster. Note: This parameter is available only when the devices in the cluster are running JUNOS OS Release 19.3R2-S1 or later.	NFX250 SRX Series Devices

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
USE_SINGLE_SSH_TO_NFX	Specify whether to manage the NFX250 device and its components by using a single SSH connection between CSO and the NFX250 device.	NFX250
ENC_ROOT_PASSWORD	Specify the Junos OS root password to be set on the device. The password that you type is masked and the password is encrypted and stored.	NFX250
GWR_VSRX_IMAGE_LOCAL_FILE_PATH	Enter the local path of the vSRX image file present on the NFX250 device; this image file is used when the gateway router virtual machine (VM) is created. For example, **./var/third-party/images/*vsrx*-15.1X*.qcow2**. If this parameter is not set or if the file is not present on the NFX250 device, then a vSRX image with the filename specified in **GWR_VSRX_IMAGE_CNAME_IN_CSO** is downloaded from the CSO file server to the NFX250 device.	NFX250
GWR_VSRX_IMAGE_CNAME_IN_CSO	Enter the name with which the vSRX image was uploaded into the Image Management Service in CSO. If the vSRX image file specified in **GWR_VSRX_IMAGE_LOCAL_FILE_PATH** is not present, then an image with the name specified is downloaded to the NFX250 device.	NFX250
ACTIVATION_CODE_ENABLED	Specify whether an activation code must be specified to activate the device or not.	NFX250
INTERNAL_OAM_SUBNET	Enter the IP address for the subnet that is used for internal OAM connectivity between various components of the NFX250 device.	NFX250
AUTO_DEPLOY_STAGE2_CONFIG	Specify whether the stage-2 configuration should be automatically deployed on the device during the ZTP workflow.	NFX250

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
OOB_MGMT_ENABLED	Specify whether the out-of-band (OOB) management port of the device is being used for management connectivity or not. If you enable this field, a default route must be available through the OOB interface. If you disable this field, there is no connectivity through the OOB management port of the device and the stage-1 configuration that is generated includes a static default route.	NFX250
S1_MODEL_HUGEPAGE_COUNT	Enter the number of 1-GB huge pages usable by the VNFs on an NFX250-S1 device with a total memory of 16 GB.	NFX250
CONTROL_LINK_PORT_NAME	Enter the physical port name for the control link connection for a dual CPE setup.	NFX250
FAB_LINK_PORT_NAME	Enter the physical port name for fabric link connection for a dual CPE setup.	NFX250
MAX_DVPN_TUNNELS_ON_SITE	Enter the maximum number of dynamic mesh tunnels that are allowed to create at the tenant site.	NFX150 NFX250 SRX Series
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE	Enter the minimum number of dynamic mesh tunnels at the tenant site after which the dynamic mesh tunnels are dynamically deleted.	NFX150 NFX250 SRX Series
WAN PORTS	Select an entry in the grid and click the Edit icon to modify the mapping of the virtual ports (WAN ports) to physical ports (heth ports). From CSO Release 6.0.0 onward, you can map up to two WAN ports to a single heth port.	NFX150

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
WAN_PORT_NAMES	Specify the mapping of the physical or logical port names used for WAN side connectivity. You specify logical port names if you want to configure more than one WAN link on the same physical interface. The WAN links are connected from the same physical interface to the Provider Edge (PE) nodes through logical sub-interfaces with VLAN separation. If an SRX Series enterprise hub device is preconfigured for aggregated Ethernet (AE), specify the AE interface name on upto two WAN interfaces. The WAN interfaces must be the same as the interfaces named in the AE configuration on the enterprise hub device.	NFX250 SRX Series
LAN_PORT_NAMES	Specify the mapping of the physical port names used for LAN side connectivity	NFX250
LAN_MEMBER_PORT_NAMES	Specify the physical ports on the dual CPE device that are used on the link aggregation group (LAG) interface connecting to the LAN-side switch.	NFX250
GWR_CPU_PIN	Specify the physical CPUs to which the vCPUs of the vSRX (gateway router) should be pinned. **WARNING:** We recommend that you *do not modify* the preconfigured CPU pinning values because these values are set based on Juniper's performance tests.	NFX250
AUX_Subnets	Specify the IP subnets assigned to the three auxiliary ports on the gateway router to which VNFs can be attached.	NFX250
LAN_Subnets	Specify the IP subnets assigned to the two LAN ports on the gateway router to which VNFs can be attached.	NFX250

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
Login Security Settings		
Login idle timeout (minutes)	Enter the time (in minutes) after which a session that is idle is timed out.	NFX250
Login attempts before locking out	Enter the maximum number of unsuccessful login attempts allowed before the user account is locked. Range: 3 through 10.	NFX250
Login lockout period in minutes	Enter the period (in minutes) for which the user account should be locked. Range: 1 through 43,200 minutes	NFX250
Login backoff factor in seconds	Specify the delay (in seconds) after each failed login attempt, which increases for each subsequent login attempt after specified login backoff threshold. Range: 5 through 10.	NFX250
Login backoff threshold	Specify the threshold for the number of failed login attempts after which each subsequent login attempt is delayed by the time specified in the login backoff factor. Range: 1 through 3	NFX250
Maximum time to enter password in seconds	Enter the maximum time allowed (in seconds) to enter a password to log in to the device after entering your username. Range: 20 through 300 seconds.	NFX250
Maintenance user account	Enter the username of the user account to be used for maintenance activities (for example, troubleshooting) on the device.	NFX250

Table 67: Fields on the Template Settings Page for All Device Templates *(continued)*

Field Name	Description	Applicable To (Device Templates)
Login Announcement	Specify the system login announcement, which is displayed after a user successfully logs in to the device.	NFX250
Login Message	Specify the system login message, which is displayed before a user logs in to the device.	NFX250
ZTP_ENABLED	Specify whether to enable ZTP for the device.	SRX Series

Table 68: Fields on the Template Settings Page

Name	Description
Customer Parameters	
AUTO_DEPLOY_STAGE2_CONFIG	Specify whether to automatically deploy stage-2 configuration at the end of the Zero Touch Provisioning (ZTP) workflow. Example: Enabled
ZTP_ENABLED	Specify whether to enable ZTP for the device. **NOTE:** This option is supported on SRX Series Services Gateways only. Example: Enabled
PRE_STAGED_CPE	Specify whether the CPE device is pre-staged with WAN configuration. **NOTE:** This option is supported on SRX Series Services Gateways only. Example: Enabled
ACTIVATION_CODE_ENABLED	Specify whether the customer must use an activation code to activate the CPE device. Example: Enabled

Table 68: Fields on the Template Settings Page *(continued)*

Name	Description
OOB_OAM_Port	Specify the name of the port used for out-of-band Operation, Administration, and Maintenance (OAM) traffic. This port is used in deployments where OAM and data traffic are on separate physical ports. **NOTE:** This option is supported on SRX Series Services Gateways only. Example: fxp0
S2_MODEL_HUGEPAGE_COUNT	Specify the number of 1-GB huge pages to be used by the VNFs on an NFX250-S2 device with a total memory of 32 GB. Example: 21
USE_SINGLE_SSH_TO_NFX	Specify whether to enable device-initiated connections (outbound SSH) with port-forwarding capability. Port forwarding enables Contrail Service Orchestration to manage an NFX250 device through a single IP address. Example: Enabled
S1_MODEL_HUGEPAGE_COUNT	Specify the number of 1-GB huge pages to be used by the VNFs on an NFX250-S1 device with a total memory of 16 GB. Example: 21
VNF_OAM_TRANSLATED_PORT_START	Specify the first port number that can be used to expose a port on the gateway router's OAM or WAN interface through port translation. Use this option in cases where the VNF does not have its own OAM IP address from the in-band OAM network.
ENC_ROOT_PASSWORD	Specify the Junos OS root password to be set on an NFX250 device. Example: **********
WAN Port Names	Specify the mapping Junos OS interface descriptors for the hardware ports. The RJ-45 port is the default port for the NFX250 device. You can change the default port if you want to use a different type of connector, such as SFP.

Table 68: Fields on the Template Settings Page *(continued)*

Name	Description
GWR_LAN_PORT	Specify the mapping of the gateway router's LAN port names to the corresponding front panel physical port names on the NFX250 device. Currently, the logical ports are created on the ge-0/0/4 interface.
JCP_LAN_PORT_NAMES	Specify the port names from LAN_0 through LAN_9.
GWR_LAN_PORT_NAMES	Specify the port names from LAN_0 through LAN_9.
LAN_PORT_NAMES	Specify the port names from LAN_0 through LAN_10.
CONTROL_LINK_PORT_NAME	Enter the physical port name for control link connection. Example: xe-0/0/12
FAB_LINK_PORT_NAME	Enter the physical port name for fabric link connection. Example: xe-0/0/13
OOB_MGMT_ENABLED	Specify whether to use the out-of-band (OOB) management port of the device for management connectivity. If the field is enabled, a default route will be available through this interface. If the field is disabled, there is no connectivity through the OOB management port of the device and the stage-1 configuration that is generated will include a static default route.
AUTO_INSTALL_LICENSE_TO_DEVICE	Click the toggle button to enable automatic installation of the license on CPE device at the end of ZTP workflow.
AUTO_INSTALL_IDP_SIGNATURE_TO_DEVICE	Click the toggle button to automatically install the IDP signature on the device based on the applicable licenses installed on the device. IDP signature includes App ID. To install IDP signature on the device, you must ensure that a valid IDP license is uploaded to CSO. If a valid IDP license is not available, only the APP ID is installed. Therefore, you must also enable the AUTO_INSTALL_LICENSE_TO_DEVICE option.

Table 68: Fields on the Template Settings Page *(continued)*

Name	Description
AUTO_INSTALL_SIGNATURE_TO_DEVICE	Click the toggle button to automatically install the App ID signature on the device. If this option is disabled, CSO checks the device for pre-installed signatures and, if there are any, updates the signature database accordingly.
GWR_VSRX_IMAGE_LOCAL_FILE_PATH	Enter the local path of the vSRX image that is installed on the NFX250 device. The image file is required when the gateway router VM is created. If this parameter is not set, or if the file is not present on the NFX250 device, then a vSRX image is downloaded from the CSO file server to the NFX250 device. Example: ./var/third-party/images/*vsrx*-15.1X*.qcow2
GWR_VSRX_IMAGE_CNAME_IN_CSO	Enter the name of the vSRX image uploaded into the Image Management Service in CSO. When creating the gateway VM, if the vSRX image file is not present locally, then the image with this name is downloaded to the NFX250 device.
INTERNAL_OAM_SUBNET	Enter the IP address for the subnet that is used for internal OAM.
ADSL_VPI	Enter the Virtual Path Identifier (VPI) setting to connect to the ADSL service provider through PPPoE. Example: 8
ADSL_ENCAP	Enter the encapsulation that is used to connect to the ADSL service provider through PPPoA. Example: llcsnap-bridged-802.1q
ADSL_VCI	Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider through PPPoE. Example: 36
DSL_VLAN	Enter the reserved internal VLAN ID to be used as the native-vlan-id on xDSL ports to ensure that untagged control frames are processed. Example: 4087

Table 68: Fields on the Template Settings Page *(continued)*

Name	Description
CLUSTER_OFFSET	Enter the cluster slot number for designated secondary node.

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates

Field Name	Description
SSH Settings	
Prevent root login via SSH?	Click the toggle button to enable root login through SSH. Root login through SSH is disabled by default.
Restrict SSH access to be from CSO only	Click the toggle button to restrict SSH access only to connections from Contrail Service Orchestration (CSO). Default: Disabled
Max number of SSH connections allowed at any time	Enter the maximum number of concurrent SSH connections to be allowed. Range: 1 through 250 Default: 50
Max number of SSH connections allowed per minute	Enter the maximum number of SSH connections allowed per minute. Range: 1 through 250 Default: 50
Max number of sessions per SSH connection	Enter the maximum number of sessions per SSH connection. Range: 1 through 65535 Default: 50
Policer Settings	
Bandwidth limit for ICMP traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Internet Control Message Protocol (ICMP) traffic towards the device. Default: 1m

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
Burst-size limit for ICMP traffic towards the device	Enter the burst-size limit, in bytes, for ICMP traffic towards the device. Default: 2k
Bandwidth limit for trace-route traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for traceroute traffic towards the device. Default: 1m
Burst-size limit for trace-route traffic towards the device	Enter the burst-size limit, in bytes, for traceroute traffic towards the device. Default: 15k
Bandwidth limit for DHCP traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Dynamic Host Configuration Protocol (DHCP) traffic towards the device. Default: 1m
Burst-size limit for DHCP traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for DHCP traffic towards the device. Default: 15k
Bandwidth limit for DNS traffic towards the device	Enter the bandwidth limit, in bits per second (bps), for Domain Name System (DNS) traffic towards the device. Default: 1m
Burst-size limit for DNS traffic towards the device	Enter the burst-size limit, in bytes, for (DNS) traffic towards the device. Default: 15k
Log Rotation Settings	
Max size (MB) for log files	Enter the maximum size of the log file, in megabytes (MB). Default: 10

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
Max number of log files	Enter the maximum number of log files. Default: 10
Feature Level Access Settings	
Allow TACACS access	Click the toggle button to enable TACACS communication. By default, TACACS communication is disabled.
Allow SNMP access	Click the toggle button to enable SNMP communication. By default, SNMP communication is disabled.
Customer Parameters	
WAN_FPC_SLOT	Enter the FPC slot number. For SRX4100 and SRX4200 devices, the value is 0. For SRX4600 devices, the value is 1.
AUTO_INSTALL_LICENSE_TO_DEVICE	Click the toggle button to enable automatic installation of the license file on the CPE device when the ZTP workflow ends. Default: Disabled
AUTO_INSTALL_DEFAULT_TRUSTED_CERTS_TO_DEVICE	Click the toggle button to disable automatic installation of default trusted certificates on the CPE device when the ZTP workflow ends. Default: Enabled
ENC_ROOT_PASSWORD	Specify the Junos OS-encrypted root password to be set on the CPE device.
ACTIVATION_CODE_ENABLED	Click the toggle button to enable the tenant to use an activation code to activate the CPE device. Default: Disabled
CLUSTER_OFFSET	Enter the cluster slot number for designated secondary node.

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
AUTO_DEPLOY_STAGE2_CONFIG	Click the toggle button to enable automatic deployment of stage-2 configuration when the ZTP workflow ends. Default: Disabled
OOB_OAM_PORT	Enter the port number for out-of-band Operation, Administration, and Maintenance (OAM) traffic. This port is used in deployments where OAM and data traffic are on separate physical ports. **NOTE:** This option is supported only on SRX Series Services Gateways. Default: fxp0
MAX_DVPN_TUNNELS_ON_SITE	Enter the maximum number of site to site dynamic mesh tunnels that can be created at a site, exceeding which the site to site tunnels are not created any more and traffic goes through the hub.
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE	Enter the minimum number of site-to-site dynamic mesh tunnels that must be present at a site to start deactivating the inactive site-to-site tunnels.

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
WAN_PORT_NAMES	Specify the mapping of the physical or logical port names used for WAN side connectivity. You specify logical port names if you want to configure more than one WAN link on the same physical interface. The WAN links are connected from the same physical interface to the Provider Edge (PE) nodes through logical sub-interfaces with VLAN separation. WAN_0 WAN_1 WAN_2 WAN_3 Use the following naming convention for the ports on the primary node: xe-*WAN_FPC_SLOT*/0/*port-number* The *WAN_FPC_SLOT* value is 0 for SRX4100 and SRX4200 devices and the value is 1 for SRX4600 devices.

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
WAN_MEMBER_PORT_NAMES	In case of dual CPE devices, specify the mapping of the physical or logical port names used for WAN side connectivity. You specify logical port names if you want to configure more than one WAN link on the same physical interface. The WAN links are connected from the same physical interface to the Provider Edge (PE) nodes through logical sub-interfaces with VLAN separation. WAN_0 WAN_1 WAN_2 WAN_3 Use the following naming convention for the ports on the secondary node: xe-*WAN_FPC_SLOT+CLUSTER_OFFSET*/0/*port-number*
LAN_PORT_NAMES	Enter the name of the physical interfaces for the ports that are used to connect to LAN side devices. LAN_0— xe-0/0/0 LAN_1— xe-0/0/1 LAN_2— xe-0/0/2 LAN_3— xe-0/0/3 LAN_4— xe-0/0/4 LAN_5— xe-0/0/5 LAN_6— xe-0/0/6 LAN_7— xe-0/0/7

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
LAN_MEMBER_PORT_NAMES	In case of dual-CPE devices, enter the name of the physical interfaces for the ports that are used to connect to LAN side switch. LAN_0_0— xe-0/0/2 LAN_0_1— xe-0/0/3 LAN_0_2— xe-0/0/4 LAN_0_3— xe-0/0/5
Login Security Settings	
Idle timeout (minutes)	Enter the maximum time (in minutes) that a session can be idle before the user is logged out of the system.
Attempts before locking out	Enter the maximum number of unsuccessful login attempts allowed before the account is locked. Range: 3 to 10
Lockout period in minutes	Enter the number of minutes an account must remain locked after the maximum number of unsuccessful login attempts. Range: 1 to 43,200
Backoff factor in seconds	Enter the length of delay (in seconds) after each failed login attempt. The length of delay increases by this value for each subsequent login attempt after the value specified in the backoff-threshold option. Range: 5 to 10
Backoff threshold	Enter the threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password. Range: 1 to 3

Table 69: Fields on the Template Settings Page for SRX4100, SRX4200, and SRX4600 Device Templates *(continued)*

Field Name	Description
Maximum time to enter password in seconds	Enter the maximum time allowed (in seconds) to enter a password to log in to the device after entering your username. Range: 20 to 300.
Maintenance user account	Enter the name of a maintenance user account to be created on the device. The maintenance user account is used by maintenance personnel for troubleshooting when required.
Announcement	Enter the system login announcement, which is displayed after a user successfully logs in to the device.
Message	Enter the system login message, which is displayed when a user logs into the device.
RESERVED_MEMBER_PORT_NAMES	Enter the port names of the two 1-Gigabit Ethernet/10-Gigabit Ethernet ports,(CTL (control port) and FAB (fabric port)) to be used for synchronizing data and maintaining state information in a chassis cluster setup. • PORT_0_0— xe-0/0/6 • PORT_0_1— xe-0/0/7
RESERVED_SUBNETS	Enter the IP address of reserved subnets that is used for System logs. • NODE_0— 10.10.12.0/24 • NODE_1— 10.10.13.0/24

Table 70: Fields on the Template Settings Page for SRX and NFX150 Platform Templates

Name	Description
Customer Parameters	
IMAGE_UPGRADE_TIME	Enter the time required to upgrade the image on a device during the bootstrap process.

Table 70: Fields on the Template Settings Page for SRX and NFX150 Platform Templates *(continued)*

Name	Description
MGMT_ZONE	Enter the zone for the management interface. This field is required only if ZTP is disabled.
BOOTSTRAP_TIME	Enter the time required for the bootstrap process (excluding the time for image upgrade).
ADSL_VPI	Enter the Virtual Path Identifier (VPI) setting to connect to the asymmetric digital subscriber line (ADSL) service provider through PPPoE.
ADSL_VCI	Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider through PPPoE.
ENC_ROOT_PASSWORD	Specify the Junos OS root password to be set on the device.
AUTO_INSTALL_LICENSE_TO_DEVICE	Click the toggle button to enable automatic installation of the license on CPE device at the end of the ZTP workflow.

Table 71: Fields on the Template Settings Page for Dual SRX Platform Template

Name	Description
Customer Parameters	
ADSL_VPI	Enter the Virtual Path Identifier (VPI) setting to connect to the asymmetric digital subscriber line (ADSL) service provider through PPPoE.
BOOTSTRAP_TIME	Enter the time required for the bootstrap process (excluding the time for image upgrade).
ADSL_VCI	Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider through PPPoE.
IMAGE_UPGRADE_TIME	Enter the time required to upgrade the image on a device during the bootstrap process.
ZTP_ENABLED	Click the toggle button to enable ZTP.
ENC_ROOT_PASSWORD	Specify the Junos OS root password to be set on the device.
MGMT_ZONE	Enter the zone for the management interface. This field is required only if ZTP is disabled.

Table 71: Fields on the Template Settings Page for Dual SRX Platform Template *(continued)*

Name	Description
CLUSTER_OFFSET	Enter the cluster slot number for the secondary node.
FAB_LINK_PORT_NAMES	
Device Model	Select the device model.
FAB Link Port	Enter the name of the fabric link and the associated interface.

RELATED DOCUMENTATION

About the Device Template Page | 194

Updating Stage-2 Configuration Template in a Device Template

Each device template has a set of configuration templates that can be used to deploy additional configuration on to the CPE device after it is activated. These templates are known as stage-2 configuration templates. You can add or remove stage-2 configuration templates from a device template.

NOTE: By default, the CPE device configuration is not supported on the CPE device. If you need the CPE device configuration, then you must configure it through stage-2 configuration in the device templates.

To add a stage-2 configuration template:

1. Select **Resources > Templates > Device Template**.

   The Device Templates page appears.

2. Select a device template for which you want to add the stage-2 configuration and select **Edit Device Template > Stage-2 Config Templates**.

   The Stage-2 Configuration Templates page appears. Table 72 on page 225 lists the fields (and their descriptions) on the Stage-2 Configuration Templates page.

3. Click the add icon (+) and complete the configuration settings according to the guidelines provided in Table 73 on page 226.

4. Click **Save**.

   The new stage-2 configuration template is included in the device template.

Table 72: Fields on the Stage-2 Configuration Templates Page

Name	Description
Name	View the name of the stage-2 configuration template. Example: LAN side config
Component Name	View the name of the component through which the settings are configured. The components that are currently supported are: • JUNOS—Supported only on SRX Series Services Gateway. • Juniper Device Manager (JDM)—Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. Example: JUNOS
Hide	Displays whether the template is hidden on Customer Portal. • true—Template is not visible on Customer Portal. • false—Template is visible on Customer Portal. Example: false
Copy input from	Displays the template from which you copied the settings.
Auto Deploy	Displays whether the stage-2 configuration is automatically pushed to the device during ZTP process.

Table 72: Fields on the Stage-2 Configuration Templates Page *(continued)*

Name	Description
Enable for	Displays whether the stage-2 configuration template is enabled for all tenants, no tenants, or specific tenants.

Table 73: Fields on the Add New Template Page

Name	Description
Template	Select the configuration template from the drop-down list. The configuration templates are designed in the Configuration Designer tool. Example: srx-basic-sdwan-cpe-config
Display Name	Specify the name of the template that you want to display on the configuration interface. Example: SDWAN Config
Component Name	Specify the component name through which the settings are configured. The components that are currently supported are: • JUNOS—Supported on SRX Series Services Gateway. • Juniper Device Manager (JDM)— Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. Example: JUNOS
Hide	Specify whether you want to hide the configuration template on Customer Portal. You might want to choose to hide the template if you are reusing the template for multiple components. • hide—White dot on right with blue background. • show—White dot on left with gray background. Example: hide

Table 73: Fields on the Add New Template Page *(continued)*

Name	Description
Copy From Template	If you have chosen to hide the configuration template on the user interface, then specify the template from which you want to copy the settings. Example: srx-mis-lan-to-wan-config
Auto Deploy	Specify whether the stage-2 configuration must be automatically pushed to the device during ZTP process. The available options are • Same as global settings • Yes • No
Enabled for	You can enable the stage-2 configuration template for all tenants, specific tenants, an SP administrator or an OpCo administrator. **NOTE:** Only users with SP administrator or OpCo administrator role can enable stage-2 configuration templates. The available options are: • **All Tenants**—Select this option to enable stage-2 configuration template for all tenants. Both SP and OpCo administrators can view templates for all tenants by switching the scope to the specific tenant. By default, stage-2 configuration templates assigned to all tenants are automatically applied to any new tenant. • **No Tenants**—Select this option to enable stage-2 configuration template for an SP administrator or an OpCo administrator. An SP administrator can modify the stage-2 configuration template. An OpCo administrator cannot modify the stage-2 configuration template. However, an OpCo administrator can clone the stage-2 configuration template and then modify the template. • **Selective Tenants**—Select this option to enable stage-2 configuration template for specific tenants. A tenant administrator can view and manage stage-2 template for a specific tenant. When you select the **Selective Tenants** option, the **Tenants** section is displayed. Select one or more tenants. Click the greater-than icon (>) to move the selected tenant or tenants from the **Available** column to the **Selected** column. You can use the search icon on the top right of each column to search for tenant names. The default option is All Tenants.

To remove a stage-2 configuration template:

1. Select **Resources > Templates > Device Templates**.

   The Device Templates page appears.

2. Select the device template for which you want to remove the stage-2 configuration and then select **Edit Device Template > Stage-2 Config Templates**.

   The Stage-2 Config Templates page appears.

3. Select a configuration template and click the delete icon (X).

   A page requesting confirmation for the deletion appears.

4. Click **Yes** to confirm that you want to delete the stage-2 configuration template.

   The configuration template is deleted.

Configuring Stage-2 Initial Configuration in a Device Template

In general, the tenant administrators initiate stage-2 configuration through Customer Portal. However, in certain cases, the same stage-2 configuration needs to be deployed to CPE devices in all sites that are activated using a specific device template. In such cases, you can attach an initial configuration to a stage-2 configuration template of a device template. When a new CPE device in the site is activated using the device template, the initial configuration is automatically deployed to the CPE device.

The list of initial configurations that are supported are:

- Policies configuration
- LAN configuration
- SD-WAN configuration
- Routing configuration
- APN configuration

To update an initial configuration for stage-2 configuration template:

1. Select **Resources > Templates > Device Templates**.

   The Device Templates page appears.

2. Select the device template for which you want to configure the stage-2 configuration and then select **Edit Device Template > Stage-2 Initial Config**.

   The Stage-2 Initial Configuration page appears, listing the existing settings.

3. Complete the configuration settings according to the guidelines provided in Table 74 on page 229, Table 75 on page 230, and Table 76 on page 230 and Table 77 on page 231.

4. Click **Ok**.

Table 74: Fields for the VLAN Settings on the Stage-2 Initial Configuration Page

Field	Description
VLAN ID	Specify the identifier for the Layer 2 VLAN for the CPE device. Example: 230

Table 74: Fields for the VLAN Settings on the Stage-2 Initial Configuration Page *(continued)*

Field	Description
IRB IP Prefix	Specify the IP address, including the subnet prefix, and the integrated routing and bridging (IRB) interface on the CPE device. Example: 192.0.2.15/24
LAN Ports	Specify the LAN ports on the CPE device. Example: ge-0/0/0

Table 75: Fields for the LAN Settings on the Stage-2 Initial Configuration Page

Field	Description
LAN port	Specify the LAN ports on the CPE device. Example: ge-0/0/0
IP Address	Specify the IP address on the CPE device. Example: 192.0.2.255

Table 76: Fields for the SRX Basic SD-WAN Settings on the Stage-2 Initial Configuration Page

Field	Description
Manage App Group	Click to manage the application groups. The application group is predefined in the system for all SRX Series and vSRX configuration settings. The settings are preloaded and displayed on the portal. You can also create new application groups.
Manage App SLA Profile	Click to manage the application service-level agreements (SLA) profiles.
Rule Name	Specify the rule name. Example: critical-apps
Application/Groups	Specify the applications or application groups for the rule. Example: Oracle, SAP
Application SLA Profile	Specify the application SLA profile for the rule. Example: critical-apps

Table 77: Fields for the APN Configuration Settings on the Stage-2 Initial Configuration Page

Field	Description
Use default APN settings	Click the toggle button to change the default APN settings. • Enabled—Select this option to use the default APN setting that is shipped along with the CPE device. This is the default option. • Disabled—Select this option to configure the APN settings.
APN Settings	
APN Name	Enter the access point name (APN) of the gateway router.
SIM Change Required	Click the toggle button to change the SIM card. You change the SIM card either to use a different LTE service provider or to use a private APN with the current LTE service provider. • Enabled—Select this option to change the APN settings and to use a new SIM card. This is the default option. • Disabled—Select this option to change the APN settings without changing the SIM card.
Authentication Method	Select the authentication method for the APN configuration. • PAP— Select to use Password Authentication Protocol (PAP) authentication. This is the default option. • CHAP— Select to use Challenge Handshake Authentication Protocol (CHAP) authentication. • None—Select to indicate that there is no authentication method.
Authentication Information	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication.
SIP Password	Enter the SIP password for authentication.

RELATED DOCUMENTATION

About the Device Template Page | 194

Modifying a Device Template Description

The device template description provides a brief overview about the supported platform, tenant, site, deployment model, and additional features supported through the template.

To modify the description of the device template:

> **NOTE:** An OpCo Administrator cannot edit a default device template.

1. Select the device template that you want to modify, and click the edit icon.

   The Edit Device template page appears.

2. Enter a meaningful description for the device template. For example: NFX250 deployed as a CPE device with SD-WAN capability.

3. Click **Ok** to save the changes.

   The description that you updated is listed in the device template table.

RELATED DOCUMENTATION

About the Device Template Page | 194

Deleting a Device Template

Before deleting a device template, ensure that the template is not associated with any tenant site or a CPE device.

> **NOTE:** An OpCo Administrator cannot delete a default device template.

To delete a device template file:

1. Select **Resources > Templates > Device Templates**.

   The Device Template page appears.

2. Select the device template that you want to delete and click **Delete**.

   A page requesting confirmation for the deletion appears.

3. Click **Yes** to confirm that you want to delete the device template.

   The device template is deleted.

RELATED DOCUMENTATION

About the Device Template Page | 194

Configuration Templates Overview

Contrail Service Orchestration (CSO) offers a fully automated, end-to-end provisioning of customer premises equipment (CPE) devices. CSO utilizes configuration templates to provision parameters to enable the onboarding and configuration of Juniper Networks devices throughout the device lifecycle. Configuration templates (referred to as stage-2 templates in releases before CSO Release 5.1.0) also enable you to deploy customized configurations on devices that are managed by CSO. In short, configuration templates enable you to make configuration changes to Juniper devices by using the CSO GUI.

Configuration changes can be of two types:

- Global, which refers to configurations are common to all devices; for example, syslog or SNMP settings.
- Device-specific, which refers to configurations are unique for each device; for example, BGP configuration.

You can use configuration templates to push global (common) configurations to all devices or to specific devices.

By default, CSO provides predefined configuration templates that are pre-assigned to device templates. You can also create your own templates by importing a template, cloning a template and modifying its settings, or adding a template. Templates can be created by users with different roles. The availability of the templates is determined by the role of the user who created the template:

- Templates created by the SP Administrator (CSO on-premises version) users, are available to operating companies (OpCos), the OpCo's tenants, and the SP Administrator's tenants.
- Templates created by the OpCo Administrator users are available only to the OpCo and the OpCo's tenants.
- Templates created by the Tenant Administrator users are available only to the tenant.

You can either attach (assign) a configuration template to a device template, which enables the configuration to be deployed on devices which use that device template, or you can deploy a configuration template directly on a device.

TIP: In CSO, you may encounter the terms stage-1 and stage-2 configuration, which refer to the following:

- Stage-1 configuration is the initial configuration (pushed to the device) that allows CSO basic connectivity to a device.
- Stage-2 configuration is the configuration that CSO pushes to the device *after* the device connects with CSO.

Benefits

- Configuration templates provide a mechanism to create customized configurations and push the configurations to one or more devices, which enables you to deploy configurations beyond the standard configuration templates provided in CSO.

RELATED DOCUMENTATION

Configuration Templates Workflow | 234

Configuration Templates Workflow

Read the "Configuration Templates Overview" on page 233 topic to gain a basic understanding of configuration templates.

In Administration Portal, users with the SP (Service Provider) Administrator role (CSO on-premises only) or OpCo (Operating Company) Administrator role can perform the configuration template workflow tasks indicated in this topic.

The high-level workflow for configuration templates is as follows:

1. You can use a pre-existing template (skip to step 2) or create a new template using one of the following methods:
   - Import a configuration template by specifying the template configuration file (Jinja syntax), Yang model file, and the Viewdef file. For more information, see "Import Configuration Templates" on page 255.
   - Clone an existing configuration template and modify the cloned template. For more information, see "Edit, Clone, and Delete Configuration Templates" on page 243.
   - Add a configuration template by specifying the template configuration and logic. For more information, see "Add Configuration Templates" on page 261.
2. (Optional) Although this is an optional step, we recommend that you validate the configuration template by using the preview workflow *before* attaching the configuration template to a device template or deploying the configuration template directly on a device. For more information, see "Preview and Render Configuration Templates" on page 254.
3. You can assign a configuration template to a device template from the Configuration Templates or the Device Templates pages. This enables you to deploy additional configuration on the device during zero touch provisioning (ZTP) and after the device is activated. For more information, see "Assign Configuration Templates to Device Templates" on page 258 and "Updating Stage-2 Configuration Template in a Device Template" on page 224.
4. You can deploy a configuration template directly on one or more devices that were previously activated, which enables you to deploy templates that were added after a device was activated or to deploy additional configuration to devices. You can deploy configuration templates to devices from the Configuration Templates or Tenant Devices pages. For more information, see "Deploy Configuration Templates to Devices" on page 246.
5. (Optional) Dissociate or undeploy configuration templates:
   - You can dissociate a configuration template from a device, which remove the references to the configuration template from the device, but retains the configuration already deployed on the device. For more information, see "Dissociate a Configuration Template from a Device" on page 253.
   - You can undeploy the configuration template, which deletes the configuration previously deployed on the device, but retains the references to the configuration template. For more information, see "Undeploy a Configuration Template from a Device" on page 251.

RELATED DOCUMENTATION

About the Configuration Templates Page | 236

Jinja Syntax and Examples for Configuration Templates | 271

About the Configuration Templates Page

IN THIS SECTION

- Tasks You Can Perform | 236
- Field Descriptions | 237

To access this page, click **Resources > Templates > Configuration Templates** in Administration Portal.

You can use the Configuration Templates page to view and manage configuration templates.

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

Tasks You Can Perform

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can perform the following tasks from this page, while users with operator roles only have read capabilities.

- Clone a configuration template—"Edit, Clone, and Delete Configuration Templates" on page 243.
- Deploy a configuration template on one or more devices—See "Deploy Configuration Templates to Devices" on page 246.
- Preview and render a configuration template—See "Preview and Render Configuration Templates" on page 254.
- View the details a configuration template—Select a configuration template and click **More** > **Template Details** or mouse over the configuration template click the Detailed View icon. The Detail for *Template-Name* pane appears on the right side of the page. See Table 79 on page 238 for an explanation of the fields.
- Import a configuration template—See "Import Configuration Templates" on page 255.
- Export a configuration template—See "Export a Configuration Template" on page 257.

- Assign a configuration template to a device template—See "Assign Configuration Templates to Device Templates" on page 258.
- Add a configuration template—See "Add Configuration Templates" on page 261.
- Edit or delete configuration templates—See "Edit, Clone, and Delete Configuration Templates" on page 243.
- View the configuration deployed on one or more devices—See "View the Configuration Deployed on Devices" on page 283.
- Search for configuration templates by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort configuration templates—Click a column name to sort the configuration templates based on the column name.

  NOTE: Sorting and filtering is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Configuration Templates page.

Field Descriptions

Table 78 on page 237 displays the description of the fields on the Configuration Templates page and Table 79 on page 238 displays the description of the fields on the Detail for *Template-Name* Pane.

Table 78: Fields on the Configuration Templates Page

Field	Description
Name	Name of the configuration template.
Family	Device family to which the configuration template belongs.
Deployed Devices	Number of devices on which the configuration template was deployed. If the configuration template is not yet deployed on any devices then a blank cell is displayed. Click the ***number-of-devices*** link to view the configuration (for that configuration template) deployed on devices. See "View the Configuration Deployed on Devices" on page 283
Description	Description of the configuration template.
Last Updated	Date and time on which the template was last updated.

Table 78: Fields on the Configuration Templates Page *(continued)*

Field	Description
Owner	Depending on who added the configuration template, displays the following: • **System**—If the template is predefined or added by the Service Provider administrator • ***OpCo-Name***—Name of the Operating Company (OpCo) if the template is added by an OpCo administrator.

Table 79: Fields on the Detail for <Template-Name> Pane

Field	Description
General tab	
Name	See Table 78 on page 237.
Description	See Table 78 on page 237.
Family	See Table 78 on page 237.
Format	Format used by the configuration template: • CLI • XML (Extensible Markup Language)
Details tab	**NOTE:** If you want to add a new configuration template based on an existing one, you can copy the three files from the Details tab, modify the files as needed, and use the Import Configuration Template page to import a new template.
Jinja Template	Displays the configuration in Jinja Template language syntax.
Data Model	Displays the Yang data model (configuration schema).
View Def	Displays the View Def (GUI configuration).

RELATED DOCUMENTATION

Device Template Overview | 188

Predefined Configuration Templates

Contrail Service Orchestration (CSO) provides predefined configuration templates that you can access from the Configuration Templates page (**Resources > Configuration Templates**).

Predefined configuration templates are available for SRX Series, NFX150, and NFX250 devices:

- Table 80 on page 239 lists the predefined configuration templates for SRX Series and NFX Series (NFX150 and NFX250) devices.
- Table 81 on page 240 lists the predefined configuration templates for SRX Series devices.
- Table 82 on page 241 lists the predefined configuration templates for NFX150 devices.
- Table 83 on page 242 lists the predefined configuration templates for NFX250 devices.

Table 80: Predefined Configuration Templates for SRX Series and NFX Series (NFX150 and NFX250) Devices

Name	Description
common-banner	Configure the banner that appears when you log in to an SRX or NFX Series device.
common-disable-auto-negotiation	Disable Ethernet autonegotiation on the interfaces of an SRX or NFX Series device. If you disable Ethernet autonegotiation, you must configure values for link mode and link speed when you deploy the template.
common-dns	Configure Domain Name System (DNS) server settings on an SRX or NFX Series device.
common-firewall-filters	Configure firewall filters that determine whether to allow or deny traffic before it enters or exits a port to which the firewall filter is applied.
common-idp-sensor-packet-log	Configure an SRX or NFX Series device for packet capture, by defining the amount of memory to be allocated for packet capture and the maximum number of sessions that can generate packet capture data for the device at a time.
common-lacp	Configure link aggregation control protocol (LACP) on an SRX or NFX Series device.
common-local-user	Configure a local user on an SRX or NFX Series device.
common-nat-global-settings	Configure network address translation (NAT) settings (such as pool utilization alarms, port randomization, and so on) on an SRX or NFX Series device.

Table 80: Predefined Configuration Templates for SRX Series and NFX Series (NFX150 and NFX250) Devices *(continued)*

Name	Description
common-ntp	Configure Network Time Protocol (NTP) settings on an SRX or NFX Series device.
common-password-config	Change the default password for a root user on an SRX or NFX Series device.
common-pre-id-default-policy	Configure the default policy action that occurs prior to dynamic application identification (AppID). During the initial policy lookup phase, which occurs prior to a dynamic application being identified, if there are multiple policies present in the potential policy list, an SRX or NFX Series device applies the default security policy until a more explicit match is found.
common-sdwan-dhcprelay	Configure extended DHCP relay and DHCPv6 relay options on an SRX or NFX Series device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
common-service	Configure the FTP, SSH, and NETCONF settings on an SRX or NFX Series device.
common-snmp-config-basic	Configure basic SNMP version 2 (SNMPv2) parameters on an SRX or NFX Series device.
common-static-routes	Configure static routes to be installed in the routing table for an SRX or NFX Series device. You can specify one or more routes within a single static statement, and you can specify one or more static options in the configuration. For more information, see static (Routing Options).
common-syslog	Configure syslog settings on an SRX or NFX Series device.
common-UTM-global	Configure the routing instance, on an SRX or NFX Series device, through which the DNS server can be reached to resolve the unified threat management (UTM) Web filtering URL.

Table 81: Predefined Configuration Templates for SRX Series Devices

Name	Description
ngfw-ipsec-vpn	Configure IPsec VPN settings for an SRX next-generation firewall (NGFW) device.

Table 81: Predefined Configuration Templates for SRX Series Devices *(continued)*

Name	Description
srx-dhcp	Configure an SRX Series device as a Dynamic Host Configuration Protocol (DHCP) server.
srx-dns	Configure Domain Name System (DNS) server settings on an SRX Series device.
srx-hub-breakout-stage2-config	Use this template to configure NAT on WAN links of provider hubs for breakout traffic. You can configure NAT on provider hubs with DATA_ONLY and OAM_AND_DATA capabilities. The configuration template can be applied per tenant provided, the tenant has at least one branch site connected to the provider hub configured for NAT. **NOTE:** You can configure NAT using the template only on existing WAN links and not on additional WAN links later added by tenants. Interface-based source NAT is used as the tunnel in the NAT configuration template.
srx-sdwan-dhcp-relay	Configure extended DHCP relay and DHCPv6 relay options on an SRX Series device and enable the device to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
srx-sdwan-mgmnt	Configure the SNMP version 3 (SNMPv3), NTP, syslog, and TACACS parameters for managing an SRX Series device. For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the **Allow TACACS Access** and **Allow SNMP Access** toggle buttons in the associated device template.
srx-vrrp	Configure virtual router redundancy protocol (VRRP) on an SRX Series device.

Table 82: Predefined Configuration Templates for NFX150 Devices

Name	Description
nfx3-sdwan-mgmnt	Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing an NFX150 device. For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the **Allow TACACS Access** and **Allow SNMP Access** toggle buttons in the associated device template.

Table 83: Predefined Configuration Templates for NFX250 Devices

Name	Description
nfx-cluster-sdwan-gwr-dhcprelay	Configure extended DHCP relay and DHCPv6 relay options on an NFX250 cluster and enable the cluster to function as a DHCP relay agent. A DHCP relay agent forwards DHCP Request and DHCP Reply packets between a DHCP client and a DHCP server.
nfx-sdwan-gwr-mgmnt	Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the gateway router (vSRX) on an NFX250 device. For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the **Allow TACACS Access** and **Allow SNMP Access** toggle buttons in the associated device template.
nfx-sdwan-jcp-mgmnt	Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the Junos Control Plane (JCP) component of an NFX250 device. For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the **Allow TACACS Access** and **Allow SNMP Access** toggle buttons in the associated device template.
nfx-sdwan-jdm-mgmnt	Configure the SNMPv3, NTP, syslog, and TACACS parameters for managing the Juniper Device Manager (JDM) component of an NFX250 device. For TACACS and SNMPv3 settings to work on the device on which you are deploying the configuration template, you must enable the **Allow TACACS Access** and **Allow SNMP Access** toggle buttons in the associated device template.

RELATED DOCUMENTATION

About the Configuration Templates Page | 236

Edit, Clone, and Delete Configuration Templates

IN THIS SECTION

- Edit a Configuration Template | 243
- Clone a Configuration Template | 244
- Delete a Configuration Template | 245

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can modify the parameters of existing configuration templates, clone existing configuration templates, and delete configuration templates that are no longer being used.

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

Edit a Configuration Template

Users with the SP Administrator role can edit predefined templates and templates that they created. Users with the OpCo role can edit only the templates that they added (created).

To edit a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want to modify and click the edit (pencil) icon.

   The Edit Configuration Template page appears. The fields on this page are same as the fields that you configure in the Add Configuration Template workflow.

3. Modify the fields as needed.

   Refer to "Add Configuration Templates" on page 261 for an explanation of the fields.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   The modifications are saved and you are returned to the Configuration Templates page, where a confirmation message is displayed. If the configuration template was previously deployed on a device or assigned to a device template, then you must redeploy the configuration template for the changes to take effect.

Clone a Configuration Template

To clone a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want to clone and click **Clone**.

   - If you select a configuration template that was added in CSO Release 5.3.0, the Clone Configuration Template page appears. Proceed to Step 3.
   - If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

     a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

        The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

     b. Select the template again and click **Clone**.

        The Clone Configuration Template page appears.

3. In the **Template Name** field, enter a unique template name that can only contain alphanumeric characters and hyphens up to a maximum of 64 characters.

4. Click **OK**.

You are returned to the Configuration Templates page and a confirmation message appears at the top of the page indicating the status of the clone operation.

After a template is cloned successfully, you can modify the template if needed. See the preceding section for details.

Delete a Configuration Template

To delete a configuration template:

NOTE:

- You cannot delete predefined configuration templates.
- You can delete a configuration template only if the following conditions hold good:
  - You added (created) the template.
  - The template is not assigned to a device template.
  - The template is not deployed on a device.

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want to delete and click the **X** (delete) icon.

   You are asked to confirm the delete operation.

3. Click **Yes**.

   You are returned to the Configuration Templates page and a popup appears indicating whether the deletion was successful or not.

RELATED DOCUMENTATION

Preview and Render Configuration Templates | 254

Deploy Configuration Templates to Devices

IN THIS SECTION

- Deploy from the Configuration Templates Page | 246
- Deploy from the Tenant Devices Page | 250

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can deploy a configuration template directly on one or more devices that were previously activated. This enables you to deploy configuration templates added after a device was activated or to deploy additional configuration to devices.

You can deploy configuration templates to devices from the Configuration Templates or Tenant Devices pages.

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

Deploy from the Configuration Templates Page

To deploy a configuration template to one or more devices:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want deploy and click **Deploy to Devices**.

   - If you select a configuration template that was added in CSO Release 5.3.0, the Deploy Template *Template-Name* To Devices page appears. Proceed to Step 3.
   - If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

   The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

b. Select the template again and click **Deploy to Devices**.

   The Deploy Template *Template-Name* To Devices page appears.

3. Complete the configuration according to the guidelines provided in Table 84 on page 247.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   The settings that you entered are saved and you are returned to the Configuration Templates page. A confirmation message appears indicating that a job was created. For each device, a separate job is triggered to deploy the configuration.

   You can view the status of the jobs from the Jobs page (**Monitor > Jobs**).

Table 84: Deploy Template <Template-Name> To Devices Settings

Setting	Guideline
Select Devices	
Configuration Template	Displays the name of the configuration template that you are deploying; you cannot modify this field.
Component Name	This field is displayed only for NFX250 devices. Select the component of the NFX250 device on which to deploy the template: • JCP—Junos Control Plane • JDM—Junos Device Manager • GWR-Gateway Router

Table 84: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Devices	You can specify the devices on which you want to deploy the configuration template in the following ways: • By adding the devices manually: 1. From the list of devices displayed, select one or more devices by clicking the check box next to each device name. **NOTE:** You can search for devices or filter the list of devices displayed. • By uploading a comma-separated values (CSV) file containing the device information: **NOTE:** You must ensure that the CSV file is in the format that CSO can read and that the number of device records is 200 or lower. You can download a sample file by clicking the **Download Sample CSV File** button. 1. Click **Upload CSV File**. The Upload CSV File page appears. 2. Click **Browse** to open the file selection dialog, select a file, and click **Open**. The name of the file that you selected is displayed in the CSV File field. 3. Click **OK**. You are returned to the previous page where the devices that you imported are selected and displayed in the table. Click **Next**. You are taken to the Configure Global Parameters or the Configure Device Parameters tab.
Configure Global Parameters	**NOTE:** This tab is displayed only if the configuration template contains parameters that are global in scope. Specify the global parameters that are common to all the devices that you selected in the preceding step. After you are done, click **Next**. You are taken to the Configure Device Parameters tab.
Configure Device Parameters	

Table 84: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Devices	The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default. For each device, the device name, device family, operational status, and the configuration status are displayed. When you first arrive on this tab, the configuration status for each device is *Not configured*. The *Device-Name* Parameters pane on the right displays the input parameters (from the configuration template) that you can specify for each device. After you specify the values for one device, you can select a different device and enter the configuration values. • If the configuration template contains validations for the parameters, CSO validates the values you entered for the device and changes the configuration status to Valid and displays a green check mark (√). • If the configuration template does not contain any validations, CSO changes the configuration status to Valid and displays a green check mark (√). • If the values that you entered do not match the validation, the configuration status displays Invalid. **NOTE:** You can optionally delete a device by selecting the device and clicking the delete (trash can) icon. After you specify the input parameter values for all the devices and ensure that the configuration status of all devices is Valid, click **Next**. You are taken to the Summary tab.
Summary	
Devices	The devices that you selected in the preceding step are displayed in the Devices table, and the first device is selected by default. For each device, the device name, device family, and operational status are displayed. For each device, the *Device-Name* Configuration pane on the right displays the actual configuration that will be deployed on the device. After you review the configuration for all the devices, click **Next**. You are taken to the Deploy tab.
Deploy	

Table 84: Deploy Template <Template-Name> To Devices Settings *(continued)*

Setting	Guideline
Deployment Schedule	Specify whether the configuration should be deployed on devices immediately(**Deploy now**) or deployed later (**Deploy later**). If you choose to deploy the configuration later, you must enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the deployment to occur.

Deploy from the Tenant Devices Page

To deploy a configuration template to one or more tenant devices:

1. Select **Resources > Tenant Devices**.

   The Tenant Devices page appears.

2. Select one or more devices on which you want deploy and click **More > Deploy Configuration Template**.

   NOTE: The devices that you select must belong to the same device family. If you select devices from different device families, CSO displays an error message.

   The Deploy Template to Device *Device-Name* page appears.

3. From the **Configuration Templates** table, select the configuration template that you want to deploy and click **Next**.

   The configuration templates displayed are filtered based on the device family of the devices that you selected.

   - If you select a configuration template that was added in CSO Release 5.3.0, proceed to Step 4.
   - If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

     a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

        The template is automatically upgraded to CSO Release 5.3.0 and the Tenant Devices page appears.

b. Select the device again and click **More > Deploy Configuration Template**.

The Deploy Template to Device *Device-Name* page appears.

4. The rest of the deploy workflow is the same as you encounter if you initiate the deployment from the Configuration Templates page. Complete the configuration according to the guidelines provided in Table 84 on page 247.

> **NOTE:** Fields marked with an asterisk (*) are mandatory.

5. Click **OK**.

The settings that you entered are saved and you are returned to the Tenant Devices page. A confirmation message appears indicating that a job was created. For each device, a separate job is triggered to deploy the configuration.

You can view the status of the jobs from the Jobs page (**Monitor > Jobs**).

RELATED DOCUMENTATION

Assign Configuration Templates to Device Templates | 258

Undeploy a Configuration Template from a Device

As an SP (Service Provider) administrator or OpCo (Operating Company) Administrator, you can undeploy a configuration template when you no longer need the configuration deployed on the device. Undeploying a configuration template removes the configuration pushed to the device when the configuration template was deployed.

To remove only the references to the configuration template, without removing the configuration pushed to the device, you must dissociate the configuration template. See *Dissociate a Configuration Template from a Device* for details.

> **NOTE:** You can undeploy configuration templates only from devices with Management Status **Provisioned**. In addition, the configuration templates must have been previously deployed (Deployment Status **Deployed**) on the device.

To undeploy a configuration template:

1. Do one of the following:
   - To undeploy a configuration template from a tenant device, select **Resources > Tenant Devices**.

     The Tenant Devices page appears.
   - To undeploy a configuration template from a provider hub device, select **Resources > Provider Hub Devices**.

     The Provider Hub Devices page appears.
2. Click the ***Device-Name*** link for the device from which you want to undeploy the configuration template.

   The ***Device-Name*** page appears.
3. From the **Configuration Template** tab, select the configuration template that you want to undeploy and click **Undeploy**.
   - If you select a configuration template that was added in CSO Release 5.3.0, an alert message appears, asking you to confirm the undeploy operation. Proceed to Step 4.
   - If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to CSO Release 5.3.0. You must go through the Edit workflow to upgrade the version.
     a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

        The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

     b. Select the template again and click **Undeploy**.

        An alert message appears, asking you to confirm the undeploy operation.
4. Click **Yes**.

   A message indicating that the undeploy configuration template job was triggered is displayed.

You can click the link in the message to view the progress of the job or view the progress on the Jobs page:

- If the job completes successfully, a confirmation message appears, indicating that the configuration template was undeployed from the device.
- If the job fails, an error message appears. You can repeat the procedure to undeploy the configuration template.

RELATED DOCUMENTATION

Deploy Configuration Templates to Devices | 246

Dissociate a Configuration Template from a Device | 253

Dissociate a Configuration Template from a Device

As an SP (Service Provider) Administrator or OpCo (Operating Company) Administrator, you can dissociate a configuration template when you no longer want the template to be associated with your device. Dissociating a configuration template removes references to the configuration template from the device but does not remove the configuration pushed to the device.

To remove the configuration pushed to the device, you must undeploy the configuration template. See "Undeploy a Configuration Template from a Device" on page 251 for details.

To dissociate a configuration template:

1. Do one of the following:

   - Select **Resources > Provider Hub Devices**.

     The Provider Hub Devices page appears.

   - Select **Resources > Tenant Devices**.

     The Tenant Devices page appears.

2. Click the ***Device-Name*** link for the device from which you want to dissociate the configuration template.

   The ***Device-Name*** page appears.

3. From the **Configuration Template** tab, select the configuration template that you want to dissociate from the device and click **Dissociate**.

   An alert message appears, asking you to confirm the dissociate operation.

4. Click **Yes**.

   If the dissociation is successful, a confirmation message appears, indicating that the references to the configuration template were removed from the device.

   If the dissociation fails, repeat the procedure to dissociate the configuration template.

Preview and Render Configuration Templates

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can use the Preview workflow to validate a configuration template by entering values for the configuration template and then render the template to view the configuration.

Although this is not mandatory, we recommend that you use this workflow to validate a configuration template before attaching it to a device template or deploying it on a device.

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

To preview and render a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want to check and click **Render Configuration**.
   - If you select a configuration template that was added in CSO Release 5.3.0, the Preview Configuration page appears displaying the parameters configured for the template. Proceed to Step 3.
   - If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.
     a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

        The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

     b. Select the template again and click **Render Configuration**.

        The Preview Configuration page appears displaying the parameters configured for the template.

3. Specify values for the parameters as needed.

> **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. After you have entered the necessary parameters, click **Render**.

   The Rendered Config page appears displaying the configuration rendered based on the configuration template and the values that you specified.

5. Check if the configuration was rendered correctly.

   If the configuration was not rendered correctly, you can modify the configuration template as needed. See "Edit, Clone, and Delete Configuration Templates" on page 243.

6. Click **OK**.

   You are returned to the Preview Configuration Template page.

7. Click **Cancel** to exit the Preview Configuration Template page.

   You are returned to the Configuration Templates page. You can assign the configuration template to one or more device templates.

RELATED DOCUMENTATION

Assign Configuration Templates to Device Templates | 258

Import Configuration Templates

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can import a configuration template by specifying the parameters using a configuration template file (Jinja template language), Yang model file (schema for the configuration), and the Viewdef file (configuration of the UI).

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

To import a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select **More** > **Import**.

   The Import Configuration Template page appears.

3. Complete the configuration according to the guidelines provided in Table 85 on page 256.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   You are returned to the Configuration Templates page and a popup appears displaying the status of the import operation.

5. Click **OK** to close the popup.

   You are returned to the Configuration Templates page.

If the configuration template is imported successfully, you can validate the configuration template by using the Preview workflow and then assign the configuration template to a device template or deploy it on a device.

Table 85: Import Configuration Template Settings

Setting	Guideline
Template Name	Enter a unique name that can only contain alphanumeric characters and hyphens; 64-character maximum.
Description	Enter a description for the configuration template.
Output Config Format	Select the output configuration format for the template: • CLI (default) • XML
Device Family	Select the device family for which you are adding the template; for example, juniper-nfx.

Table 85: Import Configuration Template Settings *(continued)*

Setting	Guideline
Configuration Template File	Specify the file containing the configuration (in Jinja Template language syntax) by clicking the **Browse** button to navigate to the directory where the configuration template file is located and selecting the file.
Yang Model File	Specify the Yang data model (configuration schema) file by clicking the **Browse** button to navigate to the directory where the Yang model file is located and selecting the file.
Viewdef File	Specify the Viewdef file, which contains the configuration for the UI, by clicking the **Browse** button to navigate to the directory where the Viewdef file is located and selecting the file.

RELATED DOCUMENTATION

Preview and Render Configuration Templates | 254

Deploy Configuration Templates to Devices | 246

Assign Configuration Templates to Device Templates | 258

Export a Configuration Template

As an SP (Service Provider) Administrator or OpCo (Operating Company) Administrator, you can export a configuration template as a ZIP file if you want to reuse the template across multiple CSO instances. To reuse the template, you can import the template files into other CSO instances as is or modify the template files offline and then import them.

The ZIP file contains the configuration template file (Jinja template language), Yang model file (schema for the configuration), and the Viewdef file (configuration of the UI).

To export a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select a configuration template from the list and click **More > Export**.

- If you select a configuration template that was added in CSO Release 5.3.0, the configuration template is automatically downloaded as a ZIP file to your local file system.
- If you select a configuration template that was added in a release before CSO Release 5.3.0, an alert message appears asking you to confirm whether you want to edit the template to automatically upgrade the template to the current CSO release version. You must go through the Edit workflow to upgrade the version.

  a. On the Edit Configuration Template page that appears, proceed to the Summary tab and click **OK**.

     The template is automatically upgraded to CSO Release 5.3.0 and the Configuration Templates page appears.

  b. Select the template again and click **Export**.

     The configuration template is automatically downloaded as a ZIP file to your local file system.

You can import the configuration template files as is or modify the files as needed and then import the files into other CSO instances.

RELATED DOCUMENTATION

About the Configuration Templates Page | 236

Import Configuration Templates | 255

Assign Configuration Templates to Device Templates

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can assign a configuration template to one or more device templates. Associating a configuration template with a device template enables you to deploy additional configuration on the device during ZTP and after the device is activated.

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

To assign a configuration template to one or more device templates:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Select the configuration template that you want to assign and select **More** > **Assign to Device Template**.

   The Assign Configuration Template to Device Templates page appears.

3. Complete the configuration according to the guidelines provided in Table 86 on page 259

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   You are returned to the Configuration Templates page and a popup appears indicating whether the assignment is successful or has failed. If the assignment failed, you can retry the assignment or contact Juniper Networks support.

   If the assignment is successful, you can navigate to the *Device-Name* page (where the configuration parameters are displayed) and enter values for the configuration and deploy the configuration on the device.

Table 86: Assign Configuration Template to Device Template Settings

Setting	Guideline
Template Settings	
Template	Displays the name of the configuration template that you are assigning; you cannot modify this field.
Display Name	Enter the name that you want displayed on the *Device-Name* page.

Table 86: Assign Configuration Template to Device Template Settings *(continued)*

Setting	Guideline
Component Name	For NFX250 devices, select the component name to which the configuration should be deployed. The components that are currently supported are: • Juniper Device Manager (JDM)—JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor.
Auto Deploy	Specify whether the configuration should be deployed automatically on the device during the zero touch provisioning (ZTP) process. The options are: • **Yes**—Deploy the configuration automatically on the device during ZTP. • **No** (Default)—Don't deploy the configuration automatically on the device during ZTP. • **Same as global settings**—Use the same settings as the one configured in the device template.
Enable For	**NOTE:** This field is enabled only if you select Auto Deploy as No. Select whether the configuration template should be enabled for: • **All Tenants**, which means that the template is available for users with SP Administrator (on-premise installation only) or OpCo Administrator roles in Administration Portal and users with tenant administrator roles in Customer Portal. • **SP Admin**, which means that the template is available only for users with the SP Administrator role (on-premise installation only). • **OpCo Admin**, which means that the template is available only for users with the OpCo Administrator role. • **Specific Tenants**, which means that the configuration template is enabled only for specific tenants, which you can specify in the Tenants field.
Tenants	This field appears only if you specified that the configuration template should be available for specific tenants. Select one or more tenants and click the greater-than icon (>) to move the selected tenant or tenants from the Available column to the Selected column. You can use the search icon on the top right of each column to search for tenant names. Click **Next** to continue.
Device Templates	

Table 86: Assign Configuration Template to Device Template Settings *(continued)*

Setting	Guideline
Select Device Templates	The list of device templates to which you can assign the configuration template are displayed in a grid along with some information about the template. CSO displays only those device templates whose device family matches the device family of the configuration template. Select one or more device templates to which you want to assign the configuration template.

RELATED DOCUMENTATION

Deploy Configuration Templates to Devices | 246

Add Configuration Templates

In Administration Portal, users with the SP (Service Provider) Administrator role (on-premises installation only) or OpCo (Operating Company) Administrator role can add a configuration template by providing the device configuration using the Jinja template language syntax.

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

- If a user with the SP Administrator role adds a template, the template is available to the OpCos, OpCo's tenants, and the SP Administrator's tenants.
- If a user with the OpCo Administrator role adds a template, the template is available only to the OpCo and the OpCo's tenants.

NOTE:

- Before you add the configuration template, ensure that you have the device configuration ready.
- We recommend that you use a working device configuration to add the configuration template.

To add a configuration template:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Click the **+** (add) icon.

   The Add Configuration Template page (wizard) appears.

   NOTE: Fields marked with an asterisk (*) are mandatory.

3. Configure the fields on the Basic Information tab according to the guidelines provided in Table 87 on page 262.

   Click **Next** to go to the Templatize Config tab.

4. Add the configuration on the Templatize Config tab. Refer to Table 88 on page 263 for an explanation of the actions on this tab.

   Click **Next** to go to the Generated UI tab, where the UI for the parameters that you entered is generated and displayed.

5. Perform one or more actions on this tab, as explained in Table 89 on page 264.

6. Click **Save**.

   The configuration template is added and you are returned to the Configuration Templates page, where a confirmation message is displayed. You can assign the configuration template to device templates or deploy the template on devices.

Table 87: Basic Information Settings (Add Configuration Template Page)

Setting	Guideline
Template Name	Enter a unique name that can only contain alphanumeric characters and hyphens; 64-character maximum.
Description	Enter a description for the configuration template.
Output Config Format	Select the output configuration format for the template: • CLI (default) • XML

Table 87: Basic Information Settings (Add Configuration Template Page) *(continued)*

Setting	Guideline
Device Family	Select the device family for which you are adding the template; for example, juniper-nfx.
Can be re-deployed	Enable this toggle button if you want CSO to deploy the configuration template again when you redeploy the template. CSO deploys the template even if there are no configuration changes since the previous deployment. If this button is disabled, which is the default, then CSO does not deploy the template again if there are no changes since the previous deployment.
	Click **Next** to continue.

Table 88: Templatize Config Actions (Add Configuration Template Page)

Action	Description
View a sample configuration	You can view a sample configuration by clicking the **Sample Configuration** link near the top of the tab. The sample configuration appears in a new tab in your browser.
Add the device configuration	In the inline editor, copy and paste the device configuration ensuring that the syntax follows the Jinja Template language. CSO detects the template parameters corresponding to the configuration that you entered and displays them in the Parameters pane. For more information, see "Jinja Syntax and Examples for Configuration Templates" on page 271.

Table 88: Templatize Config Actions (Add Configuration Template Page) *(continued)*

Action	Description
Advanced Mode	• When advanced mode is disabled, which is the default, CSO converts the configuration that you entered in Jinja Template language to a Junos OS configuration that uses Junos OS configuration groups. (Configuration groups make it easier to configure and maintain Junos OS configurations; see Understanding Junos OS Configuration Groups.) CSO also automatically includes the commands to delete the configuration groups in the configuration template. If you trigger an undeploy configuration template workflow, CSO uses these commands to delete the configuration. Therefore, to avoid conflict with the commands that CSO automatically includes, ensure that you do not manually include commands related to configuration groups (as part of the device configuration). • When advanced mode is enabled, CSO converts the configuration that you entered in Jinja Template language but does not use Junos OS configuration groups and does not include commands to delete the configuration. Therefore, if you plan to undeploy the configuration template later, you must ensure that you manually enter the commands to delete the configuration as part of the device configuration so that CSO can use these commands to delete the configuration.
[Detected Parameters]	Check that the parameters detected match the configuration that you added to the template: • If the parameters detected do not match, check the Jinja syntax that you used for the template configuration and make any changes needed in the inline editor. • If the parameters detected match the configuration that you added to the template, click **Next** to continue. CSO validates the Jinja template syntax and displays an error message if there are any errors.

Table 89: Generated UI Actions (Add Configuration Template Page)

Action	Description
Reorder the UI	Drag and drop individual fields, grids, or sections to change the order in which the parameters appear on the UI.

Table 89: Generated UI Actions (Add Configuration Template Page) *(continued)*

Action	Description
Modify the settings for a field, section, or grid	To modify the settings for a field, section, or grid: 1. Click the settings (gear) icon next to the field, section, or grid. The Parameter Settings pane appears on the right side of the page, displaying the Basic Settings and Advanced Settings tabs. 2. Modify the fields on these tabs, as needed. See Table 90 on page 265 for an explanation of the fields on these tabs. 3. Click **Save Settings** for each field to save your changes. The modifications that you made are displayed on the UI.
Reset the generated UI	Click **Undo all Edits** to discard the changes that you made and undo the changes made on the UI.
Preview configuration	Previewing the configuration enables you to check the configuration template that you added. To preview a configuration template: 1. Click **Preview Configuration**. The Preview Configuration page appears, displaying the configuration that was rendered based on the values that you entered. 2. Check if the configuration was rendered correctly. • If the configuration was not rendered correctly, click the close (**X**) icon to go back and make modifications as needed. • If the configuration was rendered correctly, click **OK**. You are returned to the Generated UI page.

Table 90: Parameter Settings (Add Configuration Template Page)

Setting	Guideline
Basic Settings Tab	Fields populated in this tab are based on the input type that you select.

Table 90: Parameter Settings (Add Configuration Template Page) *(continued)*

Setting	Guideline
Input Type	Select the input type for the parameter in the configuration template: • Text (default): If the input value for the parameter is a string of characters. • Number: If the input value for the parameter is a number. • E-mail: If the input value for the parameter is an e-mail address. • IPv4: If the input value for the parameter is an IPv4 address. • IPv4 Prefix: If the input value for the parameter is an IPv4 prefix. • IPv6: If the input value for the parameter is an IPv6 address. • IPv6 Prefix: If the input value for the parameter is an IPv6 prefix. • Toggle Button (Boolean): If the input value for the parameter is a boolean value (true or false). • Dropdown: If the input value for the parameter is selected from a list. • Password: If the input value for the parameter is a password. The value that you enter is masked (default). (Optional) Click the **Show Password** (eye) icon to unmask the password. • Confirm Password: If the input value for the parameter is to confirm the password. If you select this option, a Confirm Password field appears on the UI. The value that you enter is masked (default). (Optional) Click the **Show Password** (eye) icon to unmask the password.
Label	Enter the label that you want displayed (on the UI) for the parameter.
Default Value	Specify a default value for the parameter.
Validation Criteria	For Text input type, select one or more validation criteria against which the input value will be checked. If the value that you entered for the parameter on the UI does not meet the selected validation criteria, an error message appears.
Description	Enter an explanation for the parameter, which will appear when you hover over the Help (?) icon for the parameter; the maximum length allowed is 256 characters.
Global Scope	Click the toggle button to make the parameter common across all devices to which the configuration template is being deployed to. If you disable the toggle button, which is default, the parameter must be specified for each device.

Table 90: Parameter Settings (Add Configuration Template Page) *(continued)*

Setting	Guideline
Hidden	Click the toggle button to hide the parameter on the UI when you preview and deploy the template. Typically, this option is used to hide a parameter and display it in the template only when an event is triggered. By default, the toggle button is disabled, which means that the parameter is displayed.
Required	Click the toggle button to make the parameter mandatory; parameters that are mandatory are marked with an asterisk (*) on the UI.
Maximum Value	For parameters that are numbers, enter the maximum value (up to 16 digits) for the input.
Minimum Value	For parameters that are numbers, enter the minimum value (up to 16 digits) for the input.
Fields Visible (Toggle Disabled)	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is disabled (boolean value is FALSE).
Fields Visible (Toggle Enabled)	For Boolean parameters, select one or more parameters that must appear on the UI when the toggle button is enabled (boolean value is TRUE).

Table 90: Parameter Settings (Add Configuration Template Page) *(continued)*

Resource Type	For Dropdown input type, select the type of resource from which you want to retrieve data: • Static Resource—Resources in the list on the UI are mapped to the values that you specify. ◦ To add a static resource: 1. Click the **+** (add) icon. Cells appear in the List Values table. 2. Click inside the cells to specify values for the Label (name for the option in the list), Value (value for the option in the list), and Visibility (conditional visibility based on the option selected from the list) fields. 3. click **✓** (check mark) to save your changes. The values that you specified are displayed in the List Values table. ◦ To edit a static resource, select the resource and click the edit (pencil) icon. ◦ To delete a static resource, select the resource and click the **X** (delete) icon. • Dynamic Resource—Resources in the list on the UI are mapped to the predefined services in CSO. Click the *Resource Management* link to view add, edit, and delete dynamic resources. The Manage Dynamic Resources page appears displaying the existing resources. ◦ To add a dynamic resource: 1. Click the **+** (add) icon. The Add Dynamic Resource page appears. 2. Complete the configuration according to the guidelines specified in Table 91 on page 269. Fields marked with an asterisk (*) are mandatory. 3. Click **OK** to save the resource. You are returned to the Manage Dynamic Resources page, where the resource that you added appears. 4. Click **OK**. You are returned to the Add Configuration Template page. The resource or resources that you added are available in the **Resource** list on the Parameter Settings pane. ◦ To edit a dynamic resource, select the resource and click the edit (pencil) icon. ◦ To delete a dynamic resource, select the resource and click the **X** (delete) icon.

Table 90: Parameter Settings (Add Configuration Template Page) *(continued)*

Key	For data in a table, select a column from the dropdown list that is to be used as a key. The column that you select is marked as unique (**Unique Key**), indicating that the entries in this column must be unique. Keys are unique identifiers used in defining entries (in a table) in the Yang data hierarchy. They help distinguish entries in a column.
Advanced Settings Tab	
Regexp	Enter a regular expression (regex pattern) to validate the input value. A regular expression defines a search pattern that is used to match characters in a string. For example, the regular expression [A-Z] matches the input with the characters A through Z. If the input consists of characters other than A through Z, an error message (as specified in the Invalid Message field) appears.
Error Message (Regexp)	Enter an error message that you want displayed on the UI when the input value does not match the specified regular expression.
Remote Validation	Enter a JavaScript function to validate the input value.
Event List	
Event Name	Select an event from the list based on which the parameter is conditionally displayed.
Event Handler	Enter a JavaScript function that specifies the actions that the event handler takes in response to an event.

Table 91: Fields on the Add Dynamic Resource Page

Field	Guideline
Data Source	
Name	Enter a unique name for the resource.
Source Type	Select the source from which you want to retrieve data: • Service based, which uses predefined services to retrieve data. • URL based, which uses a URL of the API to retrieve data.

Table 91: Fields on the Add Dynamic Resource Page *(continued)*

Field	Guideline
Service	For service-based source type, select a predefined service from which you want to retrieve data.
Entity	For service-based source type, select an entity for which you want to retrieve data.
URL	For URL-based source type, enter the URL of the API to be used for the request.
Method	For the URL-based source type, select the type of HTTPS method (GET or POST) to be used for the resource.
POST Body	For POST method, enter the format of the payload (in JavaScript Object Notation [JSON] format) of the API method, which is sent to the server.
Mock Result	Specify a mock result (in JSON format) if the API request is unable to retrieve data.
Result Mapping	
Result Mapping	Select the type of processing to be done on the output of the remote request: • Script—Use this option if you want to use a script (in JSON format) to process the output. • Mapping—Use this option if you want to map the output using a base path.
Mapping Script	To process the output by using a script, enter a mapping script in JSON format.
Base Path	To process the output by using a base path, enter the base path (JSONPath expression) of the variable in the output from which you want to extract the data; for example, interface.
Label Field	Select whether you want the names, UUIDs, or management status (for the selected entity) displayed as options in the list on the UI.
Value Field	Select a value (such as names, management status, and so on) that you want to associate with the labels (options) in the list on the UI. When you select an option from the list and save the configuration template, CSO processes its associated value (in the backend).

Table 91: Fields on the Add Dynamic Resource Page *(continued)*

Field	Guideline
Extra Fields	Specify the additional values that you want to associate with the labels (options) in the list on the UI. When you select an option from the list on the UI, its associated additional value can be used to trigger an event, when a condition is met, by using a JavaScript function. You specify the JavaScript function in the Event Handler field.

RELATED DOCUMENTATION

Preview and Render Configuration Templates | 254

Jinja Syntax and Examples for Configuration Templates

IN THIS SECTION

- Jinja Syntax and CSO Keywords | 272
- Example 1: Convert a Single Junos OS Command to Jinja Syntax | 274
- Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax | 275
- Example 3: Use Conditional Logic | 277
- Example 4: Use Variable Substitution | 279
- Example 5: Use Filters, Concatenation, and Set Variables | 280
- Example 6: Test a Value | 281

CSO configuration templates consist of three components:

- A Jinja template configuration, which contains the logic and the configuration for the configuration template. (Jinja is a template engine for Python and you can find several Jinja resources on the Web.)
- A Yang data model file, which contains the descriptors for the configuration schema.
- A ViewDef (view definition) file, which is a JavaScript Object Notation (JSON) file that is used to specify the GUI aspects of the configuration template.

When you use the Add Configuration Template workflow to add a template, you specify the template configuration and logic by using the Jinja template language. CSO then generates the Yang data model and the ViewDef files automatically based on template configuration and logic that you specified. The generation of the Yang and ViewDef files is transparent to the user and doesn't require any user intervention.

Jinja Syntax and CSO Keywords

The tables below list the Jinja syntax used commonly in configuration templates and the keywords used in configuration templates respectively.

Table 92: Common Jinja Syntax Used in Configuration Templates

Syntax	Explanation
{{ }}	Denotes a variable or expression that will be printed to the template output. For example: `{{tenant_name}}` **NOTE:** Hyphens are not recognized by the CSO template engine, so use underscores (_) in variables or expressions.
{# #}	Denotes a comment that will not be included in the template output. For example: `{# This is an example of comment in Jinja syntax #}`

Table 92: Common Jinja Syntax Used in Configuration Templates *(continued)*

Syntax	Explanation

{% %}	Denotes statements that are used to create conditional logic:
	• The **{%- -%}** statement removes whitespace characters from the output.
	• The **if** statement used to execute a set of commands (enclosed between the **if** and **endif** keywords) when the condition is true.
	`{% if <condition> %}`
	`...`
	`...`
	`...`
	`{% endif %}`
	• The **if-else** statements are used to execute a set of commands (enclosed between the **if** and **else** keywords) when the condition is true and a different set of commands (enclosed between the **else** and **endif** keywords) when the condition is false.
	`{% if <condition> %}`
	`...`
	`...`
	`{% else %}`
	`...`
	`...`
	`{% endif %}`
	• The **for** statement is used to loop through a set of commands (enclosed between the **for** and **endfor** keywords) when the condition is true.
	`{% for <condition> %}`
	`...`
	`..`
	`...`
	`{% endfor %}`

Dot (.)	A dot [operator] is used to reference an attribute of a variable. The following example shows a **for** loop where you can add multiple prefixes:
	`{% for prefix in Trusted_Network_Prefix_List %}`
	`set groups trusted prefix policy options prefix list re ssh`
	`{{prefix.Trusted_Network_Prefix_List}}`
	`{% endfor %}`

NOTE: You can use configuration template keywords if you enable advanced mode for the configuration template.

Table 93: Configuration Template Keywords

Keyword	Explanation
post_config	Indicates to CSO that the variable that follows is a data type.
pre_config	Indicates to CSO the current configuration associated with a device. The pre_config keyword is used to compare a variable field's value and then modify or delete existing configuration from a target device.
diff_config	Indicates to CSO that the pre_config and post_config should be compared and that CSO should create a new rendered configuration and then push it to target device.

Example 1: Convert a Single Junos OS Command to Jinja Syntax

If you want to convert a single Junos OS command into Jinja syntax for use in a configuration template:

1. Identify the variables that are configured in the Junos OS command.

   For example, in the command **set snmp trap-group CSO-Trp-Grp targets 192.0.2.100**, the variables configured are CSO-Trp-Grp and 192.0.2.100.

2. Convert the Junos OS CLI command to Jinja syntax by enclosing each variable in double curly braces as follows: **{{ *Variable_Name* }}**.

   So, in this example, if we use *Trap_Group_Name* and *SNMP_Host_IP_Address* as the variable names, the Jinja syntax for the command is as follows:

   ```
   set snmp trap-group {{ Trap_Group_Name }} targets {{ SNMP_Host_IP_Address }}
   ```

3. If you paste this in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
    SNMP_Host_IP_Addresses
    Trap_Group_Name
```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), using the values indicated in the first step, CSO renders the configuration as follows:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Test
set snmp trap-group CSO-Trp-Grp targets 192.0.2.100
exit
set apply-groups default-domain_Juniper_Test
```

   Notice that although you provided the JInja syntax for a single Junos OS command, CSO added additional commands to the configuration. This is because, by default, CSO uses Junos OS groups to generate the configuration. Junos OS groups make it easier to apply and delete configurations. For more information, see Understanding Junos OS Configuration Groups.

   If you don't want to use Junos OS groups, you must turn on the advanced mode in the configuration template, when you specify the configuration in Jinja syntax..

Example 2: Convert a Junos OS Configuration Snippet to Jinja Syntax

In this example, we'll convert the following Junos OS configuration snippet into Jinja syntax for use in a configuration template:

```
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-Relay-Grp1 interface ge-0/0/2.0
set security zones security-zone trust host-inbound-traffic system-services
dhcp
```

To convert the Junos OS configuration into Jinja syntax:

1. Identify the variables that are configured in the Junos OS commands. For ease of understanding, the variables are enclosed within angular brackets (<>) in the example below.

   NOTE: In this example, we're not considering DHCP-SERVER as a variable.

   ```
   set forwarding-options dhcp-relay server-group DHCP-SERVER <Relay_IP>
   set forwarding-options dhcp-relay active-server-group DHCP-SERVER
   set forwarding-options dhcp-relay group <Relay_Group_Name> interface
   <Relay_Interface>
   set security zones security-zone <Relay_Zone> host-inbound-traffic
   system-services dhcp
   ```

2. Convert each Junos OS CLI command to Jinja syntax by identifying the variables, providing a name for each variable, and enclosing each variable in double curly braces. So, in this case, the Jinja syntax is as follows:

   ```
   set forwarding-options dhcp-relay server-group DHCP-SERVER {{Relay_IP}}
   set forwarding-options dhcp-relay active-server-group DHCP-SERVER
   set forwarding-options dhcp-relay group {{Relay_Group_Name}} interface
   {{Relay_Interface}}
   set security zones security-zone {{Relay_Zone}} host-inbound-traffic
   system-services dhcp
   ```

3. When you paste this in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

   ```
   Relay_IP
   Relay_Interface
   Relay_Zone
   Relay_Group_Name
   ```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), using the values for this example, CSO renders the configuration as follows:

   ```
   delete groups default-domain_Juniper_Test
   delete apply-groups default-domain_Juniper_Test
   ```

```
edit groups default-domain_Juniper_Test
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-Relay-Grp1 interface ge-0/0/2.0
set security zones security-zone trust host-inbound-traffic system-services dhcp
exit
set apply-groups default-domain_Juniper_Test
```

Example 3: Use Conditional Logic

In this example, which is a modified version of the preceding example, we'll see how you can use conditional logic (**if** and **for** statements) in a configuration template.

```
{%- if enable_Forwarding_Options %}

set forwarding-options dhcp-relay server-group DHCP-SERVER {{RelayIP }}
set forwarding-options dhcp-relay active-server-group DHCP-SERVER

{% for relay in RelayOptions %}
set forwarding-options dhcp-relay group {{ relay.Relay_Group_Name }} interface {{
relay.Relay_Interface }}
set security zones security-zone {{ relay.Relay_Zone }} host-inbound-traffic
system-services dhcp
{% endfor %}

{% endif %}
```

The explanation of the example above is as follows:

1. In this example, we add an **if** statement and enclose the configuration within that statement as follows:

   ```
   {%- if enable_Forwarding_Options %}

   ...
   ...

   {% endif %}
   ```

   This means that the configuration is applied only if the enable_Forwarding_Options is True. If enable_Forwarding_Options is False, then no configuration is applied.

> **TIP:** If you want to apply a different configuration when enable_Forwarding_Options is False, you can use the **else** statement.

2. Then, we add a **for** statement to enable the configuration of more than one set of values for the **Relay_Group_Name**, **Relay_Interface**, and **Relay_Zone** variables.

```
{% for relay in RelayOptions %}
set forwarding-options dhcp-relay group {{ relay.Relay_Group_Name }} interface
{{ relay.Relay_Interface }}
set security zones security-zone {{ relay.Relay_Zone }} host-inbound-traffic
system-services dhcp
{% endfor %}
```

   When you use a **for** statement, the GUI rendered by CSO (when you use the preview feature) displays the variables in table (grid). You can then use the Add icon (**+**) to add rows to the table and configure one or more sets of values as needed.

3. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
    RelayIP
    enable_Forwarding_Options

RelayOptions

    Relay_Interface
    Relay_Zone
    Relay_Group_Name
```

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide values for the parameters, including two sets of values for **Relay_Group_Name**, **Relay_Interface**, and **Relay_Zone**, CSO renders the configuration as follows:

```
delete groups default-domain_BLR_SOLN_test
delete apply-groups default-domain_BLR_SOLN_test
edit groups default-domain_BLR_SOLN_test
set forwarding-options dhcp-relay server-group DHCP-SERVER 192.0.2.50
set forwarding-options dhcp-relay active-server-group DHCP-SERVER
set forwarding-options dhcp-relay group CSO-RelayGrp1 interface ge-0/0/2.0
```

```
set security zones security-zone trust host-inbound-traffic system-services dhcp
set forwarding-options dhcp-relay group RelayGrp2 interface ge-1/0/2.0
set security zones security-zone untrust host-inbound-traffic system-services
dhcp
exit
set apply-groups default-domain_BLR_SOLN_test
```

Example 4: Use Variable Substitution

In this example, we use a variable as part of the configuration command such that the *value* that we specify for the variable is used in the command.

```
set groups MIST vlans V-{{pool.VLAN_Id}} vlan-id {{pool.VLAN_Id}}
```

The explanation of the example above is as follows:

1. We use the **VLAN_Id** attribute of the **pool** parameter to set the Junos OS configuration parameters **vlans** and **vlan-id**.

2. When you paste the Jinja command **set groups MIST vlans V-{{pool.VLAN_Id}} vlan-id {{pool.VLAN_Id}}** in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

   ```
   pool
       VLAN_Id
   ```

   This is because we've used the dot (.) operator to reference the attribute **VLAN_Id** of the parameter **pool**.

3. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide the value 120 for **VLAN_Id**, CSO renders the configuration as follows:

   ```
   delete groups default-domain_Juniper_Test
   delete apply-groups default-domain_Juniper_Test
   edit groups default-domain_Juniper_Test
   set groups MIST vlans V-120 vlan-id 120
   ```

```
exit
set apply-groups default-domain_Juniper_Test
```

In the rendered configuration command, you can see that the parameters **vlans** and **vlan-id** are set to **V-120** and **120** respectively, based on the value that we provided for the VLAN_Id parameter.

Example 5: Use Filters, Concatenation, and Set Variables

In this example, we'll look at how to set a variable using concatenation and filters, and then use that variable in a Junos OS configuration command.

```
{% set pool_name = Dhcp_Server_Name + '_' + Interface | replace("/", "_") %}
set system services dhcp-local-server overrides process-inform pool {{pool_name}}
```

The explanation of the example above is as follows:

1. The Jinja statement **{% set pool_name = Dhcp_Server_Name + '_' + Interface | replace("/","_") %}** is used to set a variable called *pool_name*, using two other variables *Dhcp_Server_Name* and *Interface*, as follows:

   a. The **|** (pipe) operator is used to separate variables from filters, which are functions that modify variables. In this example, we use the **replace("/","_")** filter to modify the *Interface* variable by replacing the / (forward slash) characters with _ (underscore) characters.

   b. Then, we use the **+** operator to concatenate the resulting string with the variable *Dhcp_Server_Name*.

   > **NOTE:** The operator **+** is typically used to add numbers, but when the values are strings, the strings are concatenated.

   c. Finally, the tag **set** is used (along with the **=** operator) to set the variable called *pool_name* to the concatenated variable.

2. Then, the Junos OS command **set system services dhcp-local-server overrides process-inform pool {{pool_name}}** is used to configure the Junos OS configuration statement **pool** using the variable **pool_name** that we set in the preceding step.

3. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
Interface
Dhcp_Server_Name
```

As you can see, the Junos OS command or the *pool_name* variables are not displayed because we're using the *Interface* and *Dhcp_Server_Name* variables to arrive at the final Junos OS configuration.

4. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and provide the values LA_dhcp_srvr for **Dhcp_Server_Name** and ge-0/1/2 for the **Interface**, CSO renders the configuration as follows:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Test
set system services dhcp-local-server overrides process-inform pool
LA_dhcp_srvr_ge-0_1_2
exit
set apply-groups default-domain_Juniper_Test
```

As explained in a previous step, the / characters in ge-0/1/2 are first replaced with _ characters, which changes the string to ge-0_1_2. This string is concatenated with LA_dhcp_srvr to produce the string LA_dhcp_srvr_ge-0_1_2, which is used in the Junos OS configuration command.

Therefore, the Junos OS configuration command generated is **set system services dhcp-local-server overrides process-inform pool LA_dhcp_srvr_ge-0_1_2**.

Example 6: Test a Value

In this example, we'll look at how to test a value and perform actions based on the result of the test conditions.

```
{%- if NewNetwork.VLAN_Id is defined and (NewNetwork.VLAN_Id | count) > 2 -%}
set vlan-id {{NewNetwork.VLAN_Id}}
{% else %}
set vlans VL-{{NewNetwork.VLAN_Id}}
{% endif %}
```

The explanation of the example above is as follows:

1. We test the parameter **NewNetwork.VLAN_Id** for two conditions:

a. Whether the parameter is defined (by using the **NewNetwork.VLAN_Id is defined** condition)

b. Whether the length of the parameter is greater than two (by using the condition **(NewNetwork.VLAN_Id | count) > 2**)

Because we use the keyword **and**:

- The configuration command **set vlan-id {{NewNetwork.VLAN_Id}}** is added to the configuration (that CSO generates) when *both* conditions hold true.
- The configuration **set vlans VL-{{NewNetwork.VLAN_Id}}** is added to the configuration when either of the conditions is false.

2. When you paste the Jinja commands in the Template Configuration section of the Add Configuration Template workflow, CSO detects the parameters as follows:

```
NewNetwork
    VLAN_Id
```

3. If you use the preview feature to render the configuration (for an OpCo named Juniper and a configuration template named Test), and:

- Provide the value 125 for ***VLAN_Id***, CSO renders the configuration as follows because both conditions are true:

```
delete groups default-domain_Juniper_Test
delete apply-groups default-domain_Juniper_Test
edit groups default-domain_Juniper_Testset vlan-id 125
exit
set apply-groups default-domain_Juniper_Test
```

- Provide the value 65 for ***VLAN_Id***, CSO renders the configuration as follows because one of the conditions is false (length of the parameter is not greater than 2):

```
delete groups default-domain_BLR_SOLN_testtmp
delete apply-groups default-domain_BLR_SOLN_testtmp
edit groups default-domain_BLR_SOLN_testtmp
set vlans VL-65
exit
set apply-groups default-domain_BLR_SOLN_testtmp
```

RELATED DOCUMENTATION

View the Configuration Deployed on Devices

In Administration Portal, for any configuration template, users with administrator or operator roles can view the configuration deployed on one or more devices.

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

To view the configuration deployed on one or more devices:

1. Select **Resources > Templates > Configuration Templates**.

   The Configuration Templates page appears.

2. Navigate to the Devices column of the configuration template for which you want to view the deployed configuration, and click the **Number-of-devices** link.

   The Device Configuration page appears.

   Table 94 on page 284 explains the fields on this page.

3. After you have viewed the deployed configurations, click **OK**.

   You are returned to the Configuration Templates page.

Table 94: Device Configuration Page Fields

Setting	Guideline

Devices	The devices on which the configuration was deployed are displayed in a table. For each device, the following fields are displayed:
	• Device Name
	• Device Family
	• Operational Status, indicating whether the device is up or down.
	• Deployment Status:
	  ◦ CREATED, indicating that the deployment hasn't started.
	  ◦ DEPLOYED, indicating that the configuration was successfully deployed.
	  ◦ DEPLOYING, indicating that the deployment of the configuration is in progress.
	  ◦ DEPLOY_FAILED, indicating that the deployment of the configuration failed.
	• Deployment Date, indicating the date and time on which the deployment was triggered.
	• Job—Click the **View logs** link for a device to view the deployment history for that device. The Deployment History page appears displaying the number of jobs in progress, number of successful jobs, and number of failed jobs in addition to a table listing some details of the job. You can drill down further by clicking the **Regional Log** and **Log** links.

Device-Name Configuration	Select a device by clicking the check box corresponding to the row: • For each device on which the configuration deployed successfully, this pane displays the configuration that is deployed on the device. • For each device on which the configuration deployment is in progress, DEPLOYING is displayed.

RELATED DOCUMENTATION

About the Configuration Templates Page | 236

APN Overview

The access point name (APN) is the name of the gateway between an OpCo's network and the Internet. The APN connects the CPE device to the Packet Data Network (PDN) such as Internet through the Packet Data Network Gateway (P-GW). A CPE device can access multiple APNs, which consists of domain names and its associated parameters. All CPE devices are shipped with default APN settings.

In the Long Term Evolution (LTE) architecture for the Evolved Packet Core (EPC), the APN determines the P-GW that the CPE device must use. The APN also defines the tunnel connecting the CPE device to a PDN such as the Internet. Each PDN that the user has subscribed to has an APN and an associated P-GW, often called a "PDN subscription context." An example for a context is the default APN, connecting to a PDN such as the Internet unless the user activates another APN.

The CPE device is shipped to the tenant site with the default APN settings. The APN is applicable for sites with an LTE WAN link. CSO supports LTE WAN link on SRX320, SRX340, SRX345, NFX250 and NFX150 CPE devices only.

On NFX250 device, the LTE WAN link is supported through a USB dongle. The USB dongle is plugged into the USB port of the CPE device. The LTE-VM that is pre-installed on the NFX250 device has thousands of APN settings to enable the LTE modem to work with several OpCos all over the world. The NFX150 device is also pre-configured with default APN settings.

In both the devices, the initial LTE connection is established with default APN settings. As long as an LTE connection is established with the default APN settings, the LTE WAN link is used to reach CSO and complete the device activation process. Once the CPE device is activated at the tenant site, the tenant can choose to change the SIM card on the device to use a different LTE service provider. This requires new APN settings to be applied to the CPE device. Also in some cases the APN settings may need to be changed even when there is no SIM change required; this is to choose a private APN with the current LTE service provider. The tenant administrator can change the APN settings for specific tenant by logging into the Administration Portal.

NOTE: The LTE WAN links on NFX250 devices works only with the Vodafone K5160 dongle.

Benefits of APN Configuration

When CPE devices are shipped to different regions around the world, APN configuration feature allows the administrators to change the default APN settings to support local network as opposed to remote network and consequently avoid the roaming charges.

Configuring APN Settings on CPE Devices

IN THIS SECTION

- Configuring APN Settings with SIM Change on CPE Devices | 286
- Configuring APN Settings without SIM Change on CPE Devices | 288

You can configure Access Point Name (APN) settings on the following devices, with or without SIM change. You can change the APN settings either to use a private APN with the current LTE service provider or to use a different LTE service provider.

> **NOTE:** You can only insert a SIM card in the SIM1 slot of the LTE Mini-Physical Interface Module (Mini-PIM).

Following is the list of devices on which you can configure APN settings:

- NFX Series—NFX150 and NFX250 CPE devices
- SRX Series—SRX320, SRX340, and SRX345 CPE devices

Configuring APN Settings with SIM Change on CPE Devices

To configure APN settings with SIM change:

1. Log in to Administration Portal.
2. Select **Resources > Templates > Device Templates**.

   The Device Templates page appears.
3. Select a device template and click **Edit Device Template > Stage-2 Initial Configuration**.

   The Stage-2 Initial Configuration page appears.
4. Click **APN Configuration** tab and change the APN settings according to the guidelines provided in Table 95 on page 287.

5. Click **OK**.

   The new settings are applied after one minute.

6. Remove the USB dongle from the CPE device, change the SIM card, and re-insert the USB dongle.

   The system checks for the new APN settings every minute.

   - If the applied APN setting is compatible with the new SIM card—The LTE WAN link and its tunnels goes down after one minute and remain down till the new SIM card is inserted. The LTE dongle LED indicates that the connection is down during this period. Maximum one minute after the new SIM is inserted, the LTE dongle LED indicates connection Up. The LTE WAN link and its tunnels comes up automatically.
   - If the applied APN setting is not compatible with the new SIM—The LTE WAN link and its tunnels goes down after one minute and remains down even after the new SIM card is inserted. The LTE dongle LED indicates that the connection is down even after the new SIM is inserted.

7. To revert back to the old SIM, remove the USB dongle, replace the current SIM with the previous SIM, and re-insert the dongle.

   The system checks for the new APN settings every minute. Maximum one minute after the old SIM is inserted, the LTE dongle LED indicates that the connection is up (using the old SIM and old APN). The LTE WAN link and its tunnels comes up automatically

Table 95: Fields for the APN Configuration Settings on the Stage-2 Initial Configuration Page

Field	Description
Use default APN settings	Click the toggle button to enable (default) or disable the default APN settings. • If you enable this option, the default APN settings that are shipped along with the CPE device are used for configuring the APN. • If you disable this option, you must configure the APN settings manually.
APN Settings	
APN Name	Enter the access point name (APN) of the gateway router. The name can contain alphanumeric characters and special characters.
SIM Change Required	Click the toggle button to enable or disable changing the SIM card: **NOTE:** You can change the SIM card either to use a different LTE service provider or to use a private APN with the current LTE service provider. • (Default) Enable this option to change the APN settings and to use a new SIM card. • Disable this option to change the APN settings without changing the SIM card.

Table 95: Fields for the APN Configuration Settings on the Stage-2 Initial Configuration Page *(continued)*

Field	Description
Authentication Method	Select the authentication method for the APN configuration: • (Default) PAP—Select this option to use Password Authentication Protocol (PAP) as the authentication method. • CHAP—Select this option to use Challenge Handshake Authentication Protocol (CHAP) authentication as the authentication method. • None—Select this option if you do not want to use any authentication method.
Authentication Information	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication if you have selected the APN authentication method as either **PAP** or **CHAP**.
SIP Password	Enter the SIP password for authentication if you have selected the APN authentication method as either **PAP** or **CHAP**.

Configuring APN Settings without SIM Change on CPE Devices

To configure APN settings without SIM change:

1. Log in to Administration Portal.
2. Select **Resources > Templates > Device Templates**.

   The Device Template page appears.
3. Select a device template and click **Edit Device Template > Stage-2 Initial Configuration**.

   The Stage-2 Initial Configuration page appears.
4. Click **APN Configuration** tab and change the APN settings according to the guidelines provided in Table 95 on page 287.
5. Click **OK**.

   The new settings will be applied after one minute.

   • If the applied APN settings are valid, then in CSO, the LTE WAN link and its associated tunnels will go down momentarily and then gets re-established automatically.

- If the applied APN settings are invalid, then after one minute, the LTE dongle LED will indicate connection down. In CSO, the LTE WAN link and its associated tunnels will go down. After two minutes, the LTE dongle LED will indicate connection Up (using old APN). In CSO, the LTE WAN link and its tunnels will come up automatically

Device Images Overview

An image management system provides full lifecycle management of images for all network devices, including CPE device and virtualized network function (VNF) images. A *device image* is a software installation package for the CPE device or an image for a virtual application that runs on the device. For example, for a NFX Series device platform, you require an NFX software image and a software image for the vSRX application that provides security functions and routing on the device. You install a VNF image on a CPE device.

> **NOTE:** In CSO Release 5.0.0, the software images are uploaded and managed by the Juniper Networks team that manages the cloud installation. If you need a device image or VNF that is not listed among the supported images, contact your Juniper Networks representative.

You can deploy device images or VNF images on a single device or simultaneously on multiple devices of the same family. CPE device images include software images for the NFX and SRX Series.

You can stage the image on a device, verify the checksum, and deploy the staged image using the **Deploy** option from the Images page. You can also schedule the staging, deployment, and validation of a device image.

RELATED DOCUMENTATION

About the Device Images Page | 290

About the Device Images Page

To access this page, click **Resources > Images**.

You can use the Images page to view uploaded device images for physical and virtual devices. From the Images page, you can stage, deploy, or stage and deploy an image onto a single device or simultaneously onto multiple devices of the same family. For more information, see "Device Images Overview" on page 289.

Tasks You Can Perform

You can perform the following tasks from this page:

- Stage device images. See "Staging an Image" on page 292
- Deploy device images. See "Deploying Device Images to Devices" on page 294.
- View details about a device image. Click the details icon that appears when you hover over the name of an image or click **More > Details**.
- Show or hide columns that contain information about the device image—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search an object for a device image—Click the Search icon in the top right corner of the page to search for a device image.
- View the history of image upgrade. Click **Image Upgrade History > Upgrade History** at the top right corner of a page. See Table 97 on page 291.

Field Descriptions

Table 96 on page 290 shows the fields on the Device Images page.

Table 96: Fields on the Images Page

Field	Description
Image Name	Displays the name of the device image. Example: juniper_srx_v1.tgz
Type	Displays the type of the device image. Example: VNF Image

Table 96: Fields on the Images Page *(continued)*

Field	Description
Version	Displays the version number of the device image. Example: 1.1
Vendor	Displays the vendor name of the device. Example: Juniper
Size	Displays the size of the device image. Example: 14 KB

Table 97 on page 291 shows fields on the Upgrade History page.

Table 97: Fields on the Upgrade History Page

Field	Description
In progress	Displays the number of image upgrade tasks that are in progress.
Success	Displays the number of image upgrade tasks that are successful.
Failure	Displays the number of image upgrade tasks that have failed.
Name	Displays the name of the task.
Start Date	Displays the start date and time of the task.
End Date	Displays the end date and time of the task.
Status	Displays the status of the task to know whether the task succeeded or failed.
Log	Displays the import logs. Click a log to access more detailed information about the upgrade images.

RELATED DOCUMENTATION

Uploading a Device Image | 296

Deploying Device Images to Devices | 294

Staging an Image

From the **Resource > Images** page, you can select an image and click the **Stage** button to stage the image onto one or more physical or virtual devices or Virtual Network Functions (VNF). You can stage an image onto a single device or multiple devices on a per-site basis or across all sites of a tenant.

From the **Stage Image: Select Devices** page, you can choose to stage an image, and also to either run the staging immediately or at a scheduled time.

The **Stage** option is especially useful if you are using a low-bandwidth connection. On low-bandwidth connections, manually staging an image prior to deploying the image helps prevent the image deployment from timing out because of a slow connection. On high-bandwidth connections, you can choose to stage the image along with the image deployment.

To deploy a device image onto devices:

1. Select **Resource > Images**.

   The **Images** page appears.

2. Select the device image to be staged on the device and click the **Stage** button.

   The **Stage Image: Select Devices** page appears and a list of compatible devices (CPE and VNF) for the selected image is retrieved and displayed with their associated information in the page. See Table 98 on page 292 for the details of the device.

   > **NOTE:** The **Deploy** button is enabled only for device images.

3. Select one or more devices onto which the device image needs to be staged and schedule a date and time for image staging.

Table 98: Fields on the Deploy Image: Select Devices Page

Field	Description
Device Name	Displays the name of the device configured in the point of presence (POP) or site. Example: sunny-NFX-250
Tenant	Displays the name of the tenant. Example: tenant-blue

Table 98: Fields on the Deploy Image: Select Devices Page *(continued)*

Field	Description
Site Name	Displays the name of the tenant site. Example: site-blue-white
Location	Displays the name of the location. Example: San Jose, CA
WAN Links	Displays the number of WAN links. Example: 3
POP Name	Displays the name of the POP. Example: pop_blue
Management Status	Displays the management status of the devices deployed in the cloud. • EXPECTED—Regional server has activation details for the device, but the device has not yet established a connection with the server. • ACTIVE—Device has downloaded images, but is not yet configured. • PROVISIONED—IPsec tunnel on the NFX250, SRX, or vSRX device is operational. • PROVISION_FAILED—Device failed if the vSRX was not instantiated properly.
Model	Displays the name of the device model. Example: NFX250
Active Services	Displays the number of services that are activated for the device. Example: 3
Stage Expiry Time	Specify the maximum number of seconds CSO must wait for an image staging to be complete. If staging is not complete in the specified time, the operation times out. You can use this setting to configure a longer timeout for image staging over low-bandwidth connections. The default is 7200 seconds.
Choose Staging Time	
Run now	Select this option if you want to stage the image onto the device immediately.
Schedule at a later time	Select this option to schedule the image staging for a later date and time, and specify the date and time when you want the image to be staged.

RELATED DOCUMENTATION

About the Device Images Page | 290
Deploying Device Images to Devices | 294

Deploying Device Images to Devices

From the **Resource > Images** page, you can select an image and click the **Deploy** button to deploy the image onto one or more physical or virtual devices or Virtual Network Functions (VNF). You can deploy an image onto a single device or multiple devices on a per-site basis or across all sites of a tenant.

From the **Deploy Image: Select Devices** page, you can choose to stage an image and deploy it, and also to either run the deploy immediately or at a scheduled time.

To deploy a device image onto devices:

1. Select **Resource > Images**.

   The **Images** page appears.

2. Select the device image to be deployed on the device and click the **Deploy** button.

   The **Deploy Image: Select Devices** page appears and a list of compatible devices (CPE and VNF) for the selected image is retrieved and displayed with their associated information in the page. See Table 98 on page 292 for the details of the device.

   NOTE: The **Deploy** button is enabled only for device images.

3. Select one or more devices onto which the device image needs to be deployed and schedule a date and time for image deployment.

Table 99: Fields on the Deploy Image: Select Devices Page

Field	Description
Device Name	Displays the name of the device configured in the point of presence (POP) or site. Example: sunny-NFX-250
Tenant	Displays the name of the tenant. Example: tenant-blue

Table 99: Fields on the Deploy Image: Select Devices Page *(continued)*

Field	Description
Site Name	Displays the name of the tenant site. Example: site-blue-white
Location	Displays the name of the location. Example: San Jose, CA
WAN Links	Displays the number of WAN links. Example: 3
POP Name	Displays the name of the POP. Example: pop_blue
Management Status	Displays the management status of the devices deployed in the cloud. • EXPECTED—Regional server has activation details for the device, but the device has not yet established a connection with the server. • ACTIVE—Device has downloaded images, but is not yet configured. • PROVISIONED—IPsec tunnel on the NFX250, SRX, or vSRX device is operational. • PROVISION_FAILED—Device failed if the vSRX was not instantiated properly.
Model	Displays the name of the device model. Example: NFX250
Active Services	Displays the number of services that are activated for the device. Example: 3
Stage Image	Indicates whether the Stage Image option is enabled or not. The **Stage Image** option is enabled by default and ensures that the image is staged to the device before image deployment is attempted. Click the toggle button to disable staging of the image onto the device. **NOTE:** We recommend that on low-bandwidth connections you disable the **Stage Image** option to prevent the deploy from timing out because of the delay in staging the image. On such connections, use the **Stage** option on the **Images** page to manually stage the image before you deploy the image. If you disable the **Stage Image** option without manually staging the image onto the device, the deploy operation fails.

Table 99: Fields on the Deploy Image: Select Devices Page *(continued)*

Field	Description
Stage Expiry Time	Specify the maximum number of seconds CSO must wait for an image staging to be complete. If staging is not complete in the specified time, the operation times out. You can use this setting to configure a longer timeout for image staging over low-bandwidth connections. The default is 7200 seconds.
Choose Deployment Type	
Run now	Select this option if you want to deploy the image to the device immediately.
Schedule at a later time	Select this option to schedule the image deployment for a later date and time, and specify the date and time when you want the image to be deployed.

RELATED DOCUMENTATION

About the Device Images Page | 290

Staging an Image | 292

Uploading a Device Image

On the Images page, you can upload image files for CPE and VNF devices. You can also add some metadata about the device image file that you upload to the device.

NOTE: The image being uploaded must use the same image name as the published image. Image upgrade might fail if the image name and details are changed.

To upload a device image for the device:

1. Click **Resources > Images.**

   The Images page appears.

2. Click the add icon (+).

   The Upload Image page appears.

3. Enter the required details in the fields on the Upload Image page. See the field descriptions in Table 100 on page 297.

4. Click **Upload**. If you want to discard the upload device image process, click **Abort** instead.

   The Upload Image page displays the progress of the image upload.

5. Click **OK** to save the changes.

   You are returned to the Images page.

Table 100: Fields on the Upload Device Image Page

Field	Description
Name	Specify the filename for the device image that you are uploading. Example: juniper_nfx_250_v1_img.tgz You must use the following filename format for device images of VNFs as listed below: • Riverbed—**riverbed-img** • vSRX—**vsrx-vmdisk-15.1.qcow2** • NFX—**juniper_nfx_1.5_img.tgz**
Image Type	Specify the type of device image. • **Device Image**—Software image for the physical device (CPE). • **VNF Image**—Software image for the virtual device (VNF). • **VNF Script**—Provision script for the VNF image. • **EMS Plugin Package**—EMS plugin package to support a new device family. • **Device Extension Package**—Extension software package that can be installed on the device. • **Boot Config Image**—Boot configuration ISO image that can be used to boot up the VNF or virtual device. • **Telemetry Agent Package**—Installable package containing telemetry agent to run on a device. For example, NFX. Yes • **VNFM Plugin Package**—Installable package containing VNF Manager (VNFM) plugin specific to a certain set of VNFs.
Description	Enter a description of the device image.

Table 100: Fields on the Upload Device Image Page *(continued)*

Field	Description
File Location	Click **Browse** to navigate to the file location in your local system and select an image file to upload.
Vendor	Specify the vendor name of the device. Example: Juniper Networks.
Family	Specify the name of the device family. Example: NFX
Supported Platform	Specify the platform supported by the device image. Example: NFX250
Major Version Number	Specify the major version of the device image. Example: 12
Minor Version Number	Specify the minor version of the device image. Example: 1
Build Number	Specify the build name of the device image. Example: X53-D102.2

RELATED DOCUMENTATION

Device Images Overview | 289

About the Device Images Page | 290

Deleting Device Images

You can delete one or more device images from the Images page.

To delete a device image:

1. Select **Resources > Images**.

The Images page appears with a list of device images.

2. Select the device image that you want to delete and then click the X icon.

   The Confirm Delete page appears.

3. Click **Yes** to confirm.

   The device image is deleted.

RELATED DOCUMENTATION

About the Device Images Page | 290

Network Services Overview

A *network service* is a final product offered to end users with a full description of its functionality and specified performance.

Administrative users deploy network services between two locations in a virtual network, so that traffic traveling in a specific direction on that link is subject to action from that service. The term *network service* is defined in the ETSI Network Functions Virtualization (NFV) standard.

A network service consists of a *service chain* of one or more linked network functions, which are provided by specific virtualized network functions (VNFs), with a defined direction for traffic flow and defined ingress and egress points. The term service chain refers to the structure of a network service, and although not defined in the ETSI NFV standard, this term is regularly used in NFV and software-defined networking (SDN).

A network service designer creates network services in Network Service Designer. When the designer publishes the service to the network service catalog from Network Service Designer, administrators can see the network service in Administration Portal.

RELATED DOCUMENTATION

About the Network Services Page | 300

About the Network Services Page

To access this page, click **Configuration > Network Services**.

You can use the Services page to view the complete list of network services that service designers have published to the network service catalog from Network Service Designer and to view information about the services. For an introduction to network services, see "Network Services Overview" on page 299.

Tasks You Can Perform

You can perform the following tasks from this page:

- Quickly view important data about services and about instances of those services deployed at customers' sites in the widgets that appear at the top of the page. See Table 101 on page 300.
- View full information about a service and about instances of a service at customer sites. Click the name of a service in the list. See "About the Service Instances Page" on page 304.

Field Descriptions

Table 101 on page 300 shows the descriptions of the widgets that appear at the top of the Services page.

Table 101: Widgets on the Services Page

Widget	Description
Top Network Services Used	View the numbers of instances of the three services that are most used by tenants in the network. This view might help you to identify trends for network services, especially when you introduce a new service.
Services with Critical Alerts	View the top three network services that are receiving maximum number of critical alerts in the network.
Top Services by POP CPU Usage	View the top three network services that are using the largest percentage of CPU from the assigned cores in the network.

Table 102 on page 301 shows the descriptions of the fields on the Network Services page.

Table 102: Fields on the Network Services Page

Field	Description
Name	View the name of the network service. Click the name to view full information about a service.
Tenants	View the number of tenants and the names of the tenants that have access to this nnetwork service. • View the name of the first tenant that used the network service (left of the table cell). • View the additional number of tenants using this network service (right of the table cell). • Hover over the additional number of tenants to view a complete list of all the tenants using this network service.
Sites	View the total number of sites at which the network service is deployed for the tenant.
Instances	View the total number of occurrences of the network service that administrative users have activated for the tenant.
Last Update	View the date on which the network service designer last modified the service.

Table 103 on page 301 shows the descriptions of the fields on the Detail for *Service-Name* page.

Table 103: Fields on the Service Detail Page

Field	Description
General Information	
Type	View the category of service.
Configuration	View the settings that the network service designer or you have configured for this service.
Version	View the version number of the network service.
State	View the status of the network service. Example: Published
Performance Goals	View performance of the network service which include bandwidth, number of sessions, and latency.

RELATED DOCUMENTATION

Network Services Overview | 299

About the Service Overview Page | 302

About the Service Instances Page | 304

About the Service Overview Page

To access this page, click **Configuration > Network Services > *Service Name* > Overview**.

You can use the Service Overview page to view information about a service that the service designer has published to the network service catalog from Network Service Designer.

Tasks You Can Perform

You can perform the following tasks from this page:

- View administrative details about the service. See *General Information* in Table 104 on page 302.
- View resources required for the service and its performance specification. See *Service Requirements* and *Service Performance* in Table 104 on page 302.
- View the service chain, with its constituent VNFs. See *Service Configuration* in Table 104 on page 302.

Field Descriptions

Table 104 on page 302 provides guidelines on using the fields on the Service Overview page.

Table 104: Fields on the Service Overview Page

Field	Description
General Information	
Description	View a summary about the service's capabilities. The network service designer provides this summary.

Table 104: Fields on the Service Overview Page *(continued)*

Field	Description
State	View the state of the network service: • Discontinued—Service is no longer available for customers. • Published—Service designer has published service to network catalog, and it is available for customers.
Tenants	View the number of tenants using this service.
Service Requirements	
CPU	View the number of CPUs that the service needs (cores).
Memory	View the amount of RAM that the service needs in gigabytes (GB).
Service Performance	
Sessions	View the number of sessions concurrently supported by one instance of the service.
Bandwidth	View the data rate for the service in megabytes per second (Mbps) or gigabytes per second (Gbps).
Latency	View the time a packet takes to traverse the service in milliseconds (ms) or nanoseconds (ns).
License cost	Specify the license cost for the network service in USD.
Service Configuration (graphic of the service chain)	
I	View the ingress point—the point at which packets enter the service.
E	View the egress point—the point at which packets exit the service.
One or more VNFs	Click to view settings for the VNF. The service designer can configure the VNF settings in Network Service Designer and the administrative user can configure the VNF settings in Customer Portal. **BEST PRACTICE:** The network service designer configures settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and the administrative user configures settings for the service, such as policies. The service designer can also configure a few example settings for the service. These example settings should be generic and not network-specific.

RELATED DOCUMENTATION

About the Network Services Page | 300

About the Service Instances Page

To access this page, click **Configuration > Network Services** > *Service Name* > **Instances**

You can use the Service Instances page to view information about occurrences of the service at specific customer sites.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a service instance. Click the details icon that appears when you hover over the name of a service. See Table 106 on page 305.
- Enable or disable a network service or virtualized network function (VNF) recovery. Select a service instance and click **Enable Auto Healing** to enable automatic recovery of a network service. By default, automatic recovery of a network service or VNFs is enabled.

Field Descriptions

Table 105 on page 304 shows the descriptions of the fields on the Service Instances page.

Table 105: Fields on the Service Instances Page

Field	Description
Name	View the name of the occurrence of a service at a specific tenant site.
Tenant	View the name of the tenant.
Status	View the state of the service at the customer site: • Created—Administrative user for the tenant has enabled this service instance, which is active. • Blank—Administrative user for the tenant has disabled this service instance.

Table 105: Fields on the Service Instances Page *(continued)*

Field	Description
Site	View the name of the site at which service occurrence is available.
POP	View the POP in which the site is located.
Functions	View network functions that the service offers; for example, Network Address Translation (NAT) or firewall.

Table 106 on page 305 shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

Table 106: Fields on the Service Instance Details Page

Field	Description
General	
Description	View information about this service instance. This information is generated from data in Customer Portal.

RELATED DOCUMENTATION

- Network Services Overview | 299
- About the Network Services Page | 300

Allocating a Service to Tenants

NOTE: Only a service provider administrator can allocate services to tenants.

For a tenant to have access to a service, you must assign the service to the tenant. You can assign a service to multiple tenants simultaneously; however, you can assign only one service at a time.

To assign a service to tenants:

1. Select **Configuration > Network Services**.

   The Network Services page appears.

2. Select the service that you want to assign to the tenants.

3. Click **Allocate Services**.

   The Tenants: Select Tenant(s) to allocate the Service page appears.

4. Select the tenants to which you want to assign the service.

5. Click **OK** to save the changes.

RELATED DOCUMENTATION

About the Network Services Page | 300

Removing a Service from Tenants | 306

Removing a Service from Tenants

NOTE: Only a service provider administrator can remove services allocated to tenants.

You can remove a service from one or more tenants simultaneously. You can only remove one service at a time, however.

To remove a service from tenants:

1. Click **Configuration > Network Services**.

   The Network Services page appears.

2. Select the service that you want to remove from the tenants.

3. Click **Detach Services**.

   The Detach Service from Tenants page appears.

4. Select the tenants from which you want to remove the service.

5. Click **Ok**.

RELATED DOCUMENTATION

About the Network Services Page | **300**

Allocating a Service to Tenants | **305**

7

CHAPTER

Managing Signatures

Signature Database Overview | **309**

About the Signature Database Page | **309**

Downloading a Signature Database | **311**

Download Locations for Signature Database | **313**

Application Signatures Overview | **314**

About the Application Signatures Page | **315**

Understanding Custom Application Signatures | **317**

Adding Application Signatures | **318**

Editing, Cloning, and Deleting Application Signatures | **324**

Adding Application Signature Groups | **326**

Editing, Cloning, and Deleting Application Signature Groups | **327**

Signature Database Overview

The signature database that Juniper provides contains application and intrusion prevention system (IPS) signatures:

- Application signatures are definitions of predefined attacks and applications, and can be used to identify applications for tracking firewall policies and quality-of-service (QoS) prioritization.
- IPS signatures are definitions of predefined attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.

Contrail Service Orchestration (CSO) enables users with the Service Provider (SP) administrator role to download the signature database. When you trigger a download, a job is created and the job might take some time to complete. You can track the progress of this job on the Jobs page.

After the signature download operation is complete, predefined signatures (application and IPS) and IPS profiles are available in CSO. You cannot modify predefined signatures or IPS profiles.

RELATED DOCUMENTATION

About the Signature Database Page | 309
Downloading a Signature Database | 311

About the Signature Database Page

To access this page, select **Administration** > **Signature Database**.

Use the Signature Database page to download the signature database, which contains intrusion prevention system (IPS) and application signatures. The signature database contains definitions of attacks and application, which are used in defining IPS profile rules and application firewall rules. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic.

Tasks You Can Perform

You can perform the following tasks from this page:

> **NOTE:** In Administration Portal, only users with the Service Provider (SP) Administrator role can download the signature database.

- Download the signature database—See "Downloading a Signature Database" on page 311.
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Signature Database page.

Field Descriptions

Table 107 on page 310 describes the fields on this page.

Table 107: Fields on the Signature Database Page

Field	Description
Active Database	
Database Version	Version of signature database.
Publish Date	Date and time (YYYY-MM-DD HH:MM:SS 24-hour format) when the signature database was published.
Update Job	Job ID of the last successful download signatures job. Click the hyperlinked job ID to go to the Jobs page where you can view the details of the job.
Installed Device Count	Number of devices on which the signature database was successfully installed.
Detectors	Version numbers of the detector engines associated with the signature database. Click the *detector-versions* link to view the detector details. The Detector Details for *Signature-Database-Version* page appears displaying (in a table) the platform, OS version, and version of the detectors for the signature database. Click **Close** to return to the Signature Database page.

Table 107: Fields on the Signature Database Page *(continued)*

Field	Description
Latest List of Signatures	The available signature databases are listed in a table. You can search the list of signature databases by using the search option.
Database Version	Version of the signature database.
Publish Date	Date and time (YYYY-MM-DD HH:MM:SS 24-hour format) when the signature database was published.
Update Summary	Displays the summary of changes from the previous version of the signature database; for example, 6 new signatures, 1 updated signature, 1 renamed signature. Click the hyperlinked text to view the details of the updates. The Signature Update Details for Database *Version* page appears displaying (in a grid) the list of signatures updated and action (add, update, rename), the type, and the name for each signature. Click **Close** to return to the Signature Database page.
Detectors	Version numbers of the detector engines associated with the signature database. Click the *detector-versions* link to view the detector details. The Detector Details for *Signature-Database-Version* page appears displaying (in a table) the platform, OS version, and version of the detectors for the signature database. Click **Close** to return to the Signature Database page.
Action	Click the **Full Download** link to download the complete signature database; the download might take a while to complete. **NOTE:** This field is displayed only for users with the SP administrator role.

RELATED DOCUMENTATION

Signature Database Overview | 309

Downloading a Signature Database

Users with the Service Provider (SP) Administrator role can use the Signature Download Settings page to specify the URL from which the signature database must be downloaded and trigger the download of the

signature database. When you trigger a download, a job is created; and this job might take some time to complete. You can track the progress of the signature download job on the Jobs page.

To download the signature database:

1. Select **Administration > Signature Database**.

   The Signature Database page appears.

2. Click **Signature Download Settings**.

   The Signature Download Settings page appears.

3. Enter the download settings according to the guidelines provided in Table 108 on page 312.

4. Click **OK** to save the changes:

   - If you specified that the signature database should be downloaded immediately, a Job Tasks page appears displaying information about the signature download job. Click **OK** to close this page and return to the Signature Database page.
   - If you scheduled the signature download for later, a job is created and you are returned to the Signature Database page. A confirmation message (with the job ID) is displayed at the top of the page.

Table 108: Fields on the Signature Download Settings Page

Field	Description
Download URL	Specifies the location of the Juniper hosted server from which the signature database is downloaded to the CSO server. The default download URL is https://signatures.juniper.net/. To download signatures from this location, Internet connectivity must be available from CSO. If Internet connectivity from CSO is not available, you can download the signatures from a local source such as your laptop or any other web server connected through the intranet to CSO. To do this, enter the location from which you want to download the signatures in the **Download URL** field. For more information, see "Download Locations for Signature Database" on page 313.
Signature Version	**NOTE:** This field is enabled only when you change the download URL from https://signatures.juniper.net/. Enter the numeric value of the signature database version. The value must only contain numbers and not have any special characters or negative values.

Table 108: Fields on the Signature Download Settings Page *(continued)*

Field	Description

Type	You can chose to download the signature database immediately or schedule the download for later.
	• Select **Run now** to automatically download the signature database immediately.
	• Select **Schedule at a later time** to download the signature database later and specify the date and time, as follows:
	  ◦ Click on the calendar icon to choose the date for the download.
	  ◦ Enter the time for the download. You can choose the 12 hour (AM or PM) or 24 hour format to specify the time by selecting the option from the drop-down list provided beside the time field.
	NOTE: The time-zone is picked-up based on the time-zone specified when CSO is installed.

RELATED DOCUMENTATION

Signature Database Overview | 309
About the Signature Database Page | 309

Download Locations for Signature Database

In order to perform offline download of signature database or package, you must first download the signature database to a folder location on any webserver. You need to start a local webserver to host the signature database or package.

The following are the folder locations to which you must download the signature package or database for different servers:

- **Python server**—You can use the **python -m SimpleHTTPServer 8000** command to start an HTTP server on port 8000. You need to log in as the root user and then execute the command at the root directory of the server. You must download the signature package to the folder location **/space/2/*version*/**. Therefore, the URL of the downloaded signature package is ***IP address*: *portnumber* /space/2/*version*/*latest-space-update.zip***.

  For example, **10.213.18.101:8000/space/2/2981/*latest-space-update*.zip**
- **Apache server**—In Mac OS, you must download the signature package, *latest-space-update*.zip, to the folder location **/Library/WebServer/Documents/space/2/version/**.
- **Other servers**—For other servers, download the signature package, *latest-space-update*.zip, in the folder location **location /space/2/*version*/**.

RELATED DOCUMENTATION

Signature Database Overview

Application Signatures Overview

Juniper Networks regularly updates the predefined application signature database, making it available to subscribers on the Juniper Networks website. This database includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, and quality-of-service prioritization.

Use the **Application Signatures** page to get an overall, high-level view of your application signature settings. You can filter and sort this information to get a better understanding of what you want to configure.

RELATED DOCUMENTATION

About the Application Signatures Page | **315**

Adding Application Signature Groups | **326**

Editing, Cloning, and Deleting Application Signature Groups | **327**

About the Application Signatures Page

To access the **Application Signatures** page, select **Configuration** > **Shared Objects** > **Application Signatures**.

Use this page to view application signatures and application signature groups that are already downloaded and to create, modify, clone, and delete custom application signatures and custom application signature groups. This page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create custom application signatures and custom application signature groups with a set of similar signatures for consistent reuse when defining policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an application signature. See "Adding Application Signatures" on page 318.
- Modify, clone, or delete an application signature. See "Editing, Cloning, and Deleting Application Signatures" on page 324.
- Create an application signature group. See *Adding Application Signature Groups*.
- Modify, clone, or delete an application signature group. See *Editing, Cloning, and Deleting Application Signature Groups*.
- View the configured parameters of an application signature or application signature group— Hover over the application signature or group name and click the Detailed View icon or click **More > Detailed View**.

  The Detailed View page appears, displaying the same values that you specified for each parameter in the selected application or application signature group.
- Show or hide columns displayed on the page—Click the **Show Hide columns** icon in the top right corner of the table and select the columns that you want to view on the page.
- Search for a specific application signature or application signature group—Click the Search icon in the top right corner of the table and enter the search text in the text box, and press **Enter**. The search results are displayed on the same page.
- Filter the application signature information based on the selected criteria—Select the filter icon at the top right corner of the table to apply a filter. For example, you can filter information based on the object type (application signature or application signature group) or risk level (Low, Moderate, and so on).

  Click **Clear All** to remove the applied filter.

Field Descriptions

Table 109 on page 316 describes the fields on the **Application Signatures** page.

Table 109: Fields on the Application Signatures Page

Field	Description
Name	Name of the application signature or application signature group.
Object Type	Signature type—either application signature or application signature group.
Category	UTM category of the application signature. For example, the value of **Category** can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Subcategory	UTM subcategory of the application signature. For example, the value of **Subcategory** can be Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Level of risk associated with the application signature. For example, the value of **Risk** can be low, moderate, high, critical, unsafe, and so on.
Characteristic	One or more characteristics of the application signature. For example, supports file transfer, loss of productivity, and so on.
Predefined or Custom	A list of predefined application signatures and application signature groups, and a list of custom application and custom application signature groups that you created.
Cacheable	Indicates whether the information related to an application signature is cacheable (True) or non-cacheable (False).

RELATED DOCUMENTATION

Application Signatures Overview | 314
Adding Application Signature Groups | 326
Editing, Cloning, and Deleting Application Signature Groups | 327

Understanding Custom Application Signatures

Application identification supports user-defined custom application signatures to detect applications as they pass through the device. Custom application signatures are unique to your environment and are not part of the predefined application package. You use this custom application signature in SD-WAN policies and firewall policies to steer, and block traffic when a threat is detected.

Custom application signatures are required to:

- Control traffic particular to an environment.
- Bring visibility to unknown or unclassified applications.
- Identify Layer 7 applications or temporary applications, and to achieve further granularity of known applications.
- Perform QoS for your specific application.

CSO supports the following custom application signatures:

- ICMP-Based Mapping—The Internet Control Message Protocol (ICMP) mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages.
- IP Address-Based Mapping—Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic.

  To ensure adequate security, use address mapping when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy in handling traffic from a known application.

  With Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port range. When IP address and port range are configured, they must match the destination tuples (IP address and port range) of the packet.

  For example, consider a Session Initiation Protocol (SIP) server that initiates sessions from its known port 5060. Because all traffic from this IP address and port is generated by only the SIP application, the SIP application can be mapped to an IP address of the server and port 5060 for application identification. In this way, all traffic with this IP address and port is identified as SIP application traffic.
- IP Protocol-Based Mapping—Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
- Layer 7-Based Signatures—Layer 7 custom signatures define an application running over TCP or UDP or Layer 7 applications. Layer 7-based custom application signatures are required for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications

running on the same Layer 7 protocol. The custom signature is cacheable for Layer 7 signatures only. You can create multiple signatures and each signature can contain multiple members (maximum 15 members).

Layer 7-based custom application signatures detect applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS). Application identification can extract the server name information or the server certification from the TLS or SSL sessions. It can also detect patterns in TCP or UDP payload in Layer 7 applications.

RELATED DOCUMENTATION

Adding Application Signatures | 318

Editing, Cloning, and Deleting Application Signatures | 324

Adding Application Signatures

You can add custom application signatures for applications that are not part of the Juniper Networks predefined application database. When you add custom application signatures, make sure that your application signatures are unique, by providing a unique and relevant name.

You can add custom application signatures by specifying a name, protocol, port number where the application runs, and match criteria.

To create a custom application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.
2. Click **Create > Signature**.
3. Complete the configuration according to the guidelines provided in Table 110 on page 319.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature with your configurations is created. You use this application signature while creating SD-WAN policy and firewall policy intents.

Table 110 on page 319 provides guidelines on using the fields on the **Create Application Signature** page.

Table 110: Fields on the Create Application Signature Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature.
Signature Order and Priority	
Order	Enter the order for the custom application signature. A lower order value has higher priority. This option is used when multiple custom application signatures of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications. Range is 1-50000.
Priority	Specify the application signature priority (high or low) over other application signatures.
Signature Classification	
Category	Enter the category of the application signature. For example, Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Sub Category	Enter the subcategory of the application signature. For example, Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Select the level of risk associated with the application signature. For example, low, moderate, high, critical, unsafe, and so on.
Characteristics	Enter one or more characteristics of the application signature. For example, supports file transfer, loss of productivity, and so on.
Application Criteria	Enable one or more application matching criteria: • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature

Table 110: Fields on the Create Application Signature Page *(continued)*

Field	Description
ICMP Mapping	Click the toggle button to specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.
ICMP Type	Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. Range is 0-254.
ICMP Code	Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field. Range is 0-254.
IP Protocol Mapping	Click the toggle button to specify the IP protocol value for an application. This parameter is used to identify an application based on it's IP protocol value and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
IP Protocol	Enter an IP Protocol number for the application. Standard IP protocol numbers map an application to IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers. Range is 0-254. You can find a complete list of industry standard protocol numbers at the IANA website. **NOTE:** You cannot use IP protocol numbers 1(ICMP), 6(TCP) and 17(UDP) for custom application signature creation. Instead, we recommend you to use L7 signature policies for these protocols.

Table 110: Fields on the Create Application Signature Page *(continued)*

Field	Description
Address Mapping	Click the toggle button to specify address mapping information. Layer 3 and Layer 4 address mapping defines an application by matching the destination IP address or port range (optional) of the traffic. Use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy while handling traffic from a known application. For more information, see Table 111 on page 321. **NOTE:** • You must specify either IP address or TCP/UDP port range for address mapping. • If both IP address and TCP/UDP ports are configured, both should match destination tuples (IP address and port range) of the packet.
L7 Signature	Click the toggle button to specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols. Configure a custom signature based on L7 applications. You create Layer 7-based custom application signatures for the identification of multiple applications running on the same L7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. For more information, see Table 112 on page 322.
Cacheable	Click the toggle button to enable caching of application identification results on the device. Enable this option to **True** only when L7 signatures are configured alone in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.

Table 111: Fields on the Add IP Address Mapping Page

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.
IP Address	Enter the destination IPv4 or IPv6 address of the application.
CIDR	Enter a CIDR value for the IP Address that you assign to the application. Range for IPv4 address is 1-32. Range for IPv6 address is 1-128.

Table 111: Fields on the Add IP Address Mapping Page *(continued)*

Field	Description
TCP Port range	(Optional) Enter space-separated list of ports or port ranges to match a TCP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 80-82 443.
UDP port range	(Optional) Enter space-separated list of ports or port ranges ranges to match an UDP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535. Example: 160-162 260.

Table 112: Fields on the Add Signature Page

Field	Description
Over Protocol	Displays the signature to match the application protocol. Example: HTTP.
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Port Range	Enter the port range for the application. Range is 0-65535 Example: 80-82,443
Add Members	Click the plus icon (+) to add the member details.
Member No.	Enter the member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01—m15.)

Table 112: Fields on the Add Signature Page *(continued)*

Field	Description

Context	Select the service-specific context.
	• For L7 Signatures over HTTP, select any of the following context:
	  ◦ http-get-url-parsed-param-parsed
	  ◦ http-header-content-type
	  ◦ http-header-cookie
	  ◦ http-header-host
	  ◦ http-header-user-agent
	  ◦ http-post-url-parsed-param-parsed
	  ◦ http-post-variable-parsed
	  ◦ http-url-parsed
	  ◦ http-url-parsed-param-parsed
	• For L7 Signatures over SSL, select the service-specific context as **ssl-server-name**.
	• For L7 Signatures over TCP, select the service-specific context as **stream**.
	• For L7 Signatures over UDP, select the service-specific context as **stream**.
	For possible combinations of context and direction for L7 application creation, refer context (Application Identification).

Direction	Select the direction of the packet flow to which the signature must be matched. • any—The direction of packet flow can either be from client-side to server-side or from server-side to client-side. • client-to-server—The direction of packet flow is from client-side to server-side. • server-to-client—The direction of packet flow is from server-side to client-side.
Pattern	Enter the deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.

RELATED DOCUMENTATION

Understanding Custom Application Signatures | 317

Editing, Cloning, and Deleting Application Signatures | 324

Adding SLA-Based Steering Profiles | 357

Adding Path-Based Steering Profiles | 369

Editing, Cloning, and Deleting Application Signatures

IN THIS SECTION

- Editing Application Signatures | 324
- Cloning Application Signatures | 325
- Deleting Application Signatures | 325

You can edit, clone, and delete application signatures from the **Application Signatures** page.

Editing Application Signatures

To modify the parameters configured for a cloned user-created (custom) application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature that you want to edit, and then click on the edit icon (pencil), on the top right corner of the table, or right-click and select **Edit Application Signature**.

   The **Edit Application Signature** page appears, showing the same options as those displayed when you create a new application signature.

3. Modify the parameters according to the guidelines provided in “Adding Application Signatures” on page 318.

4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature appears on the **Application Signatures** page.

Cloning Application Signatures

You can clone a custom application signature when you want to reuse an existing application signature, but with a few minor changes. This way, you can save time recreating the application signature from scratch.

To clone a custom application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature that you want to clone, and then select **More > Clone**, or right-click the application signature and then select **Clone**.

   The **Clone** page appears with editable fields.

3. Modify the fields as required. Refer to the guidelines provided in "Adding Application Signatures" on page 318

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The cloned application signature is displayed on the **Application Signatures** page.

Deleting Application Signatures

To delete a cloned user-created (custom) application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature you want to delete and then click the delete icon.

   An alert message appearsto verify that you want to delete the selected application signature.

3. Click **Yes** to delete the selected application signature. If you do not want to delete, click **Cancel** instead.

The deleted application signature is removed from the Application Signatures page.

RELATED DOCUMENTATION

Understanding Custom Application Signatures | 317
Adding Application Signatures | 318

Adding Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you create custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

To create an application signature group:

1. Select **Configure > Shared Objects > Application Signatures**.
2. Click **Create > Signature Group**.
3. Complete the configuration according to the guidelines provided in Table 113 on page 326.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature group with your configurations is created. You can use this application signature group in firewall, NAT, and SD-WAN policies.

Table 113 on page 326 provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 113: Fields on the Create Application Signature Group Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature group.
Group Members	Click the add icon (+) to add signatures to your application group. On the **Add Application Signatures** page, select the check boxes next to the signatures you want to add to the group and click **OK**.

RELATED DOCUMENTATION

Application Signatures Overview | 314
About the Application Signatures Page | 315
Editing, Cloning, and Deleting Application Signature Groups | 327

Editing, Cloning, and Deleting Application Signature Groups

IN THIS SECTION

- Editing Application Signature Groups | 327
- Cloning Application Signature Groups | 328
- Deleting Application Signature Groups | 328

You can edit, clone, and delete application signature groups from the **Application Signatures** page.

Editing Application Signature Groups

To modify the parameters configured for an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature group that you want to edit, and then select **More > Edit**, or click on the edit icon (pencil symbol), on the top right corner of the table, or right-click and select **Edit**.

   The **Edit** page appears, showing the same options as those displayed when you create a new application signature group.

3. Modify the parameters according to the guidelines provided in "Adding Application Signature Groups" on page 326.

4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature group appears in the **Application Signatures** page.

Cloning Application Signature Groups

You can clone an application signature group when you want to reuse an existing application signature group, but with a few minor changes. This way, you can save time recreating the application signature group from the start.

To clone an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Right-click the application signature group that you want to clone and then select **Clone**, or select **More > Clone**.

   The **Clone** page appears with editable fields.

3. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

The cloned application signature group is displayed on the **Application Signatures** page.

Deleting Application Signature Groups

To delete an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature group you want to delete and then click the delete icon **(X)** .

   An alert message appears, verifying that you want to delete the selected item.

3. Click **Yes** to delete the selected application signature group. If you do not want to delete, click **Cancel** instead.

RELATED DOCUMENTATION

Application Signatures Overview | 314
About the Application Signatures Page | 315
Adding Application Signature Groups | 326

8
CHAPTER

Managing Profiles

Application Quality of Experience Overview | **332**

Configure and Monitor Application Quality of Experience | **334**

About the Application Traffic Type Profiles Page | **335**

Predefined Application Traffic Type Profiles | **338**

Add Traffic Type Profiles | **340**

Edit and Delete Application Traffic Type Profiles | **346**

SLA Profiles and SD-WAN Policies Overview | **348**

About the SLA-Based Steering Profiles Page | **354**

Adding SLA-Based Steering Profiles | **357**

Editing and Deleting SLA-Based Steering Profiles | **364**

About the Path-Based Steering Profiles Page | **366**

Adding Path-Based Steering Profiles | **369**

Editing and Deleting Path-Based Steering Profiles | **371**

About the Breakout Profiles Page | **373**

Adding Breakout Profiles | **376**

Application Quality of Experience Overview

IN THIS SECTION

- Benefits of Application Quality of Experience | 333

Contrail Service Orchestration (CSO) supports Application Quality of Experience (AppQoE) that enables you to effectively prioritize, segregate, and route business-critical application traffic without compromising performance or availability.

AppQoE utilizes the capabilities of two application security services:

- Application identification (AppID) to identify specific applications in your network.
- Advanced policy-based routing (APBR) to specify a path for the application traffic.

AppQoE-enabled devices perform service- level agreement (SLA) measurements across the available WAN links, and then dynamically map the application traffic to the path that best serves the application's SLA requirement.

NOTE: AppQoE is applicable only for SD-WAN sites.

AppQoE is supported on the following devices in both hub-and-spoke and full mesh topologies:

- vSRX instances
- SRX300 series
- SRX550M
- SRX1500
- SRX4100
- SRX4200

You can configure an AppQoE between two SRX Series device endpoints (book-ended) when both the devices run the same version of Junos OS.

CSO pushes the SLA parameters, path selection parameters and related configuration to the device and the device monitors the links for SLA violation. If there is a violation, the device switches the link and generates **APPQOE_(APP)_SLA_METRIC_VIOLATION** and **APPQOE_BEST_PATH_SELECTED** system

log messages. The device also aggregates and averages the SLA metrics, and generates periodic **APPQOE_APP_PASSIVE_SLA_METRIC_REPORT** system log messages.

AppQoE measures the application performance across multiple links by collecting real-time data by continuously the monitoring application traffic and identifying any network or device issues by sending active and passive probes. To monitor the SLA compliance of the link on which the application traffic is sent, the Customer Premises Equipment (CPE) device sends inline probes (called passive probes) along with the application traffic. Additionally, to identify the best available link for an application if the active link fails to meet the SLA criteria, the CPE constantly monitors and collects the SLA compliance data for the other available links by sending probes (called active probes) over the links. The active probes are sent based on the probe parameters that you configure in the application traffic type profile.

The CPE device switches links at the application level, which means that only the traffic corresponding to the application that reported the SLA violation is moved to a link that meets the specified SLA. Traffic for the remaining applications remain on the same link until those applications report an SLA violation.

You can configure traffic type profiles to specify the class of service (CoS) and probe parameters for each traffic type. When you add a steering profile (SLA-based or path-based), you specify the SLA parameters and SLA sampling criteria, and link the steering profile with a traffic type profile. The steering profile is then linked to an SD-WAN policy intent and the SD-WAN policy is deployed to enable AppQoE.

You can view the SLA performance details of all tenants from the Tenant SLA Performance (**Monitor > Tenant SLA Performance**) page. For more information on the AppQoE workflow, see “Configure and Monitor Application Quality of Experience” on page 334.

Benefits of Application Quality of Experience

- Enables cost-effective QoE by real-time monitoring of application traffic, which provides a consistent and predictable level of service.
- Improves the user experience at the application level by ensuring that the application data is sent over the most SLA-compliant link.

RELATED DOCUMENTATION

Application Quality of Experience

Configure and Monitor Application Quality of Experience

Application Quality of Experience (AppQoE) improves the user experience by constantly monitoring the class of service (CoS) parameters and service-level agreement (SLA) compliance of the available WAN links, ensuring that the application data is sent over the most SLA-compliant link. For more information, see "Application Quality of Experience Overview" on page 332.

As an SP administrator user, to configure and monitor AppQoE in Administration Portal:

1. Review the "Predefined Application Traffic Type Profiles" on page 338 and enable the required profiles. You can also "modify the default profiles" on page 346 or "add new profiles" on page 340.

   NOTE: This step is applicable only for on-premise version of Contrail Service Orchestration (CSO).

2. Add a tenant with SD-WAN service. For more information, see "Adding a Single Tenant" on page 79.

3. Add an SLA-based steering profile or a path-based steering profile and associate an application traffic type profile with the added steering profile. For more information, see "Adding SLA-Based Steering Profiles" on page 357 or "Adding Path-Based Steering Profiles" on page 369.

4. Change the scope to the tenant you added previously.

5. Add an SD-WAN policy intent that references to the steering profile you added previously. For more information, see *Creating SD-WAN Policy Intents* in the *Customer Portal User Guide*.

   NOTE: Before you deploy an SD-WAN policy, ensure that you have added one or more SD-WAN sites. For more information, see *About the Sites page* in *Customer Portal User Guide*.

6. Deploy the SD-WAN policy intent on one or more SD-WAN sites to deploy AppQoE. For more information, see *Deploying Policies* in *Customer Portal User Guide*.

7. View the SLA performance details of all the sites in the tenant on the Application SLA Performance page (**Monitor > Application SLA Performance**). For more information, see *About the SLA Performance of a Single Tenant Page* in *Customer Portal User Guide*.

NOTE: As an SP administrator user, you can view the SLA performance details of all tenants on the Tenants SLA Performance page (**Monitor > Tenants SLA Performance**). For more information, see "Monitoring Application-Level SLA Performance for Secure SD-WAN-Advanced" on page 467.

RELATED DOCUMENTATION

About the Application Traffic Type Profiles Page | 335

About the SLA-Based Steering Profiles Page | 354

About the Application Traffic Type Profiles Page

IN THIS SECTION

- Tasks You Can Perform | 336
- Field Descriptions | 336

To access this page from Administration Portal, select **Configuration** > **Application Traffic Type Profiles**.

You can use the **Application Traffic Type Profiles** page to:

- configure class-of-service parameters for various traffic types based on your specific business requirements.
- assign a priority and service-level criteria to the traffic types.

Application traffic type profiles are used in path-based steering, SLA-based steering, and breakout profiles.

Contrail Service Orchestration (CSO) provides predefined application traffic type profiles. For more information, see "Predefined Application Traffic Type Profiles" on page 338.

Tasks You Can Perform

You can perform the following tasks from this page:

> **NOTE:** Starting from CSO 5.4.0 Release, in addition to an SP administrator, an OpCo administrator can also create, edit, and delete traffic type profiles.

- View details of the application traffic type profiles. To view more details about each profile, click the details icon that appears when you hover over the name of the application traffic type profile. Alternatively, select the application traffic type profile and click **More** > **Detail**.

  The **Details for <Application-Traffic-Type-Profile>** pane appears on the right side of the page.
- Add an application traffic type profile. See "Add Traffic Type Profiles" on page 340.
- Edit or delete an application traffic type profile. See "Edit and Delete Application Traffic Type Profiles" on page 346.
- Show or hide columns that contain information about the application traffic type profiles. Click the **Show/Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for application traffic type profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

Table 114 on page 336 describes the fields on the Application Traffic Type Profiles page and Details for <Application-Traffic-Type-Profile> Pane.

Table 114: Fields on Application Traffic Type Profiles Page and Details for <Application-Traffic-Type-Profile> Pane

Field	Description	Displayed In
Name	Name of the application traffic type profile.	Application Traffic Type Profiles Page

Table 114: Fields on Application Traffic Type Profiles Page and Details for <Application-Traffic-Type-Profile> Pane *(continued)*

Field	Description	Displayed In
Priority	Priority level of the application traffic type profile (arranged in decreasing order of priority): • S-High (Strict high) • M-High (Medium high) • High • M-Low (Medium low) • Low	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
Status	Status (enabled or disabled) of the application traffic type profile.	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
Probe Parameters	Displays the probe parameters configured for the application traffic type profile: • Data Size: Size (in bytes) of the data packet. • Probe Interval: Interval (in seconds) between the time that two probes are sent. • Probe Count: Number of probes to be evaluated to assess service-level agreement (SLA) compliance of the link. • Burst Size: Maximum number of probes that can be sent at a time.	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
DSCP Value	Differentiated Services Code Point (DSCP) value assigned to the application traffic type profile. DSCP values define the forwarding properties of the packet within the Differentiated Services framework.	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
IEEE802.1P Value	IEEE802.1p values assigned to the application traffic type profile. The IEEE802.1p value specifies the QoS at the media access control (MAC) level	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
Bandwidth	Minimum and maximum bandwidth allocation (as percentage of the total available bandwidth) for the application traffic type profile.	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane

Table 114: Fields on Application Traffic Type Profiles Page and Details for <Application-Traffic-Type-Profile> Pane *(continued)*

Field	Description	Displayed In
Buffer	Buffer allocation (in percentage) for the application traffic type profile.	Application Traffic Type Profiles Page Details for <Application-Traffic-Type-Profile> Pane
Created by	Name of the user who created the application traffic type profile.	Application Traffic Type Profiles Page

RELATED DOCUMENTATION

- *About the SLA-Based Steering Profiles Page*
- *About the Path-Based Steering Profiles Page*

Predefined Application Traffic Type Profiles

Table 115 on page 338 lists the predefined application traffic type profiles provided by Contrail Service Orchestration (CSO) and the default parameters for each profile.

Table 115: Predefined Application Traffic Type Profiles and Parameters

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
High Priority Video	Low	20%	Minimum: 20% Maximum: 25%	Data size (bytes)	64	af31
				Probe interval (seconds)	30	
				Probe count	10	
				Burst size	1	

Table 115: Predefined Application Traffic Type Profiles and Parameters *(continued)*

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
Premium-Internet	Low	10%	Minimum: 12% Maximum:15%	Data size (bytes)	64	af12
				Probe interval (seconds)	20	
				Probe count	10	
				Burst size	2	
Internet	Low	5%	Minimum: 15% Maximum: 20%	Data size (bytes)	64	af11
				Probe interval (seconds)	10	
				Probe count	5	
				Burst size	1	
Hosted-AV	Low	10%	Minimum: 16% Maximum: 20%	Data size (bytes)	64	af32
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	

Table 115: Predefined Application Traffic Type Profiles and Parameters *(continued)*

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
Voice-Video	Low	5%	Minimum: 20% Maximum: 20%	Data size (bytes)	64	af41
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	

NOTE:

- By default, Voice-Video, Internet, and Premium-Internet application traffic type profiles are enabled on the on-premise and cloud versions of CSO. In the cloud version of CSO, the Juniper team can enable additional profiles, add new profiles, and edit or delete the existing profiles on a need-basis. In the on-premise version of CSO, the Service Provider (SP) administrator user can enable additional profiles, create new profiles, edit or delete the existing application traffic type profiles.
- You can enable a maximum of six application traffic type profiles at a time.
- The total buffer allocation of the enabled traffic type profiles cannot exceed 100%.

RELATED DOCUMENTATION

About the SLA-Based Steering Profiles Page

About the Path-Based Steering Profiles Page

Add Traffic Type Profiles

You can use traffic type profiles to configure class-of-service parameters for various types of traffic. Traffic type profiles enable you to configure class-of-service parameters based on your specific business

requirements, and assign priority and service level criteria for traffic types. You can link an application traffic type profile with a steering profile, which can be linked to an SD-WAN policy intent.

> **NOTE:** The Add Traffic Type Profiles operation can be performed by users with an SP Administrator role or an OpCo administrator role.

To add an application traffic type profile:

1. Select **Configuration** > **SD-WAN** > **Application Traffic Type Profiles**.

   The **Application Traffic Type Profiles** page appears.

2. Click the Add (**+**) icon.

   The **Create New Traffic Type Profile** page appears.

3. Configure the traffic type profile parameters as per the guidelines provide in Table 116 on page 341.

   > **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   A confirmation message appears indicating the job is created for adding a traffic type profile. You can view the status of the job from the Jobs page (Monitor > Jobs).

   After the job is complete, the traffic type profiles that you configured appear on the Application Traffic Type Profiles page.

Table 116: Fields on the Create Traffic Type Profiles page

Field	Description
General	
Name	Enter a unique name that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.

Table 116: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
Priority	Select the priority value that you want to assign to the traffic type profile. The following list is arranged in the decreasing order of priority, where the first item indicates the highest priority and the fifth item, the lowest priority. 1. **S-High**, which denotes strict high or the highest priority. 2. **M-High**, which denotes medium high. 3. **High** 4. **M-Low**, which denotes medium low. 5. **Low** When network congestion occurs, traffic type profiles with higher priority take precedence over the ones with lower priority. **NOTE:** You can enable only one profile with S-High and one profile with High priority at any given time
Status	Click the toggle button to enable the traffic type profile. By, default, the traffic type profile is disabled. You can enable a maximum of six traffic profiles at a time. You can assign only those traffic type profiles that are marked as enabled to application SLA profiles.
Quality of Service	
Probe Parameters	The following are the parameters for probes that are sent on links other than the active links: • Data Size • Probe Interval • Probe Count • Burst Size Probe results are used to verify the SLA compliance of links and to identify the best available link to which traffic can be routed if the active link fails to meet SLA.
Copy probe parameters from	You can select an existing traffic type profile from the **Copy probe parameters from** list to copy the probe parameters from that profile, and, if required, modify the values.
Data Size	Specify the size of the data packets, in bytes, to be used for active probes. Range: 4 through 256.

Table 116: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
Probe Interval	Specify the interval, in seconds, between two probes. Range: 1 through 10.
Probe Count	Specify the number of probes within a test packet. Range: 10 through 1000.
Burst Size	Specify the maximum number of probes that can be sent in one go. The burst size must be less than or equal to the probe count. Range: 10 through 100.
Bandwidth	

Table 116: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
DSCP Value	Choose the Differentiated Services Code Point (DSCP) value that you want to assign to the traffic type profile. DSCP values define the forwarding properties of the packet within the Differentiated Services framework. You can assign an Expedited Forwarding (ef), an Assured Forwarding (af), the Best Effort (be), or a Class Selector (CS) value. Class Selector value provides backward compatibility with IP Precedence. You can choose one of the following DSCP values: **NOTE:** For a traffic profile you assign only one type of DSCP value. . • ef • af11 • af21 • af22 • af23 • af31 • af32 • af33 • af41 • af42 • af43 • be • cs1 • cs2 • cs3 • cs4 • cs5 • nc2/cs7

Table 116: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
IEEE 802.1P Value	Select an IEEE 802.1p value to assign to the traffic type profile. IEEE 802.1p value specifies the QoS at the media access control (MAC) level. You can assign an Expedited Forwarding (ef), an Assured Forwarding (af), the Best Effort (be), or a Class Selector (CS) for the IEEE 802.1p Value. You can choose one of the following values: • None • be (000) • be1 (001) • ef (010) • ef1 (011) • af11 (100) • af12 (101) • nc1 (110) • nc2 (111) • cs6 (110) • cs7 (111)
Drop Priority	Drop priority, in case of congestion. The values for drop priority in order of high-to-low is: • Strict High • High • Medium-High • Medium-Low • Low
Minimum Bandwidth	(Optional) Move the slider button to choose the minimum bandwidth, as percentage of the total available bandwidth, that you want to allocate to the traffic type profile. The minimum bandwidth value denotes the guaranteed bandwidth allocation for the traffic type.
Maximum Bandwidth	(Optional) Move the slider button to choose the maximum bandwidth, as percentage of the total available bandwidth, that you want to allocate to the traffic type profile. The bandwidth allocation for a traffic type never exceeds the maximum bandwidth configured for the traffic type.
Buffer	

Table 116: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
Allocation	Move the slider button to choose the bandwidth buffer that you want to allocate to the traffic type profile. Buffer allocation enables interfaces to queue and transmit traffic when there are large bursts of traffic and thus reduces the packet loss when network congestions occur. You can specify the buffer allocation as a percentage of the total available delay buffer. **NOTE:** The total buffer allocation of all the traffic type profiles that are in enabled state cannot exceed 100%.

RELATED DOCUMENTATION

About the Application Traffic Type Profiles Page | 335
Edit and Delete Application Traffic Type Profiles | 346

Edit and Delete Application Traffic Type Profiles

IN THIS SECTION

Edit Application Traffic Type Profiles | 347
Delete Application Traffic Type Profiles | 347

Users with the Service Provider (SP) Administrator role (on-premises installation only) or Operating Company (OpCo) Administrator role can modify the parameters of existing application traffic type profiles and delete application traffic type profiles that are no longer being used.

Edit Application Traffic Type Profiles

To edit an application traffic type profile:

1. Select **Configuration** > **Application Traffic Type Profiles**.

   The **Application Traffic Type Profiles** page appears.

2. Select the application traffic type profile that you want to modify and click the **Edit** icon.

   The **Edit Traffic Type Profile** page appears displaying the same fields that are presented when you add an application traffic type profile.

3. Modify the fields as required.

   Refer to "Add Traffic Type Profiles" on page 340 for an explanation of the fields.

   NOTE: You cannot modify the name of the application traffic type profile.

4. Click **OK** to save the changes.

   The modifications are saved and you are returned to the Application Traffic Type Profiles page, where a confirmation message appears.

   If you edit a traffic type profile that is associated with a steering or breakout profile and the traffic type profile is used in an SD-WAN policy intent that was previously deployed, you must redeploy the SD-WAN policy for the changes to take effect.

Delete Application Traffic Type Profiles

You can delete an application traffic type profile only if both the following conditions hold good:

- The traffic type profile is disabled.

  To delete a traffic type profile that's enabled, edit the profile and disable it, and then trigger the deletion.

- The traffic profile is not associated with a steering or breakout profile.

  To delete a traffic type profile that's associated with a steering or breakout profile, do one of the following:

  - Edit the traffic type profile to remove the steering or breakout profile, disable the traffic type profile, and then trigger the deletion.

- Delete the associated steering or breakout profile, disable the traffic type profile, and then trigger the deletion.

To delete an application traffic type profile:

1. Select **Configuration** > **Application Traffic Type Profiles**.

   The **Application Traffic Type Profiles** page appears.

2. Select the application traffic type profile that you want to delete and click the **Delete** icon.

   The **Confirm Delete** page appears asking you to confirm the delete operation.

3. Click **Yes**.

   You are returned to the **Application Traffic Type Profiles** page.

   If the selected application traffic type profile is disabled and is not associated with a steering or breakout profile, the application traffic type profile is deleted and a confirmation message appears.

SEE ALSO

About the SLA-Based Steering Profiles Page

About the Path-Based Steering Profiles Page | 366

About the Breakout Profiles Page | 373

SLA Profiles and SD-WAN Policies Overview

IN THIS SECTION

Traffic-Based Steering Profiles | 349

SD-WAN Policies | 352

Contrail Service Orchestration (CSO) enables you to add traffic-based steering profiles and map them to software-defined WAN (SD-WAN) policies for traffic management.

Traffic-Based Steering Profiles

Traffic-based steering profiles are created for applications or groups of applications for all tenants. Traffic-based steering profiles are categorized as follows:

- SLA-Based Steering Profiles—An SLA-based steering profile consists of a set of configurable constraints such as SLA configuration, SLA threshold, SLA parameters, path selection criteria, Class of Service, and upstream and downstream data rates.

  NOTE: The Secure SD-WAN Essentials service does not support SLA-based steering profiles.

- Path-Based Steering Profiles—A path-based steering profile consists of a set of configurable constraints such as path preference, traffic type profiles, and upstream and downstream data rates.
- Breakout Profiles—A breakout profile consists of set of configurable constraints such as type of breakout, traffic type profiles, path preference, and upstream and downstream data rates. A cloud breakout profile is added by Contrail Service Orchestration (CSO) by default.

Table 117 on page 349, Table 118 on page 350 and Table 119 on page 351 lists the categories of configurable constraints that are defined in an SLA-based profile, path-based profile and breakout profiles.

Table 117: SLA-Based Profile Categories

Category	Description

SLA profile parameters	You can define one or more than one of the following SLA profile parameters:
	• SLA Configuration—Whether to use recommended or custom values for the SLA threshold and SLA parameters.
	• SLA Threshold—Whether to use, liberal, baseline, or conservative settings for the threshold.
	• SLA parameters:
	  ◦ Packet loss—Percentage of data packets dropped by the network to manage congestion.
	  ◦ RTT—Target round-trip time (RTT) for the SLA profile.
	  ◦ Jitter—Difference between the maximum and minimum round-trip times (in ms) of a packet of data.

Path preference and failover	Paths are the WAN links to be used for the SLA profile. You can select MPLS, Internet, or any link as the preferred path. MPLS is more latency-sensitive than Internet. You can trigger the path failover criteria when any of the SLA parameters is violated, or when all the SLA parameters are violated.

Table 117: SLA-Based Profile Categories *(continued)*

Category	Description
Class of service	Class of service (CoS) provides different levels of service assurances to various forms of traffic. CoS enables you to divide traffic into classes and offer an assured service level for each class. The classes of service listed in increasing order of priority and sensitivity to latency are best effort, voice, interactive video, streaming audio or video, control, and business essential. The default CoS is voice.
Rate limiters	Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters: • Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. • Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.

Table 118: Path-Based Profile Categories

Category	Description
Path preference	Paths are the WAN links to be used for the SLA profile. You can select an MPLS or Internet link as the preferred path. MPLS is more latency-sensitive than Internet.
Class of service	Class of service (CoS) provides different levels of service assurances to various forms of traffic. CoS enables you to divide traffic into classes and offer an assured service level for each class. The classes of service listed in increasing order of priority and sensitivity to latency are best effort, voice, interactive video, streaming audio or video, control, and business essential. The default CoS is voice.
Rate limiters	Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters: • Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. • Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.

Table 119: Breakout Profile Categories

Category	Description
Type	The type of breakout profile that you want to add: • **Local Breakout (Underlay)**—Select this option if you want traffic to break out locally (on the underlay) from the site. • **Backhaul**—Select this option if you want traffic to break out through a hub or a enterprise hub (if configured). • **Local Breakout (Cloud)**—Select to break out traffic through a cloud-based security platform. Currently, Zscaler is the only cloud-based security platform supported.
Traffic Type Profile	The traffic type profile to apply class of service parameters to the breakout traffic. You can select only a traffic type profile that is enabled.
Preferred Path	The preferred path (MPLS, Internet, or Any) to be used for breaking out the traffic. If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic. If you specify that any path can be used, then there is no preference and all breakout-enabled links are used in a load-balancing mode.
Rate Limiting	Rate limiting of breakout traffic for cacheable applications. By default, rate limiting is disabled. If you enable rate limiting, you must specify the upstream and downstream parameters, and the loss priority.
Upstream Rate	The maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Upstream Burst Size	The maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the upstream rate limit for short periods.
Downstream Rate	The maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Downstream Burst Size	The maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the downstream rate limit for short periods.
Loss Priority	Loss priority based on which packets are dropped or retained when network congestion occurs. Packet drops are most likely when the loss priority is High and least likely when the loss priority is Low.

SD-WAN Policies

SD-WAN policy intents help in optimum utilization of the WAN links and efficient load distribution of traffic. SD-WAN policy intents are applied to source endpoints (such as sites and departments) and destination endpoints (applications or application groups) and can be defined for site-to-site traffic (by using SLA profiles) or for breakout traffic (by using breakout profiles).

Policy intents consist of the following parameters:

- **Source**—A source endpoint that you can choose from a list of sites, site groups, and departments or a combination of all of these. The SD-WAN policy intent is applied to the selected source endpoint.
- **Destination**—A destination endpoint that you can choose from a list of applications and predefined or custom application groups. You can select a maximum of 32 applications or application groups as destination endpoints. The SD-WAN policy intent is applied to the selected destination endpoint.

  Applications are classified into the following categories:

  - Cacheable applications, which refer to applications or application groups that are stored in the application cache when they are recognized by the device. After they are stored in the application cache, subsequent sessions are routed directly through the correct WAN link.
  - Non-cacheable applications, which refer to applications or application groups that are not stored in the application cache and all sessions are first routed through the default path, and then routed to the correct WAN link based on the SD-WAN policy.
- **Traffic Steering Profile**—Depending on whether you want to apply the policy intent to site-to-site traffic or breakout traffic, you can associate the traffic steering profile with the policy intent. The following options are available:
  - SLA-based steering profile— Applicable for site-to-site traffic (Not applicable to the Secure SD-WAN Essentials service.)
  - Path-based steering profile— Applicable for site-to-site traffic
  - Breakout profile—Applicable for breakout traffic (local, central, or cloud).
- **Intent name**—A unique name for the SD-WAN policy intent.

SD-WAN supports advanced policy-based routing (APBR). APBR enables you to dynamically define the routing behavior of the SD-WAN network based on applications. Dynamic application-based routing makes it possible to define policies and to switch WAN links on the fly based on the application's defined SLA parameters. The APBR mechanism classifies sessions based on applications and application signatures and uses policy intents to identify the best possible route for the application. When the best possible route does not meet the application's defined SLA requirements, the SD-WAN network finds the next best possible route to meet SLA requirements.

For example, consider an application in a site. If you want the application group to use custom throughput, latency, or jitter, you can create an SLA profile with these custom values. You can then create an intent

and configure the intent with the application and apply the custom SLA profile. When the intent is deployed, CSO determines the best suited WAN link to route traffic based in the application. If the WAN link fails to meet SLA requirements in runtime, the SD-WAN network switches WAN links to the next best suited path.

On the basis of the configured traffic-based steering profile constraints, you can categorize SD-WAN policies into three types:

- **Path-based steering policy**—If only the path preference is defined and none of the SLA parameters are defined in the SLA profile, then the policy is called a path-based steering policy. In path-based steering profile, you can define the path (MPLS or Internet) that must be used for a given traffic type profile, You cannot configure SLA parameters or path failover criteria for a path-based steering profile. The traffic type profile must be in enabled state in order to be used in any profile.
- **SLA-based steering policy**—If one or more SLA parameters in the SLA profile are defined, then the policy is called an SLA-based steering policy. In an SLA-based steering profile, each profile is associated with a traffic type profile and tracks the SLA parameters such as packet loss, Jitter and RTT. The traffic type profile must be in enabled state in order to be used in any profile. Based on your requirements, you can choose the recommended SLA threshold or enter custom SLA threshold for the traffic type profile. You can even set the path preference (Any, MPLS, or Internet) to switch traffic from one WAN interface to another based on the path failover criteria.

  When an intent is deployed on a site, if the WAN link chosen by the SD-WAN network does not meet the SLA requirements and the network performance deteriorates, then the site switches WAN links to meet the SLA requirements. The link switching is recorded as an SD-WAN event and displayed in the SD-WAN Events page in the customer portal and the *Tenant_name* SLA Performance pages in the administration and customer portals.
- **Breakout policy**—If local breakout, central breakout, or cloud breakout parameters are defined, then the policy is called a breakout policy.

RELATED DOCUMENTATION

Adding SLA-Based Steering Profiles | **357**

Adding Path-Based Steering Profiles | **369**

About the SLA-Based Steering Profiles Page

To access this page, select **Configuration > SLA-Based Steering Profiles** in the Administration Portal.

In an SLA-based steering profile, each profile is associated with a traffic type profile and tracks the SLA parameters such as packet loss, Jitter and RTT. The traffic type profile must be in enabled state in order to be used in any profile. Based on your requirements, you can choose the recommended SLA threshold or enter custom SLA threshold for the traffic type profile. You can even set the path preference (Any, MPLS, or Internet) to switch traffic from one WAN interface to another based on the path failover criteria.

You can use the SLA-Based Steering Profiles page to view information about service-level agreement (SLA)-based steering profiles for all tenants.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of SLA-based steering profiles for all tenants.
- Add an SLA-based steering profile for all tenants. See "Adding SLA-Based Steering Profiles" on page 357.
- Edit or delete an SLA-based steering profile. See "Editing and Deleting SLA-Based Steering Profiles" on page 364.
- Show or hide columns that contain information about SLA-based steering profiles—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for SLA-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

Table 120 on page 354 shows the descriptions of the fields on the SLA-Based Steering Profiles page.

Table 120: Fields on the SLA-Based Steering Profiles Page

Field	Description	Displayed On
Name	Name of the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for *SLA-Profile-Name* pane

Table 120: Fields on the SLA-Based Steering Profiles Page *(continued)*

Field	Description	Displayed On
Priority	Priority of the SLA-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for *SLA-Profile-Name* pane
Traffic Type Profile	Indicates the traffic type profile associated with the SLA-based steering profile. • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for *SLA-Profile-Name* pane
Packet Loss (%)	Target packet loss for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for *SLA-Profile-Name* pane
Jitter (ms)	Target jitter for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for *SLA-Profile-Name* pane
RTT	Target round-trip time (RTT) for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for *SLA-Profile-Name* pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for *SLA-Profile-Name* pane
Created By	Name of the user who created the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)
Path Preference	The preferred path for the SLA profile. The available options are: • MPLS • Internet • Any (default)	Detail for *SLA-Profile-Name* pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for *SLA-Profile-Name* pane

Table 120: Fields on the SLA-Based Steering Profiles Page *(continued)*

Field	Description	Displayed On
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for *SLA-Profile-Name* pane
Sampling Period	The sampling period, in milliseconds, for which the SLA violations are counted.	Detail for *SLA-Profile-Name* pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for *SLA-Profile-Name* pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the SLA parameters is violated or when all (All) the SLA parameters are violated.	Detail for *SLA-Profile-Name* pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the SLA-based steering profile.	Detail for *SLA-Profile-Name* pane
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for *SLA-Profile-Name* pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the SLA-based-steering profile.	Detail for *SLA-Profile-Name* pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for *SLA-Profile-Name* pane

RELATED DOCUMENTATION

SLA Profiles and SD-WAN Policies Overview | 348

Adding SLA-Based Steering Profiles

You can use the Add SLA Profile page to add a new service-level agreement (SLA)-based steering profile, specify the traffic type profile, SLA configuration, SLA threshold, SLA parameters, path selection criteria, and rate limiting parameters for the profile. Table 121 on page 358 lists the SLA-based steering profiles that are tuned for specific application categories and traffic types.

Table 121: Predefined SLA-Based Steering Profiles

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-AV	VOICE-VIDEO	CSO_Collaboration_AV	Skype for Business Zoom Video GotoMeeting Jive Jabber Citrix Online WebEx Zoho Meeting Google Hangout Adobe Connect

Table 121: Predefined SLA-Based Steering Profiles *(continued)*

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Productivity	PREMIUM-INTERNET	CSO_Productivity	ERP: Salesforce, Oracle, SAP Office365 (including SharePoint) Zendesk HRPayroll Zoho Office Suite Slack Square Concur Adobe Quickbooks Freshbooks Workday Project Management-MS PJ Basecamp Asana
CSO-Security	INTERNET	CSO_Security	Symantec McAfee Sophos Zonealarm Lookout

Table 121: Predefined SLA-Based Steering Profiles *(continued)*

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Email	PREMIUM-INTERNET	CSO_Collaboration_Email	MS Exchange IMAP POP3 Gmail OWA Yahoo
CSO-FileShare	INTERNET	CSO_File_Share	Box Dropbox Gsuite OneDrive Skype for Business-File Transfer Zoho Share

NOTE: Tenants with the Secure SD-WAN Essentials service do not support SLA-based steering profiles.

To add an SLA-based steering profile:

1. Select **Configuration > SLA Based Steering Profiles**.

   The SLA-Based Steering Profiles page appears.

2. Click the add icon (+).

   The Add SLA Profile page appears.

3. Enter the SLA profile information according to the guidelines provided in Table 122 on page 361.

> **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. Click **OK** to add the SLA profile.

   The SLA-Based Steering Profiles page appears with the new SLA profile information. You are returned to the SLA-Based Steering Profiles page and a confirmation message indicating that the SLA-based steering profile was added is displayed. The page refreshes to display the SLA-based steering profile that you added.

   Alternatively, if you want to discard your updates, click **Cancel** instead.

> **NOTE:** After you add an SLA-based steering profile, you must add an SD-WAN policy intent that references the SLA-based steering profile in order to enable site-to-site traffic.

Table 122: Fields on the Add SLA Profile page

Field	Guidelines
General	
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the **Enabled** state.
SLA Configuration	Choose one of the following options: • **Use Recommended**: To use the default SLA threshold and SLA parameters for the SLA-based steering profile. • **Enter Custom**: To specify customized values for SLA configuration and SLA parameters for the SLA-based steering profiles.
SLA Threshold	Choose one of the following options: • **Liberal**—To use a relaxed SLA threshold. • **Baseline**—To use the default SLA threshold. • **Conservative**—To use a strict SLA threshold.
SLA Parameters	

Table 122: Fields on the Add SLA Profile page *(continued)*

Field	Guidelines
Packet Loss	Enter the target packet loss (in %) for the SLA-based steering profile. Packet loss is the percentage of data packets dropped by the network to manage congestion.
RTT	Enter the target round-trip time (RTT) for the SLA-based steering profile.
Jitter	Enter the target jitter (in ms) for the SLA-based steering profile. Jitter is the difference between the maximum and minimum round-trip times of a packet of data.
Path Selection Criteria	
Path Preference	Select the preferred WAN link type (MPLS, Internet, or Any) to associate with the SLA profile. **Any** is the default value. If a WAN link type that matches the preferred path is enabled, then that WAN link type is used for all traffic from the site. If you specify that any path can be used, then there is no preference and all traffic-enabled links are used in a load-balancing mode.
Strict Affinity	This field is displayed only if you select MPLS or Internet as the path preference. Enable the toggle button to use strict link affinity. For strict link affinity, AppQoE ensures that the path selected is always of the preferred link type. If the preferred link does not meet the SLA, then the traffic remains on the preferred link with the status as **SLA not met**. 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. If the link affinity is not strict and if SLA meeting links belonging to the preferred link type are not available, then AppQoE selects a link outside the preferred link type that meets the SLA requirements. 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 when the preferred link recovers and conforms to the SLA.

Table 122: Fields on the Add SLA Profile page *(continued)*

Field	Guidelines
Path Failover Criteria	Specify the failover criteria to determine how links are switched when the active links fail to meet the SLA criteria. In such cases, the traffic is routed to links that meet SLA criteria. Choose one of the following options: • **Does not meet one or more SLA parameters**—This triggers the path failover if any of the SLA parameters is violated. • **Does not meet all SLA parameters**—This triggers the path failover only when all the SLA parameters are violated.
Advanced Configuration-	
Rate Limiting	
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Upstream Burst Size	Enter the maximum upstream burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Maximum Downstream Rate	Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Downstream Burst Size	Enter the maximum downstream burst size (in bytes). Range: 1 through 1,342,177,280
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to **High**. Other available values are **Medium High**, **Medium Low**, and **Low**.
Real Time Optimized Mode Setting **NOTE:** The following fields are applicable only for sites configured with the real-time-optimized SD-WAN mode.	
SLA Sampling	

Table 122: Fields on the Add SLA Profile page *(continued)*

Field	Guidelines
Session-sampling %	Enter the matching percentage of sessions for which you want to run the passive probes.
SLA-violation-count	Enter the number of SLA violations after which you want CSO to switch paths. The range is 1 through 32.
Sampling-period	Enter the sampling period, in seconds, for which the SLA violations are counted. The range is 2 through 60.
Switch-cool-off-period	Enter the waiting period, in seconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links. The range is 5 through 300.
NOTE: If you do not specify the **Switch-cool-off-period** and **SLA-violation-count** parameters, the traffic does not automatically revert to the preferred link when the preferred link comes back online after an SLA violation.	

RELATED DOCUMENTATION

- SLA Profiles and SD-WAN Policies Overview | 348
- About the SLA-Based Steering Profiles Page | 354
- Editing and Deleting SLA-Based Steering Profiles | 364

Editing and Deleting SLA-Based Steering Profiles

IN THIS SECTION

- Editing an SLA-Based Steering Profile | 365
- Deleting SLA-Based Steering Profiles | 366

You can use the SLA-Based Steering Profiles page to edit and delete SLA profiles.

NOTE: Only SP administrator can edit the SLA-Based steering profiles that are automatically created by Contrail Service Orchestration (CSO).

Editing an SLA-Based Steering Profile

To edit an SLA-based steering profile:

NOTE: If you edit an SLA-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SLA-Based Steering Profiles**.

   The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profile that you want to edit, and click the Edit (pencil)icon .

   The Edit SLA Profile page appears displaying the same fields that are presented when you add a SLA-based steering profile. For more information, see “Adding SLA-Based Steering Profiles” on page 357.

3. Modify the fields as needed.

   NOTE: You cannot edit the SLA-based steering profile name.

4. Click **OK**.

   You are returned to the SLA-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed.

Deleting SLA-Based Steering Profiles

You can delete the SLA-based steering profile if they are no longer needed. To delete one or more SLA-based steering profile:

> **NOTE:** You cannot delete an SLA-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > SLA-Based Steering Profiles**.

   The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profiles that you want to delete and click the delete (trash can) icon .

   A popup dialog appears asking you to confirm the deletion.

3. Click **Yes**.

   You are returned to the SLA-Based Steering Profiles page. The selected SLA-based steering profile is deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

SLA Profiles and SD-WAN Policies Overview | 348

About the SLA-Based Steering Profiles Page | 354

Adding SLA-Based Steering Profiles | 357

About the Path-Based Steering Profiles Page

To access this page, select **Configuration > Path-Based Steering Profiles** in the Administration Portal.

In path-based steering profile, you can define the path (MPLS or Internet) that must be used for a given traffic type profile. You cannot configure SLA parameters or path failover criteria for a path-based steering profile. The traffic type profile must be in enabled state in order to be used in any profile.

You can use the Path-Based Steering Profiles page to view information about the path-based steering profiles for all tenants.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of path-based steering profiles for all tenants.
- Add path-based steering profiles for all tenants. See "Adding Path-Based Steering Profiles" on page 369.
- Edit or delete a path-based steering profiles. See "Editing and Deleting Path-Based Steering Profiles" on page 371.
- Show or hide columns that contain information about path-based steering profiles—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for path-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

Table 123 on page 367 shows the descriptions of the fields on the Path-Based Steering Profiles page.

Table 123: Fields on the Path-Based Steering Profiles Page

Field	Description	Displayed on
Name	Name of the path-based-steering profile.	Path-Based Steering Profiles Page (Path Profiles List tab) Detail for *Path-Profile-Name* pane
Traffic Type Profile	Indicates the traffic type profile associated with the path-based-steering profile. • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET	Path-Based Steering Profiles Page (Path Profiles List tab) Detail for *Path-Profile-Name* pane
Path Preference	The preferred path for the SLA profile. The available options are: • MPLS • Internet	Path-Based Steering Profiles Page (Path Profiles List tab) Detail for *Path-Profile-Name* pane

Table 123: Fields on the Path-Based Steering Profiles Page *(continued)*

Field	Description	Displayed on
Created by	The name of the user who created the path profile.	Path-Based Steering Profiles Page (Path Profiles List tab)
Priority	Priority of the path-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for *Path-Profile-Name* pane
Packet Loss	Target packet loss for the SLA profile.	Detail for *Path-Profile-Name* pane
RTT	Target round-trip time (RTT) for the SLA profile.	Detail for *Path-Profile-Name* pane
Jitter	Target jitter for the SLA profile.	Detail for *Path-Profile-Name* pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for *Path-Profile-Name* pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for *Path-Profile-Name* pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for *Path-Profile-Name* pane
Sampling Period	The sampling period, in milliseconds, for which the path-based steering profile violations are counted.	Detail for *Path-Profile-Name* pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for *Path-Profile-Name* pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the path-based steering profile parameters is violated or when all (All) the path-based steering profile parameters are violated.	Detail for *Path-Profile-Name* pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the path-based steering profile.	Detail for *Path-Profile-Name* pane

Table 123: Fields on the Path-Based Steering Profiles Page *(continued)*

Field	Description	Displayed on
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for *Path-Profile-Name* pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the path-based-steering profile.	Detail for *Path-Profile-Name* pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for *Path-Profile-Name* pane

RELATED DOCUMENTATION

SLA Profiles and SD-WAN Policies Overview | 348

Adding Path-Based Steering Profiles

You can use the Add Path Profile page to add a new path-based steering profile, and specify the traffic type profile, path preference, and advanced configuration for the profile.

To add a path-based steering profile:

1. Select **Configuration > Path-Based Steering Profiles**.

   The Path-Based Steering Profiles page appears.

2. Click the add (+) icon.

   The Add Path Profile page appears.

3. Enter the path-based steering profile information according to the guidelines provided in Table 124 on page 370.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK** .

   You are returned to the Path-Based Steering Profiles page and a confirmation message indicating that the path-based steering profile was added is displayed. The page refreshes to display the path-based steering profile that you added.

NOTE: After you add a path-based steering profile, you must add an SD-WAN policy intent that references the path-based steering profile in order to enable site-to-site traffic.

Table 124: Fields on the Add Path Profile page

Field	Guidelines
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the **Enabled** state.
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are MPLS, and Internet.
Advanced Configuration	
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps
Maximum Upstream Burst Size	Enter the maximum burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Maximum Downstream Rate	Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile. Range: 64 through 10,485,760 Kbps

Table 124: Fields on the Add Path Profile page *(continued)*

Field	Guidelines
Maximum Downstream Burst Size	Enter the maximum burst size (in bytes). Range: 1 through 1,342,177,280 bytes
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to **High**. Other available values are **Medium High**, **Medium Low**, and **Low**.

RELATED DOCUMENTATION

- SLA Profiles and SD-WAN Policies Overview | 348
- About the Path-Based Steering Profiles Page | 366
- Editing and Deleting Path-Based Steering Profiles | 371

Editing and Deleting Path-Based Steering Profiles

IN THIS SECTION

- Editing a Path-Based Steering Profile | 372
- Deleting a Path-Based Steering Profile | 373

You can use the Path-Based Steering Profiles page to edit and delete path-based steering profiles.

Editing a Path-Based Steering Profile

To edit a path-based steering profile:

> **NOTE:** If you edit a path-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > Path-Based Steering Profiles**.

   The Path-Based Steering Profiles page appears.

2. On the Path Profiles tab, select the path-based steering profile that you want to edit.

3. Click the edit (pencil) icon.

   The Edit Path Profile page appears displaying the same fields that are presented when you add a path-based steering profile. For more information, see "Adding Path-Based Steering Profiles" on page 369.

4. Modify the fields as needed.

   > **NOTE:** You cannot edit the path profile name.

5. Click **OK**.

   You are returned to the Path-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed..

Deleting a Path-Based Steering Profile

You can delete path-based steering profiles if they are no longer needed. To delete one or more path-based steering profiles:

> **NOTE:** You cannot delete a path-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > Path-Based Steering Profiles**.

   The Path-Based Steering Profiles page appears.

2. On the Path Profiles List tab, select the path profiles that you want to delete.

3. Click the delete (trash can) icon.

   A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

   You are returned to the Path-Based Steering Profiles page. The selected path-based steering profiles are deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

- SLA Profiles and SD-WAN Policies Overview | 348
- About the Path-Based Steering Profiles Page | 366
- Adding Path-Based Steering Profiles | 369

About the Breakout Profiles Page

IN THIS SECTION

- Tasks You Can Perform | 374
- Breakout Profiles Field Descriptions | 374

To access this page, click **Configuration > SD-WAN Breakout Profiles**.

You can use the Breakout Profiles page to view existing breakout profiles, add local, backhaul, and cloud breakout profiles, edit breakout profiles, and delete breakout profiles. You can also add settings for cloud breakout, edit cloud breakout settings, assign the settings to one or more sites, detach the settings from one or more sites, and delete the settings.

The breakout profiles are displayed on the Breakout Profiles tab and the cloud breakout settings (applicable only to tenants with the Secure SD-WAN Advanced service) are displayed on the Cloud Breakout Settings tab.

> **NOTE:** Tenants with the Secure SD-WAN Essentials service do not support cloud breakout profiles.

Tasks You Can Perform

You can perform the following tasks from this page:

- View existing breakout profiles—See Table 125 on page 374 for a description of the fields.
- View the details of a breakout profile—On the Breakout Profiles tab, select a breakout profile and from the More menu, select **Detail View**. The Detail for *Breakout-Profile-Name* pane appears on the right-hand side of the page. See Table 125 on page 374 for a description of the fields on this pane.
- Add a breakout profile—See "Editing and Deleting Breakout Profiles" on page 378.
- Edit and delete a breakout profile—See "Adding Breakout Profiles" on page 376.

Breakout Profiles Field Descriptions

Table 125: Breakout Profiles Field Descriptions

Field	Description	Displayed On
Name	Name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab) Detail for *Breakout-Profile-Name* pane

Table 125: Breakout Profiles Field Descriptions *(continued)*

Field	Description	Displayed On
Type	Indicates whether the breakout profile is for local breakout (underlay) or backhaul (central breakout) or cloud breakout.	Breakout Profiles page (Breakout Profiles tab) Detail for *Breakout-Profile-Name* pane
Description	Description of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Path Preference	Indicates the preferred path to be used for breakout traffic: • MPLS • Internet • Any, which indicates no preference.	Breakout Profiles page (Breakout Profiles tab)
Added by	Username of the user who added the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
FqName	Internal name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Rate Limiting	Indicates whether rate limiting is enabled or disabled for the breakout profile.	Detail for *Breakout-Profile-Name* pane
Downstream Rate	Indicates the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for *Breakout-Profile-Name* pane
Downstream Burst Size	Indicates the maximum downstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for *Breakout-Profile-Name* pane
Upstream Rate	Indicates the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for *Breakout-Profile-Name* pane
Upstream Burst Size	Indicates the maximum upstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for *Breakout-Profile-Name* pane

Table 125: Breakout Profiles Field Descriptions *(continued)*

Field	Description	Displayed On
Loss Priority	Indicates the loss priority associated with the breakout profile. The loss priority determines which packets are dropped or retained when network congestion occurs.	Detail for *Breakout-Profile-Name* pane

RELATED DOCUMENTATION

Adding Breakout Profiles

You use the Add Breakout Profile page to add a local breakout (underlay), backhaul, or a cloud breakout profile. A cloud breakout profile (applicable only to the Secure SD-WAN Advanced service) is added by Contrail Service Orchestration (CSO) by default.

> **NOTE:** The Secure SD-WAN Essentials service does not support cloud breakout profiles.

To add a breakout profile:

1. Select **Configuration > SD-WAN Breakout Profiles**.

   The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, click the add icon (**+**).

   The Add Breakout Profile page appears.

3. Complete the configuration according to the guidelines provided in Table 126 on page 377.

   > **NOTE:** Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

You are returned to the Breakout Profiles page (Breakout Profiles tab) and a confirmation message indicating that the breakout profile was added is displayed. The page refreshes to display the breakout profile that you added.

> **NOTE:** After you add a breakout profile, you must add an SD-WAN policy intent that references the breakout profile in order to enable breakout traffic.

Table 126: Fields on the Add Breakout Profile Page

Field	Description
Type	Select the type of breakout profile that you want to add: • **Local Breakout (Underlay)**—Select this option if you want traffic to break out locally (on the underlay) from the site. • **Backhaul**—Select this option if you want traffic to break out through a hub or a enterprise hub (if configured). • **Local Breakout (Cloud)**—(Not applicable to Secure SD-WAN Essentials service.) Select to break out traffic through a cloud-based security platform. Currently, Zscaler is the only cloud-based security platform supported.
Name	Enter a unique name for the breakout profile. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Description	Enter a description for the breakout profile.
Traffic Type Profile	Select a traffic type profile to apply class of service parameters to the breakout traffic. You can select only a traffic type profile that is enabled.
Preferred Path	Select the preferred path (MPLS, Internet, or Any) to be used for breaking out the traffic. If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic. If you specify that any path can be used, then there is no preference and all breakout-enabled links are used in a load-balancing mode.
Advanced Configuration	
Rate Limiting	Click the toggle button to enable rate limiting of breakout traffic for cacheable applications. By default, rate limiting is disabled. If you enable rate limiting, you must specify the upstream and downstream parameters, and the loss priority.

Table 126: Fields on the Add Breakout Profile Page *(continued)*

Field	Description
Upstream Rate	Specify the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Upstream Burst Size	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the upstream rate limit for short periods.
Downstream Rate	Specify the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
Downstream Burst Size	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the downstream rate limit for short periods.
Loss Priority	Select a loss priority based on which packets are dropped or retained when network congestion occurs. Packet drops are most likely when the loss priority is High and least likely when the loss priority is Low.

RELATED DOCUMENTATION

Editing and Deleting Breakout Profiles

IN THIS SECTION

- Editing Breakout Profiles | **379**
- Deleting Breakout Profiles | **379**

On the Breakout Profiles page, you can edit breakout profiles and delete breakout profiles that are not used in SD-WAN policy intents.

Editing Breakout Profiles

To edit a breakout profile:

> **NOTE:** If you edit a breakout policy that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > Breakout Profiles**.

   The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to edit.

3. Click the edit (pencil) icon.

   The Edit Breakout Profile page appears displaying the same fields that are presented when you add a breakout profile. For more information, see *Adding Breakout Profiles*.

4. Modify the fields as needed.

   > **NOTE:** You can modify only some fields when you are editing a breakout profile

5. Click **OK**.

   You are returned to the Breakout Profiles page. The modifications that you made are saved and a confirmation message is displayed.

Deleting Breakout Profiles

To delete a breakout profile that is not used in an SD-WAN policy intent:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

   The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

   You are returned to the Breakout Profiles page. The selected breakout profile is deleted and a confirmation message is displayed.

RELATED DOCUMENTATION

9

CHAPTER

Managing Licenses

About the Device License Files Page | **382**

Uploading a Device License File | **383**

Editing and Deleting Device Licenses | **384**

Pushing a License to Devices | **386**

About the CSO Licenses Page | **387**

Add a CSO License | **389**

Edit and Delete CSO Licenses | **392**

Assign CSO Licenses, and Update or Unassign CSO License Assignments | **394**

About the Device License Files Page

To access this page, click **Administration > Licenses> Device Licenses**.

You can use the Device License Files page to upload licenses for devices and virtual network services from your local file system. Each device license file should contain only one license key. A license key is required to enable various features including virtual network services such as application-based routing, application monitoring, and vSRX security features.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add device license files. See "Uploading a Device License File" on page 383.
- Edit and delete device license entries. See "Editing and Deleting Device Licenses" on page 384.
- Push licenses to devices. See "Pushing a License to Devices" on page 386.
- View details of a device license. Click the details icon that appears when you mouse over the row for each license file or click **More > Details**.
- Show or hide columns about the device license files—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Sort the device license files.
- Search an object about the device license files—Click the Search icon in the top right corner of the page. You can enter partial text or full text of the keyword in the text box and press **Enter**. The search results are displayed on the same page.

Field Descriptions

Table 127 on page 382 describes the fields on the License Files page.

Table 127: Fields on the License Files Page

Field	Description
File Name	Displays the filename of the license. Example: license_Image_v1.txt

Table 127: Fields on the License Files Page *(continued)*

Field	Description
Description	Displays the description of the license. Example: License file for application routing.
Tenant	Displays the name of the tenant if the license is associated with a tenant. Example: Tenant 1
Uploaded By	Displays the administrator who uploaded the license. Example: test_admin
Uploaded	Displays the date and time when the license was uploaded. Example: Jun 5, 2018, 12:41:08 PM
Devices	Displays the number of devices to which the license is pushed. Click the number to view the devices to which the license is pushed.

RELATED DOCUMENTATION

- Uploading a Device License File | 383
- Editing and Deleting Device Licenses | 384
- Pushing a License to Devices | 386

Uploading a Device License File

To upload a device license file:

1. Click **Administration > Licenses > Device Licenses**.

   The Device License Files page appears.

2. Click the plus icon (+).

   The Add Device Licenses page appears.

3. In the Device License File field, specify the location of the license file that you want to upload. Alternatively, you can click Browse to navigate to the file location and select the file.

   NOTE: Each license file should contain only one license key.

4. (Optional) From the Tenants list, select the tenant to which you want to associate the license file.

   If you associate a license with a tenant, you can apply that license only to devices that belong to that tenant. If a tenant has licenses associated with the tenant, when a device is activated during ZTP, a matching license from the licenses associated with the tenant is downloaded to the device.

   You can apply a license that is not associated with a tenant to any device of any of the tenants. During ZTP, when a device is activated for a tenant that does not have any license associated with it, a matching license from the licenses that are not associated with any tenant is downloaded to the device.

5. In the Description field, enter a description for the license that you want to upload.

6. Click **OK** to upload the license.

   You are returned to the Device License Files page.

RELATED DOCUMENTATION

About the Device License Files Page | 382
Device Images Overview | 289

Editing and Deleting Device Licenses

IN THIS SECTION

Editing a Device License Entry | 385
Deleting a Device License | 385

The following sections describe the procedure for editing and deleting uploaded device licenses:

Editing a Device License Entry

You can edit a device license entry to modify the description for the license file.

1. Click **Administration > Licenses > Device Licenses**.

   The Device License Files page appears.

2. Select the device license for which you want to modify the description and click the Edit icon.

   The Update Device License page appears.

3. Update the description.

4. Click **OK** to save the changes. To discard the changes, click **Cancel**.

   If you click **Cancel**, a confirmation message appears. Click **Yes** to confirm that you want to cancel the update.

Deleting a Device License

To delete a device license:

1. Click **Administration > Licenses > Device Licenses**.

   The Device License Files page appears.

2. Select the device license that you want to delete and click the delete icon.

3. In the confirmation message, click **Yes** to delete the device license.

   To cancel the delete operation, click **No**.

Pushing a License to Devices

You can push licenses on to devices from the Licenses page of the Administration portal. If a license is associated with a tenant, you can push that license only to devices associated with that tenant. However, if no tenant is associated with a license, you can apply the license to any device that belongs to any tenant.

When a license is applied to a device, the license information is added to the device object. When the same license is pushed to the device again, the a device-level error message is created. Similarly, if a pushed license does not match a device, the device generates an error message.

To push a license to a device:

1. Click **Administration > Licenses > Device Licenses**.

   The License Files page appears.

2. Select the license that you want to push to a device.

   The **Push License** button is enabled.

3. Click the **Push License** button.

   The Push License page appears.

4. From the Tenants list, select the tenant associated with the site and devices to which you want to apply the license.

   > **NOTE:** If the license has already been associated with a tenant, you cannot select a different tenant. You can apply the license only to the sites and devices associated with the tenant.

   Sites and devices associated with the selected tenant appear.

5. Select the sites and devices to which you want to apply the license and click **Push Licenses**.

   CSO applies the license to the selected devices.

RELATED DOCUMENTATION

About the Device License Files Page | 382

Editing and Deleting Device Licenses | 384

About the CSO Licenses Page

To access this page, click **Administration > Licenses > CSO Licenses**.

You use the CSO Licenses page in Administration Portal to manage CSO licenses.

Tasks You Can Perform

You can perform the following tasks from this page:

> **NOTE:** The tasks that you can perform depends on your role, so some tasks are available only with users with a specific role, which is indicated below.

- Group CSO licenses by sales order or SKUs:
  - Click **Group By** and select **Sales Order** to group CSO licenses by sales orders. By default, CSO licenses are grouped by sales order.
  - Click **Group By** and select **SKU** to group CSO licenses by SKUs.
- (SP Administrator user only) Add CSO licenses for a tenant or an operating company (OpCo)—See "Add a CSO License" on page 389.
- (SP Administrator user only) Edit a license—See "Edit and Delete CSO Licenses" on page 392.
- (SP Administrator user only) Delete a license—See "Edit and Delete CSO Licenses" on page 392.
- (OpCo Administrator user only) Assign CSO licenses to one or more tenants—See "Assign CSO Licenses, and Update or Unassign CSO License Assignments" on page 394.
- (OpCo Administrator only) Update or unassign CSO license assignments—See "Assign CSO Licenses, and Update or Unassign CSO License Assignments" on page 394.
- (OpCo Administrator user only) View the tenants previously assigned to a CSO license—Click *assigned-number* corresponding to a CSO license. The View Assigned page appears displaying the tenants and quantity assigned to each tenant.
- Search for CSO licenses by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

  You can search using license SKU, sales order, type, tier, or device class.
- Sort CSO licenses—Click a column name to sort based on the column name.

> **NOTE:** Sorting is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the CSO Licenses page.

Field Descriptions

Table 128 on page 388 describes the fields on the CSO Licenses page.

Table 128: Fields on the CSO Licenses page

Field	Description
License SKU	Displays the license SKU name; for example, S-CSO-C-S1-A-3.
OpCo/Tenant	Displays the operating company or a tenant to which the license SKU is applicable.
Sales Order	Sales order number; for example, 15563238.
Type	Displays whether the license is for an on-premise installation or for a cloud-hosted CSO installation.
Tier	Support tier associated with the license (standard or advanced).
Device Class	Class of the Juniper device associated with the license; for example, B-class.
SSRN	Software support reference number (SSRN), which is necessary to identify your purchase order when you contact Juniper Networks for support.
Start Date	Date (in MMM DD , YYYY format) from which the license is valid; for example, Aug 29, 2019.
End Date	Date (in MMM DD , YYYY format) up to which the license is valid. CSO calculates the end date based on the validity of the license SKU.

Table 128: Fields on the CSO Licenses page *(continued)*

Field	Description
Device Quantity	For a license assigned to an OpCo, displays the total number of devices that the OpCo Administrator can assign for the license. For a license assigned to a tenant, displays the total number of devices that the tenant can add.
Available	For a license assigned to an OpCo, displays the available number of devices (that the tenant can add) that the OpCo Administrator can assign to tenants.
Assigned	**NOTE:** This field is applicable only for licenses assigned to an OpCo. Number of devices (that the tenant can add) that are already assigned to one or more tenants: • An OpCo Administrator can click *assigned-number* to view the tenants and quantity assigned for each tenant. The View Assigned page appears displaying the tenants and quantity assigned to each tenant. • If the CSO license is not assigned to any tenants, an OpCo Administrator can click **Assign** to assign the license to one or more tenants. See "Assign CSO Licenses, and Update or Unassign CSO License Assignments" on page 394.

RELATED DOCUMENTATION

About the Device License Files Page | 382

Add a CSO License

To maintain a record of CSO licenses purchased by tenants or operating companies (OpCos), a user with the SP Administrator role can add the CSO license for a tenant or an OpCo from the CSO Licenses page.

To add a CSO license:

1. In Administration Portal, select **Administration** > **Licenses** > **CSO Licenses**.

   The CSO Licenses page appears.

2. Click the add (+) icon.

   The Add CSO License page appears.

3. Complete the configuration according to the guidelines in Table 129 on page 390.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   You are returned to the CSO Licenses page. A job is triggered to add the license and a confirmation message appears at the top of the page. After the job completes successfully, a confirmation message appears and the page refreshes to display the newly added license SKUs.

Table 129: Fields on the Add CSO License page

Setting	Guideline
Add License	Select whether you are adding the license for a tenant or for an operating company.
Tenant	If you are adding the license for a tenant, select the name of the tenant from the drop-down list.
Operating Company	If you are adding the license for an OpCo, select the name of the OpCo from the drop-down list.
Sales Order	Specify the sales order number; For example, 15563238.
SSRN	Specify the software support reference number (SSRN). This information is necessary to identify your sales order if you contact Juniper Networks for support.
Start Date	Specify the start date (in MM/DD/YYYY format) from which the license is effective.

Table 129: Fields on the Add CSO License page *(continued)*

Setting	Guideline
License SKUs	To add one or more license SKUs: 1. Click the add (+) icon. A row appears inline in the License SKU List grid. 2. In the **License SKU** field, enter the SKU name. The SKU format is as follows: S-CSO-*Release-Type-License-Type-Device-Class-License-Period*, where: • S, which indicates that the SKU is for software. • CSO, which indicates that the SKU is for CSO. • *Release-Type*, which indicates whether the SKU is for a cloud release (C) or an on-premise release (P). • *License-Type*, which indicates whether the license is standard (S1) or advanced (A1) • *Device-Class* ◦ A denotes SRX300, SRX320, SRX340, SRX345, vSRX (2 vCPUs), NFX150 devices ◦ B denotes NFX250 (2 vCPUs), SRX550 High Memory Services Gateway (SRX550M), SRX1500, vSRX (5 vCPUs) devices. ◦ C denotes NFX250 (8 vCPUs), SRX4100, SRX4200, vSRX (9 or 17 vCPUs) devices. • *License-Period*, which indicates the term for the CSO license (1, 3, or 5 years). 3. In the **Device Quantity** field, enter the maximum number of branch sites that a tenant is authorized to create. You must enter a non-zero number to proceed. 4. Click **✓** (check mark) to save your changes. The license SKU is saved and displayed in the grid. 5. (Optional) Repeat the preceding steps if you want to add more license SKUs. You can modify a license SKU by selecting the corresponding row and clicking the edit (pencil) icon.

RELATED DOCUMENTATION

About the CSO Licenses Page | 387

Edit and Delete CSO Licenses

IN THIS SECTION

- Edit a CSO License | 392
- Delete a CSO License | 393

In Administration Portal, users with the SP Administrator role can edit or delete CSO licenses.

Edit a CSO License

To edit a CSO license:

1. In Administration Portal, select **Administration** > **Licenses** > **CSO Licenses**.

   The CSO Licenses page appears.

2. Select the license that you want to edit and click the edit (pencil) icon.

   The Edit CSO License page appears.

3. Modify the license according to the guidelines in Table 130 on page 393.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   You are returned to the CSO Licenses page. A job is triggered to update the license and a confirmation message appears at the top of the page. After the job completes successfully, a confirmation message appears and the page refreshes to display the modified information.

Table 130: Fields on the Edit CSO License page

Setting	Guideline
Tenant/OpCo	Displays the tenant or OpCo to which the license is applicable. You cannot modify this field.
Sales Order	Displays the sales order number associated with the license SKU. You cannot modify this field.
SSRN	Displays the software support reference number (SSRN) associated with the license SKU. If you modify the SSRN, the modified SSRN is applicable to all license SKUs associated with the sales order.
Start Date	Displays the start date (in MM/DD/YYYY format) from which the license is effective. If you modify the start date, the modified start date is applicable to all license SKUs associated with the sales order.
SKU Name	Displays the license SKU name. You cannot modify this field.
Assigned	Displays the quantity that is already assigned to tenants. You cannot modify this field.
Quantity	Displays the quantity that is available to be assigned tenants.

Delete a CSO License

In Administration Portal, users with the SP Administrator role can delete CSO licenses.

To delete a CSO license:

1. In Administration Portal, select **Administration** > **Licenses** > **CSO License**:

   The CSO Licenses page appears.

2. Select the license that you want to delete and click the delete (trash can) icon.

   A popup dialog appears asking you to confirm the deletion.

3. Click **Yes** to confirm the delete operation.

   You are returned to the CSO Licenses page. A job is triggered to delete the license and a confirmation message appears at the top of the page. After the job completes successfully, a confirmation message appears at the top of the page.

RELATED DOCUMENTATION

About the CSO Licenses Page | 387

Assign CSO Licenses, and Update or Unassign CSO License Assignments

IN THIS SECTION

- Assign CSO Licenses to Tenants | 394
- Update or Unassign CSO License Assignments | 396

Users with the Operating Company (OpCo) Administrator role can:

- Assign a CSO license to one or more tenants.
- Update the assignment of a CSO license that was previously assigned to one or more tenants.
- Unassign a CSO license that was previously assigned to a tenant.

Assign CSO Licenses to Tenants

To assign a CSO license that is not yet assigned to a tenant:

1. Select **Administration** > **Licenses** > **CSO Licenses**.

   The CSO Licenses page appears.

2. Click the **Assign** link corresponding to the license that you want to assign (in the Assigned column).

   The Assign CSO License page appears.

3. Configure the fields according to the guidelines provided in Table 131 on page 395.

4. Click **Assign**.

   CSO validates the quantities that you assigned against the total quantity for the license:

- If the sum of assigned quantities is greater than the total quantity, an error message is displayed. You must then modify the assigned quantities to proceed.
- If the sum of assigned quantities is less than or equal to the total quantity, a job is triggered. You are returned to the CSO Licenses page and a confirmation message is displayed on the top of the page. After the job completes successfully, the CSO Licenses page displays the updated information in the Available and Assigned columns.

Table 131: Fields on the Assign CSO License page

Field	Description
License Information	Displays the following information for the license: • Sales Order • License SKU • Start Date
License Assignment	
Device Quantity	Displays the total quantity that can be assigned to tenants.
Available	Displays the available quantity that can be allocated to tenants.
Tenants List	To assign the license to one or more tenants: 1. Click the **+** icon. A row is added in the grid and selected. 2. In the **Tenant** column, select the tenant to which you want to assign the license. 3. In the **Device Quantity** column, enter the quantity that you want to assign to the tenant. 4. Click **✓** (check mark) to save your changes. 5. (Optional) Click the pencil icon to modify the tenant name or the quantity and click **✓** (check mark) to save your changes. 6. (Optional) Repeat the steps if you want to assign the license to additional tenants.

Update or Unassign CSO License Assignments

For a CSO license that is already assigned to one or more tenants, to update or unassign the license assignment:

1. Select **Administration** > **Licenses** > **CSO Licenses**.

   The CSO Licenses page appears.

2. Select the license for which you want to update or unassign the license assignment and click the **Update Assignment** button.

   The Assign CSO License page appears.

3. From the list of tenants displayed in the grid, select the tenant (row) and do one of the following:

   - To update the license assignment:

     a. Click the edit (pencil) icon.

     b. In the **Device Quantity** column, modify the device quantity.

     c. Click ✓ (check mark) to save your changes.

        The modification that you made is displayed in the grid.

   - To unassign the license assignment:

     a. Click the delete (trash can) icon.

        A popup appears asking you to confirm the unassign operation.

     b. Click **Yes**.

        The license is unassigned from the tenant that you selected and the tenant is removed from the grid.

4. (Optional) If the available quantity is non-zero, you can assign the license to additional tenants. See Table 131 on page 395 for more information.

5. Click **Assign**.

   CSO validates the modifications against the total device quantity for the license:

   - If the sum of assigned quantities is greater than the total quantity, an error message is displayed. You must then modify the assigned quantities to proceed.

- If the sum of assigned quantities is less than or equal to the total quantity, a job is triggered and you are returned to the CSO Licenses page. A confirmation message is displayed on the top of the page.

  After the job completes successfully, the CSO Licenses page displays the updated information in the Available and Assigned columns.

RELATED DOCUMENTATION

About the CSO Licenses Page | **387**

10
CHAPTER

Managing Users and Roles

Role-Based Access Control Overview | **399**

About the Users Page in Administration Portal | **400**

Add Service Provider and OpCo Users | **402**

Edit and Delete Service Provider Users and OpCo Users | **406**

Resetting the Password for Service Provider, OpCo, and Tenant Users | **407**

Roles Overview | **408**

About the Roles Page | **412**

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users | **413**

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users | **415**

Access Privileges for Role Scopes (Operating Company and Tenant) | **417**

Role-Based Access Control Overview

Contrail Service Orchestration supports the authentication and authorization of users. Service Provider, OpCo, and tenant users access the pages within the unified Administration Portal and Customer Portal based on their role and access permissions.

In addition to predefined roles, CSO enables you to add object-based custom roles. You can create custom roles and assign access privileges (read, create, update, delete, and other actions) to each role.

Table 132 on page 399 shows predefined Service Provider, OpCo, and tenant roles and their access privileges.

Table 132: Roles and Access Privileges

Role	Role Scope	Access Privileges
SP Admin	Service Provider	Users with the SP Admin role have full access to the Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with SP Admin, SP Operator, and custom roles. They can onboard tenants, and add the first tenant user during the tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant. **NOTE:** When the SP administrator creates one or more operating companies under the service provider, the service provider is called a global service provider and the SP administrator is called the global SP administrator.
SP Operator	Service Provider	Users with the SP Operator role have read-only access to the Administration Portal UI and APIs.
NOTE: Roles in the service provider scope are not applicable when you use CSO as SaaS		
Tenant Admin	Tenant	Users with the Tenant Admin role have full access to the Customer Portal UI and APIs. They can add one or more users with the Tenant Administrator or Tenant Operator roles.
Tenant Operator	Tenant	Users with the Tenant Operator role have read-only access to the Customer Portal UI and APIs.

Table 132: Roles and Access Privileges *(continued)*

Role	Role Scope	Access Privileges
OpCo Admin	Operating Company	Users with the OpCo Admin role have full access to the OpCo's Administration Portal UI and API capabilities. They can use the UI or APIs to add one or more users with OpCo Admin, OpCo Operator, and custom roles. They can onboard tenants, and add the first tenant user during the OpCo's tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant.
OpCo Operator	Operating Company	Users with the OpCo Operator role have read-only access to the OpCo's Customer Portal UI and APIs.

RELATED DOCUMENTATION

Authentication Methods Overview | 61

About the Users Page in Administration Portal

To access the Users page, select **Administration** > **Users** in the Administration Portal.

Use this page to manage users in the Service Provider and Operating Company (OpCo) scopes.

For information about service provider and OpCo user roles and access permissions, see "Role-Based Access Control Overview" on page 399.

The information listed on the Users page changes depending on the authentication method configured:

- **Local** —The Users page lists all local users that you can add, edit, and delete.
- **Authentication and Authorization with SSO Server**—The Users page is not displayed because users are externally managed in the single sign-on (SSO) server.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a service provider user, or an OpCo user. See “Add Service Provider and OpCo Users” on page 402.
- Edit and delete a service provider user or an OpCo user. See “Edit and Delete Service Provider Users and OpCo Users” on page 406.

  NOTE: You can edit or delete the information for a tenant user or an OpCo tenant user from the Customer Portal.

- View details of users in the Service Provider and OpCo scopes. See Table 133 on page 401.
- Show or hide columns displayed on the page—Click the **Show Hide columns** icon in the top right corner of the table and select the columns that you want to view on the page.
- Reset password for a user. See “Resetting the Password for Service Provider, OpCo, and Tenant Users” on page 407.
- Search for a user—Click the Search icon in the top right corner of the table and enter the search text in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

Table 133 on page 401 displays the fields on the Users page in the Service Provider and OpCo scopes.

Table 133: Fields on the Users Page

Field	Description
Username	Username of the user. Example: *xyz@example.com*
First Name	First name of the user.
Last Name	Last name of the user.
Status	Indicates whether the user can log in to CSO (enabled) or cannot log in to CSO (disabled).

Table 133: Fields on the Users Page *(continued)*

Field	Description
Role	Depending on the scope selected, indicates the roles assigned to the service provider user or the OpCo user. By default, this column lists only one role assigned to the user. When a user is assigned more than one role, a ***+<integer>***icon (for example: +2) appears to the right of the role. The integer indicates the number of additional roles assigned to the user. Click on the integer to view the additional roles.
Last Login	Date and time (in MM/DD/YYYY HH:MM formats) when the user last logged into the Administration portal. Example: 07/22/2017 20:07 Date and time are not displayed when the user has not logged in to the Administration Portal.

RELATED DOCUMENTATION

Role-Based Access Control Overview | 399

Add Service Provider and OpCo Users

Use the Add User page or Add OpCo User page in the Administration portal to add service provider or Operating Company (OpCo) users respectively. After you add a user, the user receives an e-mail with the initial login credentials.

In the service provider scope, you can create a user and assign the following roles or a combination of roles to the user:

- Service provider roles
- Service provider and OpCo roles.

- Service provider and tenant roles. If a user is assigned both service provider and tenant roles, then the user is a service provider user. The user can view all tenants and access tenant objects based on the access privileges assigned in the tenant roles.
- Service provider, OpCo, and tenant roles. If a user is assigned service provider, OpCo, and tenant roles, then the user is a service provider user. The user can view all tenants and OpCos, and access tenant and OpCo objects, based on the access privileges assigned in the tenant and OpCo roles.

> **NOTE:** Users with the SP Operator role have read-only access to Administration Portal, Customer Portal and APIs and they cannot add new users.

In the OpCo scope, you can create a user and assign the following roles or combination of roles to the user:

- OpCo roles
- OpCo and OpCo tenant roles

To add a service provider user or an OpCo user:

1. Click **Administration > Users**.

   The Users page appears.

2. Click the add icon (**+**) or click the **Add User** button. The Add User button appears when there are no users configured in the scope you have logged in.

   In the Service Provider scope, the Add User page appears. In the OpCo scope, the Add OpCo User page appears.

3. Complete the configuration as described in Table 134 on page 404.

4. Click **OK** to save the changes or click **Cancel** to discard the changes.

   If you click OK, a confirmation message indicating that the user account is created appears and the user account is listed on the Users page.

   To enhance the security related to your login credentials, an automatically generated password is sent to the e-mail address that you have specified for the user. You are prompted to change the password after you log in with the automatically generated password. For more information about changing the password on first login, see “Changing the Password on First Login” on page 44.

Table 134: Fields on the Add User and Add OpCo User Pages

Field	Description
First Name	Enter the first name as a string of alphanumeric characters, some special characters [underscore (_) and period(.)] and spaces. The maximum length allowed is 32 characters.
Last Name	Enter the last name as a string of alphanumeric characters, some special characters [underscore (_) and period(.)] and spaces. The maximum length allowed is 32 characters.
Username (Email)	Enter a valid e-mail address in the *user@domain* format.
Status	Click the toggle button to enable or disable the user. By default, the status is enabled. A user can log in to CSO only when the status is enabled.

Table 134: Fields on the Add User and Add OpCo User Pages *(continued)*

Field	Description
Role	In the Service Provider scope, specify whether you want to assign specific roles to the user or make the user a Global Administrator: • **Select specific roles**—Select this option to assign specific roles to the user in the SP, OpCo, and tenant scopes, and assign one or more roles in the different scopes. To assign roles: 1. Click the scope in which you want to assign one or more roles to the user. The available roles are listed under the **Available** column. 2. Select one or more roles that you want to assign to the user and click the right-arrow icon to move the selected roles from the **Available** column to the **Selected** column. You can use the search icon on the top right of each column to search for role names. • **Make Global Administrator**—Select this option to make the user a Global Administrator. As a Global Administrator, the user has permissions to perform all administration tasks in the SP, OpCo, and tenant scopes. In the OpCo scope, you can only assign OpCo and OpCo tenant roles to a user. To assign roles: 1. Click the scope in which you want to assign one or more roles to the user. The available roles are listed under the **Available** column. 2. Select one or more roles that you want to assign to the user and click the right-arrow icon to move the selected roles from the **Available** column to the **Selected** column. You can use the search icon on the top right of each column to search for role names. To know more about the predefined roles for service provider, OpCo and tenant users, see "Role-Based Access Control Overview" on page 399.

RELATED DOCUMENTATION

Roles Overview | 408

Edit and Delete Service Provider Users and OpCo Users

IN THIS SECTION

- Edit Service Provider and OpCo Users | 406
- Delete Service Provider and OpCo Users | 407

You can edit the information about a service provider or an Operating Company (OpCo) user, and also delete users from Contrail Service Orchestration (CSO).

> **NOTE:** To edit and delete users, you should be assigned a role, such as an SP Admin or OpCo Admin, that allows you to edit and delete users.

Edit Service Provider and OpCo Users

To modify the information about a service provider user or an OpCo user:

1. Select **Administration > Users**.

   The Users page appears.

2. Select the user that you want to modify, and click the edit icon.

   In the Service Provider scope, the Edit User page appears. In the OpCo scope, the Edit OpCo User page appears.

3. Modify the parameters by following the guidelines provided in Table 134 on page 404.

   > **NOTE:** You cannot modify the **Username (E-mail)** field.

4. Click **OK** to save the changes or click **Cancel** to discard the changes.

If you click OK, a confirmation message indicating that the user information is successfully updated appears on top of the Users page.

Delete Service Provider and OpCo Users

To delete one or more service provider users or OpCo users:

1. Select **Administration > Users**.

   The Users page appears.

2. Select the users that you want to delete and click the delete icon.

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected users or **No** to cancel the deletion.

   If you click **Yes**, a confirmation message indicating that the user account is deleted from CSO appears on top of the Users page.

RELATED DOCUMENTATION

Roles Overview | 408

Resetting the Password for Service Provider, OpCo, and Tenant Users

As an SP administrator or OpCo administrator, you can reset the password for OpCo and tenant users. Also, users with the Update permission for user objects can reset the password for service provider, OpCo, and tenant users.

You must reset the password when a user's account is locked. A user's account is locked when the user enters password incorrectly for five times successively.

To reset the password:

1. Select **Administration > Users** in Administration Portal.

   The Users page appears, displaying a list of service provider, OpCo, and tenant users.

2. Select the username for which you want to reset the password, and then select **More > Reset Password**.

   An alert message appears, asking you to confirm the reset password operation.

3. Click **Yes** to confirm the reset password operation.

   A confirmation message appears, indicating that the password is successfully reset, and CSO sends an e-mail with a link to reset the password to the e-mail address associated with the user ID for which you are resetting the password.

   NOTE: The link is active only for 24 hours.

The user can set a new password by accessing the mail from CSO and use the new password to log in to CSO.

RELATED DOCUMENTATION

About the Users Page in Administration Portal | 400

Roles Overview

IN THIS SECTION

- Types of Roles | 409
- Role Scopes | 409
- Access Privileges | 410
- Relationship Between Users, Roles, and Access Privileges | 411
- Benefits of Roles in CSO | 411

A role is a function assigned to a user that defines the tasks that the user can perform within CSO. Each user can be assigned one or more roles depending on the tasks that the user is expected to perform.

User roles enable you to classify users based on the privileges to perform tasks on CSO objects. Roles assigned to a user determine the tasks and actions that the user can perform.

This topic contains the following sections:

Types of Roles

There are two types of roles: predefined roles and custom roles.

- **Predefined roles**—System-defined roles with a set of predefined access privileges assigned to a user to perform tasks within the CSO application. Predefined roles are created in the system during CSO installation. For more information about predefined roles, see "Role-Based Access Control Overview" on page 399.
- **Custom roles**—Object-based user-defined roles with a set of access privileges assigned to a user to perform tasks within the CSO application. Objects include menu and submenu items (for example, Resources, Devices, Images, and POPs) in the CSO application, from which you can create, edit, clone, and delete objects.

  Custom roles can be created by:

  - An SP administrator, OpCo administrator, or a tenant administrator.
  - A service provider user with the Create Role privilege. This user can create custom roles for service provider, tenant, and OpCo users.
  - A tenant user with the Create Role privilege. This user can create custom roles for tenant users.
  - An OpCo user with the Create Role privilege. This user can create custom roles for both OpCo and tenant users.

You can create custom roles and assign access privileges to each role by using the Roles page (**Administration > Roles**).

You can assign one or more roles to a user when you create or edit a user account. Each role can have one or more access privileges.

Role Scopes

A role scope defines the capabilities of the user under a scope (service provider, OpCo, and tenant).

- A service provider administrator can assign service provider, OPCo, and tenant roles to service provider, OpCo, and tenant users.
- An OpCo administrator can assign OpCo and tenant roles to OpCo users and tenant roles to tenant users.
- A tenant administrator can assign tenant roles only to tenant users.

A role can have the following scopes:

- **Service provider**—Represents a provider that offers services to other service providers and customers. A service provider could be a global service provider that provides services to its operating companies in different geographical locations. The operating companies act as service providers and provide services to their tenants. An SP administrator with access privileges can view and access resources across operating companies.
- **Tenant**—Represents a customer that can view, configure, and manage tenant sites through Customer Portal.
- **Operating company**—An operating company (OpCo) is a service provider that manages its tenants and provides services to them. Tenants managed by one OpCo are isolated from tenants of another OpCo. An OpCo can manage all activities related to its own tenants. For more information, see "Operating Companies Overview" on page 108.

Access Privileges

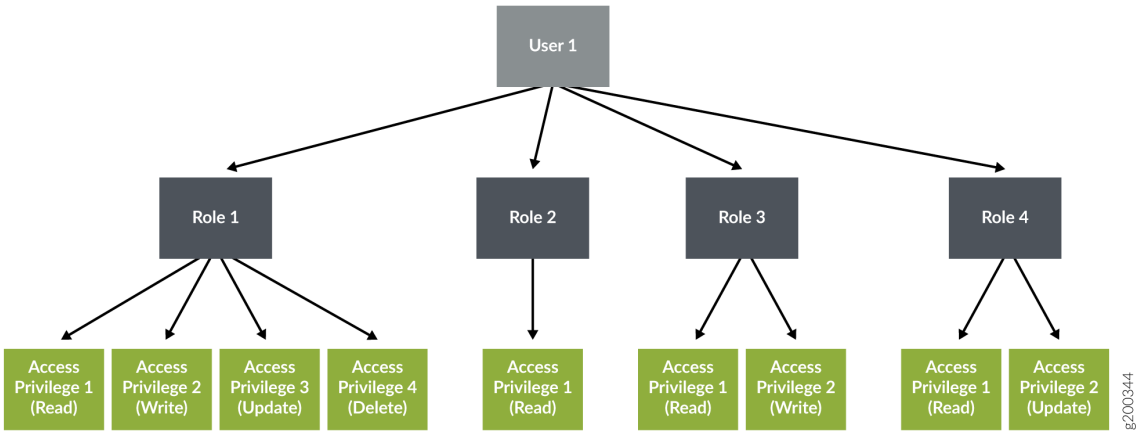
The following access privileges and actions can be assigned to a user role to access objects (Dashboard, Device Templates, Tenants, and so on) in CSO. For example, a user can be given only read, create, update privileges to device objects and only the delete privilege to security alerts objects.

- Read
- Create
- Update
- Delete
- Other actions (for example, for the device templates object, other actions such as cloning and editing the device template are supported).

Relationship Between Users, Roles, and Access Privileges

Figure 11 on page 411 shows the relationship between users, user roles, and access privileges. A user can have one or more roles and each role can have one or more access privileges.

Figure 11: Relationship Between a User, Roles, and Access Privileges



Benefits of Roles in CSO

- Provide a well-defined separation of responsibility and visibility.
- Provide granular-level access control on CSO objects within each navigation menu. Roles enable you to control which system users can access CSO objects based on certain business and operational needs.

RELATED DOCUMENTATION

Role-Based Access Control Overview | 399

About the Roles Page | 412

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users | 415

About the Roles Page

To access this page, select **Administration > Roles** in Administration Portal.

You can use the Roles page to view a list of predefined (system-defined) and custom (user-defined) roles that can be assigned to SP administrator, OpCo and tenant users. You can create, edit, or delete custom roles and clone both custom and predefined roles.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a custom role. See "Add User-Defined Roles for Service Provider, OpCo, and Tenant Users" on page 413.
- Edit, clone, or delete a role. See "Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users" on page 415.

Field Descriptions

Table 135 on page 412 describes the fields on the Roles page.

Table 135: Fields on the Roles Page

Field	Description
Role Name	Displays the name of the role.
Role Scope	Displays the role scope, such as OpCo, or tenant.
Role Type	Displays whether the role is a predefined role or a custom role.
Created By	Displays the username of the user that created the role.

RELATED DOCUMENTATION

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users | 413

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users | 415

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users

Use the Add Role page to create custom (user-defined) roles and assign access privileges (read, create, update, delete, and other actions) to service provider, OpCo, and tenant user roles.

A user with the Create Role privilege can create custom roles for service provider, OpCo, and tenant users.

To create a custom role:

1. Select **Administration > Roles** in Administration Portal.

   The Roles page appears.

2. Click the add icon (+) to create a new role.

   The Add Role page appears.

3. Complete the configuration according to the guidelines provided in Table 136 on page 413.

4. Click **OK**.

   A new role is created and listed on the Roles page.

> **NOTE:** The tenant list in the top banner of CSO is not displayed if the Service Provider or OpCo user that is logged in to CSO does not have tenant roles assigned.

Table 136: Fields on the Add Role Page

Field	Description
Role Name	Enter a unique role name. The name can contain alphanumeric characters, underscore, period, and space.
Description	Enter a description for the role.

Table 136: Fields on the Add Role Page *(continued)*

Field	Description
Role scope	Select the scope of the role. You can assign the role to a service provider, OpCo, or tenant user. There are three scopes for user roles: • Service Provider—Select this option to assign the role to service provider users. If you select the role scope as Service Provider, then the Privileges section displays the objects of the Administration Portal • **Tenant**—Select this option to assign the role to tenant users. If you select the role scope as Tenant, then the **Privileges** section displays the objects of the Customer Portal. • **OpCo**—Select this option to assign the role to OpCo users. If you select the role scope as OpCo, then the **Privileges** section displays the objects of the OpCo.
Access Privileges	**All Objects**—Displays the objects of Administration Portal and Customer Portal based on the scope of the role that you selected. You must select the check box against each object and then select the type of privileges (read, write, update, delete, and other actions) that you want to assign the user for the selected object. You can select one or more access privileges to assign to the user role. **NOTE:** You must assign at least one access privilege to a role. If you select the first-level objects, the submenu items that belong to the main object and the corresponding access privileges are also selected. The following access privileges can be assigned to a user role: • **Read**—Enables the user to read existing objects. • **Create**—Enables the user to create new objects. • **Update**—Enables the user to modify existing objects. • **Delete**—Enables the user to delete existing objects. You can also assign other actions to user roles. The other actions include retry, schedule update, schedule delete, activate, reboot, push license, clone, edit template, deploy, and upgrade history.

RELATED DOCUMENTATION

Role-Based Access Control Overview | 399

About the Roles Page | 412

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users | 415

Edit, Clone, and Delete User-Defined Roles for Service Provider, OpCo, and Tenant Users

IN THIS SECTION

- Edit Roles | 415
- Clone Roles | 416
- Delete Roles | 417

You can edit and delete custom (user-defined) roles of service provider, OpCo, and tenant users from the Roles page. You can also clone both predefined and custom roles.

> **NOTE:** You cannot edit or delete predefined roles.

This topic has the following sections:

Edit Roles

To modify the parameters configured for a role:

1. Select **Administration > Roles**.

   The Roles page appears, displaying the details of the available roles.

2. Select the role that you want to edit and click the edit icon (pencil) to modify the attributes.

   The Edit Role page appears. The fields on the Edit Role page are available for editing.

   > **NOTE:** You cannot modify the role name and role scope.

3. Modify the role description and privileges as needed.

4. Click **OK** to save the changes.

   A confirmation message appears, indicating the status of the edit operation.

Clone Roles

You can clone a role (both custom and predefined) when you want to quickly create a copy of an existing role and modify its access privileges.

1. Select **Administration > Roles**.

   The Roles page appears, displaying the details of the available roles.

2. Select the role that you want to clone and then click the **Clone** button at the top-right corner of the page.

   The Clone Role: *Role-Name* page appears.

3. Specify an appropriate name for the clone role.

4. Click **OK** to save your changes.

   A confirmation message appears, indicating the status of the clone operation.

   The name of the clone role is displayed on the Roles page.

5. Select the new clone role and click the edit icon (pencil) to modify the parameters.

   The Edit Role page appears.

6. Select the objects, and modify the access privileges of the role, as needed.

   NOTE: You cannot modify the role name and role scope.

7. Click **OK** to save your changes.

   A confirmation message appears, indicating the status of the edit operation.

Delete Roles

To delete a role:

1. Select **Administration > Roles**.

   The Roles page appears, displaying the details of the available roles.

2. Select the role that you want to delete and then click the delete icon (X).

   An alert message appears, asking you to confirm the delete operation.

3. Click **Yes** to delete the selected role.

   A confirmation message appears, indicating the status of the delete operation.

RELATED DOCUMENTATION

About the Roles Page | **412**

Add User-Defined Roles for Service Provider, OpCo, and Tenant Users | **413**

Access Privileges for Role Scopes (Operating Company and Tenant)

This topic describes the access privileges for the Operating Company (OpCo) and tenant role scopes. For more information about roles and role scopes, see "Roles Overview" on page 408.

Table 137 on page 418 shows the access privileges for operating company scope.

Table 138 on page 420 shows the access privileges for tenant scope.

Table 137: Access Privileges for Operating Company Scope

Role Scope	Menu Name	Actions	Other Actions
Operating company (OpCo)	SP Geo Map	Read	-
	Tenants SLA Performance	Read	-
	Alerts	Read and Delete	-
	Alarms	Read and Delete	-
	SD-WAN Alerts Definitions	Read	-
	Security Alert Definitions	Read	-
	Jobs	Read	Retry Schedule Update Schedule Delete
	POPs	Read	-
	Provider Hub Devices	Read	-
	Tenant Devices	Read	Configure Stage-2
	Device Templates	Read, Create, Update, and Delete	Clone Edit Template
	Images	Read	Upgrade History Deploy Stage
	SLA Based Steering Profiles	Read, Create, Update, and Delete	-
	Path Based Steering Profiles	Read, Create, Update, and Delete	-

Table 137: Access Privileges for Operating Company Scope *(continued)*

Role Scope	Menu Name	Actions	Other Actions
	Application Traffic Type Profiles	Read	-
	Network Services	Read	Detach Allocate
	Tenants	Read, Create, Update, and Delete	-
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Audit Logs	Read	Purge
	Authentication	Read, Create, Update, and Delete	-
	Device Licenses	Read, Create, Update, and Delete	Push
	CSO Licenses	Read, Create, and Update	-
	Dynamic Mesh	Read and Update	
	Signature Database	Read	-
	SMTP	Read and Update	-
	Terms of Use	Read and Update	
	Email Templates	Read and Update	-
	Getting Started	Read	-
	What's New	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

Table 138: Access Privileges for Tenant Scope

Role Scope	Menu Name	Actions	Other Actions
Tenant	Tenant GeoMap	Read	-
	Link Switch Events	Read	-
	Jobs	Read	Retry Schedule Update Schedule Delete
	SD-WAN Alert Definitions	Read	-
	Security Alert Definitions	Read, Create, Update, and Delete	-
	Alerts	Read and Delete	Jump to Event Viewer
	Alarms	Read and Delete	-
	Security Events	Read	Manage Filter Create Alert Create Report
	Application Visibility	Read	-
	Threats Map (Live)	Read	-
	Application SLA Performance	Read	-
	Devices	Read	

Table 138: Access Privileges for Tenant Scope *(continued)*

Role Scope	Menu Name	Actions	Other Actions
			Activate Traceroute Ping Push License Reboot RMA Discover APs Configure Stage2
	Device Configuration	Read and Update	-
	Images	Read	Upgrade History Stage Deploy
	Deployments	Read	Deploy Schedule
	Network Services	Read, Update, and Delete	Start Disable
	SD-WAN Policy	Read and Update	Deploy
	Tenant SLA Based Steering Profiles	Read, Create, Update, and Delete	-
	Tenant Path Based Steering Profiles	Read, Create, Update, and Delete	-
	Cloud Breakout Profiles	Read, Create, Update, and Delete	Assign Sites
	Firewall Policy	Read, Create, Update, and Delete	Deploy
	SSL Policy	Read, Create, Update, and Delete	Deploy

Table 138: Access Privileges for Tenant Scope *(continued)*

Role Scope	Menu Name	Actions	Other Actions
	NAT	Read, Create, Update, and Delete	Deploy
	UTM	Read, Create, Update, and Delete	-
	Schedule	Read, Create, Update, and Delete	-
	Address	Read, Create, Update, and Delete	-
	Department	Read, Create, and Delete	-
	Service	Read, Create, Update, and Delete	-
	Application Signature	Read, Create, Update, and Delete	Clone
	Site Management	Read, Create, and Delete	Configure Upgrade
	Site Groups	Read, Create, Update, and Delete	-
	Site LAN Segment	Read, Create, and Delete	Deploy Deploy History Re-assign
	Mesh Tags	Read, Create, and Delete	-
	Report Definitions - Security	Read, Create, Update, and Delete	Run Preview Send Clone
	Report Definitions - SD-WAN	Read, Create, Update, and Delete	Run Preview Send Clone
		Read and Delete	-

Table 138: Access Privileges for Tenant Scope *(continued)*

Role Scope	Menu Name	Actions	Other Actions
	Generated Reports -Security		
	Generated Reports SD-WAN	Read and Delete	-
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Audit Logs	Read	Purge
	Device Licenses	Read, Create, Update, and Delete	Push License
	CSO Licenses	Read	-
	Tenant Setting	Read, Create, and Update	-
	Tenant Signature Database	Read	Install
	Certificates	Read, Create, Update, and Delete	-
	VPN Authentication	Read	Renew CRL
	Identity Management	Read and Update	-
	Wi-Fi Settings	Read and Update	-
	Getting Started	Read	-
	What's New	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

RELATED DOCUMENTATION

Role-Based Access Control Overview | 399

About the Roles Page | 412

11

CHAPTER

Managing Jobs

About the Jobs Page | **426**

Viewing Job Details | **428**

Editing and Deleting Scheduled Jobs | **429**

Retrying a Failed Job on Devices | **431**

About the Jobs Page

To access this page, click **Monitor > Jobs**.

A job is an action that is performed on any object that is managed by CSO, such as a device, tenant, site, or user. You can monitor the status of jobs that have run or are scheduled to run in CSO. You can run the job immediately or schedule it for a later date and time. You can view the status of the job whether it is completed or failed. You can retry tssm.ztp type jobs that are failed.

Use this page to view the list of all jobs and the jobs that are scheduled to be executed. You can view general information about the jobs and the overall progress and status of the jobs. You can also edit and delete scheduled jobs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a job. See "Viewing Job Details" on page 428.
- Retry a job. See "Retrying a Failed Job on Devices" on page 431.
- Edit and delete schedule jobs. See "Editing and Deleting Scheduled Jobs" on page 429.

Field Descriptions

Table 139 on page 426 provides guidelines on using the fields on the Jobs page.

Table 139: Fields on the Jobs Page

Field	Description
Job Name	View the name of the job. CSO automatically generates the job name. Example: MSEC_DOWNLOAD_IPS/APPLICATION_SIGNATURES_08_Jul_17_124229_024
Status	View the status of the job to know whether the job succeeded, failed, or in progress. Example: Success
Owner	View the name of the owner who created the job. Example: cspadmin

Table 139: Fields on the Jobs Page *(continued)*

Field	Description
Number of Tasks	View the number of tasks associated with the job. Example: 2 For example, the tasks **site.ucpe-32** and **customer.sdwan** are associated with this job.
Job ID	When a job is initiated from a object in CSO, CSO assigns a unique ID to that job, which serves to identify the job (along with the job type) on the Jobs page. The following is a list of some of the job types supported in CSO: • Import POP • Configure Sites • Download Signature • Create Sites • Onboard Tenant • Create OpCo • Remove Site
Start Date	View the start date and time of a task associated with the job.
End State	View the end date and time of a task associated with the job.

Field Descriptions

Table 140 on page 427 provides guidelines on using the fields on the Scheduled Jobs page.

Table 140: Fields on the Scheduled Jobs Page

Field	Description
Schedule ID	View the unique ID of the scheduled job. The value is generated by the database when a new schedule record is inserted into the database. Example: 48
Name	View the unique name of the scheduled job. Example: Tenant Delete_csp.tssm_remove_site_e340354716ae43859fad5ba15669eee2

Table 140: Fields on the Scheduled Jobs Page *(continued)*

Field	Description
Status	View the status of the last triggered job. The default status is scheduled.
Record Type	View the job type. Example: tssm onboard tenant
Owner	View the name of the owner who scheduled the job. Example: cspadmin
Next Run Time	View the time when the job is scheduled to run next.

RELATED DOCUMENTATION

Editing and Deleting Scheduled Jobs | 429

Retrying a Failed Job on Devices | 431

Viewing Job Details

You can use the Detail for *Job-Name* page to view all the parameters of a job. This page has the following two tabs:

- **Details**—Displays the overall progress of the job and lists general information about the job (for example, the Job ID, Request ID, Created By, and so on). For more information about the field description on this page, see *About the Jobs Page*.
- **Tasks**—Displays the number of tasks associated with the job. A green check mark (success) or a red cross mark (failed) is displayed next to each task indicating the status of the task. You can click the Detailed View icon to view the summary of the task.

To view details of a job:

- Right-click the job name that you want to see the detailed view for and select **Detail View**.
- Select the job and click **More > Detail View**.

- Alternatively, hover over the job name and click the Detailed View icon that appears before it.

The Detail for *Job-Name* page appears, showing the details of the job and the number of tasks associated with the job. See *About the Jobs Page* for a description of each fields on this page.

RELATED DOCUMENTATION

About the Jobs Page | 426

Editing and Deleting Scheduled Jobs

IN THIS SECTION

Editing Scheduled Jobs | 429
Deleting Scheduled Jobs | 430

You can edit or delete scheduled jobs.

Editing Scheduled Jobs

You can modify the date and time of deployment of scheduled jobs.

To modify a scheduled job:

1. Select **Monitor > Jobs > Scheduled Jobs**.

   The Jobs page displays all scheduled jobs.

2. Select the job that you want to reschedule the deployment, and click the edit icon.

   The Edit Schedule page appears. This page displays the option that you have selected initially.

3. Modify the deployment type.

   To execute the job immediately, select the **Run now** option.

To reschedule the job for a later date and time, select the **Schedule at a later time** option and select the date and time of deployment.

4. Click **Save** to save the changes.

   A success message is displayed indicating that the scheduled job is modified.

Deleting Scheduled Jobs

You can delete one or more scheduled jobs.

To delete a scheduled job:

1. Select **Monitor > Jobs> Scheduled Jobs**.

   The Jobs page displays all scheduled jobs.

2. Select the job that you want to delete and then click the delete icon (X). You can select one or more jobs

   The Confirm Delete page appears.

3. Click **Yes** to confirm.

   A success message is displayed indicating that the scheduled job is deleted.

RELATED DOCUMENTATION

About the Jobs Page | 426

Viewing Job Details | 428

Retrying a Failed Job on Devices

As a service provider user or OpCo user with the Job Retry capability, you can retry a failed job instead of redoing the tasks involved in the job, to save time.

> **NOTE:** Before you retry a failed job, identify the reason for the failure and then fix it, before retrying the job.
>
> For example, if the bootstrap process failed because the device could not establish an outbound SSH connection, you must fix the problem and ensure that the outbound SSH connection is established before you retry the bootstrap job.

You can retry only the following jobs that did not complete successfully on your devices:

- ZTP jobs
- Bootstrap jobs

To retry a job that was not successful:

1. Select **Monitor > Jobs**.

   The Jobs page appears.

2. Select the failed job that you want to retry.

3. Click the **Retry Job** button on the top-right corner of the page.

   A retry job is created and executed.

   If the job is successful, a confirmation message appears and the job status changes to **Success** on the Jobs page.

RELATED DOCUMENTATION

About the Jobs Page | 426

Editing and Deleting Scheduled Jobs | 429

12

CHAPTER

Managing Audit Logs

Audit Logs Overview | **433**

About the Audit Logs Page | **433**

Viewing the Details of an Audit Log | **435**

Exporting Audit Logs | **437**

Purging Audit Logs (After Archiving or Without Archiving) | **439**

Audit Logs Overview

An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data.

Audit logs contain information about tasks initiated by using the Contrail Service Orchestration (CSO) GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries usually include details about user-initiated tasks, such as the name, role, and IP address of the user who initiated a task, the status of the task, and date and time of execution.

> **NOTE:** Device-driven tasks (that is, tasks not initiated by the user) are not recorded in audit logs.

Administrators can use audit logs to review events. For example, administrators can identify the user accounts associated with an event, determine the chronological sequence of events. For audit log entries that have an associated job, you can click the hyperlinked job ID to go to the Jobs page, where you can view the details of the job.

RELATED DOCUMENTATION

- About the Audit Logs Page | 433
- Exporting Audit Logs | 437
- Purging Audit Logs (After Archiving or Without Archiving) | 439

About the Audit Logs Page

To access this page, select **Administration** > **Audit Logs**.

Use the Audit Logs page to view the tasks that you have initiated either by using the Contrail Service Orchestration (CSO) GUI or APIs. You can also export audit logs as a comma-separated values (CSV) file and purge audit logs after archiving them or without archiving them.

Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of various user-initiated tasks by selecting **More** > **Details**. You can also mouse over the audit log and click on the **Detailed View** icon. See "Viewing the Details of an Audit Log" on page 435.
- Export audit logs as a CSV file—See "Exporting Audit Logs" on page 437.
- Purge audit logs—See "Purging Audit Logs (After Archiving or Without Archiving)" on page 439.
- Search for audit logs by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort and filter audit logs:

  NOTE: Sorting and filtering is applicable only to some fields.

  - Click a column name to sort the audit logs based on the column name.
  - Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. For example, you can use audit log filtering to track user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, monitor user login and logout activities over time, and so on.
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Audit Logs page.

Table 141 on page 434 provides description of the fields on the Audit Logs page.

Table 141: Fields on the Audit Logs Page

Field	Description
Username	Displays the username of the user who initiated the task.
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Object Name	Displays the name of the object on which the task was initiated. An object can be a tenant, site, device, device image, template, and so on.
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Description	Displays details about the task.

Table 141: Fields on the Audit Logs Page *(continued)*

Field	Description
Status	Displays the status of the task that triggered the audit log: • Success—Job or task was completed successfully. • Failure—Job or task failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Recurring job is scheduled.
End Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
Job ID	For tasks that have associated jobs, displays the ID of the job associated with the task. You can click the job ID to go to the Jobs page, where you can view the status of the job.

RELATED DOCUMENTATION

About the Jobs Page | **426**

Viewing the Details of an Audit Log

Use the Audit Log Details pane to view details of an audit log.

To view the details of an audit log:

1. Select **Administration** > **Audit Logs**.

   The Audit Logs page appears displaying the audit logs.

2. Select the audit log for which you want to view details and click **More** > **Details**. Alternatively, mouse over the audit log, and click on the **Detailed View** icon.

   The Audit Log Details pane appears on the right side of the Audit Logs page. Table 142 on page 436 provides descriptions of fields on the Audit Log Details pane.

3. Click the close icon (X) to close the Audit Log Details pane.

You are returned to the Audit Logs page.

Table 142: Fields on the Audit Log Details Pane

Field	Description
Details	
User	
Username	Displays the user who initiated the task.
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Task	
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Status	Displays the status of the task that triggered the audit log: • Success—Job or task was completed successfully. • Failure—Job or task failed and was terminated. • Job Scheduled—Job is scheduled but has not yet started. • Recurring Job Scheduled—Recurring job is scheduled.
Description	Displays details about the task.
Affected Objects	
Object Name	Displays the name of the affected object on which the task was initiated. An affected object can be a tenant, site, device, device image, template, and so on.. Click the hyperlinked object name to view details of the object: **NOTE:** If the object is deleted or if you do not have permissions to view it, an error message is displayed.
Object UUID	Displays the Universally Unique Identifier (UUID) of the affected object.
Log Info	
Audit Log ID	Displays the automatically-generated unique ID of the audit log associated with the task.

Table 142: Fields on the Audit Log Details Pane *(continued)*

Field	Description
Job ID	For tasks that have associated jobs, displays the ID of the job associated with the task. You can click the job ID to go to the Jobs page, where you can view the status of the job.
End Time	Displays the date and time at which the task completed execution. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
Raw Audit Log	
Microservice	Displays the name of the microservice that initiated the task.
Raw Audit Log	Displays all the fields of the audit log that are stored in the database. The raw audit log typically contains additional details or parameters associated with the audit log.

RELATED DOCUMENTATION

- About the Audit Logs Page | 433
- Audit Logs Overview | 433

Exporting Audit Logs

You can export audit logs as comma-separated values (CSV) file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration** > **Audit Logs**.

   The Audit Logs page appears displaying the audit logs.

2. Click **Export**.

   The Export Audit Logs page appears.

3. Specify the time period for which you want to export the audit logs according to the guidelines provided in Table 143 on page 438.

> **NOTE:** You can export audit logs for a maximum of 30 days prior to the current date and time. For example, if the current date is May 31, 2018, you can export the audit logs starting from May 1, 2018.

4. Click **OK** to export the audit logs.

   Depending on the settings of the browser that you are using, the CSV file containing the audit logs for the specified time period is either downloaded directly, or you are asked to open or save the file.

   You are returned to the Audit Logs page.

   After the file is downloaded, you can open the CSV file in an application such as Microsoft Excel and view and analyze the logs as required.

Table 143: Fields on the Export Audit Logs Page

Field	Description
Start Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when the audit logs should be exported.
End Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) up to when the audit logs should be exported.

RELATED DOCUMENTATION

- Audit Logs Overview | 433
- About the Audit Logs Page | 433
- Viewing the Details of an Audit Log | 435

Purging Audit Logs (After Archiving or Without Archiving)

You can manage the volume of audit log data stored by purging log files from the CSO database without archiving them or by purging log files after archiving them. You can purge audit logs immediately or schedule the purging for a later date and schedule the purging on a recurring basis.

To purge audit logs after archiving or without archiving them:

1. Select **Administration** > **Audit Logs**.

   The Audit Logs page appears displaying the audit logs.

2. Click **Purge**.

   The Purge Audit Logs page appears.

3. Complete the configuration according to the guidelines provided in Table 144 on page 439.

   NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **OK**.

   You are returned to the Audit Logs page and one of the following operations occur:

   - If you triggered a purge of the audit logs without archiving, a job to purge the audit logs is created.
   - If you triggered a purge of the audit logs after archiving, a job is created to archive the audit logs and then purge the audit logs after archiving.

   After the audit logs are purged successfully, the Audit Logs page refreshes automatically and displays only the audit logs that were not purged.

Table 144: Purge Audit Logs Settings

Field	Description
Purge Options	

Table 144: Purge Audit Logs Settings *(continued)*

Field	Description
Purge Logs	Select one of the following options to purge audit logs: • Purge audit logs that were generated before a specified date and time—If you select this option, you must enter a date and time in the **Before** field. • Purge generated audit logs that are older than a specified number of days—If you select this option, you must specify the number of days in the **Older than** field.
Before	To purge audit logs before a specified date and time, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) You specify the time in the local time zone of the client computer.
Older than	To purge generated audit logs older than a specified number of days, enter the number of days (from 1 through 90)
Archive Logs Before Purging	To archive audit logs *before* purging them, select this check box. By default, this check box is cleared, which means that audit logs are purged without archiving them. **CAUTION:** If you choose not to archive the audit logs before purging, the audit logs are deleted from the CSO database and cannot be recovered.
Archive Mode	Specify whether you want to archive the log files locally (**local**) or on a remote server (**remote**). If you archive the logs on a remote server, which is the default option, you must enter access and login details for the remote server. **NOTE:** • Archived log files are saved in a single file in compressed comma-separated values (CSV) format (extension .zip). • When you archive data locally, the archived log files are saved on the central microservices virtual machine (VM).
Username	Enter a valid username to access the remote server.
Password	Enter a valid password to access the remote server on which the audit logs will be archived.
Confirm Password	For confirmation, re-enter the password to access the remote server.
Remote Server IP Address	Enter the IPv4 address of the remote server; for example, 192.0.2.10.

Table 144: Purge Audit Logs Settings *(continued)*

Field	Description
Remote Server Path	Enter the directory path on the remote server on which to store the archived log files. The directory that you specify must already exist on the remote server.
Schedule Purge	
Type	Specify whether the audit logs should be purged immediately (**Run now**) or schedule the purge for later (**Schedule at a later time**). If you schedule the purge for later, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the purge to occur. You specify the time in the local time zone of the client computer.
Recurrence	To specify whether the purge operation should occur on a recurring basis, select this check box. **NOTE:** This option is enabled only if you choose to archive and purge audit logs older than a specified number of days.
Repeat	Specify the periodicity of the recurrence. Currently, a weekly periodicity is the only option supported.
On	For purges that recur every week, specify one or more days on which you want the purge to recur.
Time	Enter the time (in HH:MM:SS 24-hour or AM/PM format) that you want the recurring purge to occur. By default, the purge recurs at 12.00 AM. You specify the time in the local time zone of the client computer.
Ends	Specify whether the recurring purge ends or not: • Select **Never** to continue (without an end date) the recurring purge operation at the specified recurrence interval. • Select **On** and enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) on which to stop the recurring purge operation. You specify the time in the local time zone of the client computer.

RELATED DOCUMENTATION

Audit Logs Overview | 433

About the Audit Logs Page | 433

13

CHAPTER

Monitoring

About the Monitor Overview Page | **445**

Alerts Overview | **446**

About the Generated Alerts Page | **447**

About the Alert Definitions/Notifications Page | **449**

Managing Security Alerts Definitions | **449**

Creating Security Alert Definitions | **451**

Editing, Cloning, and Deleting Security Alert Definitions | **452**

About the Alarms Page | **454**

Enable E-mail Notifications for SD-WAN Alarms | **456**

Rogue Device Detection | **458**

Multitenancy | **459**

About the SLA Performance of All Tenants Page | **460**

About the SLA Performance of a Single Tenant Page | **463**

Monitoring Application-Level SLA Performance for Secure SD-WAN-Advanced | **467**

Viewing the SLA Performance of a Site | **469**

Viewing the SLA Performance of an Application or Application Group | 474

Understanding SLA Performance Score for Applications, Links, Sites, and Tenants | 476

About the Monitor Overview Page

To access this page, click **Monitor > Overview**.

You can use the Monitor Overview page to view information about the alarms and alerts for tenants, POPs, connections, and sites on a geographical map. The network operator views the alarms and alerts, and then takes the necessary actions to resolve the issues.

Tasks You Can Perform

You can perform the following tasks from this page:

- View POP details.
- View site details.
- View connections.
- View only the nodes with alerts.

Field Descriptions

Table 145 on page 445 shows the descriptions of the fields on the Monitor Overview page.

Table 145: Fields on the Monitor Overview Page

Field	Description
POPs	View the POP in which the site is located. Click the **POPs** drop-down list and select **POP Name**. Enter the name of the POP.
Sites	View the sites at which the service is deployed. Click the **Sites** drop-down list and enter the name of the site.
Connections	View the connections in the network. Click the **Connections** drop-down list and select **Show connections**.

Table 145: Fields on the Monitor Overview Page *(continued)*

Field	Description
Only the node with alerts	View the nodes with issues with the service. Click the drop-down list located next to the **Only the nodes with alerts** check box and select the type of alerts. • Critical—Issues that prevent the node from working and require action from the operator. The nodes with critical alerts are displayed in red. • Major—Issues that prevent the node from working at this time, but they do not require action from the operator. The nodes with major alerts are displayed in orange. • Minor—Issues that allow a node to continue working, but not optimally. The network operator may need to take action to resolve the issue. The nodes with minor alerts are displayed in yellow. **NOTE:** The nodes without any alerts are displayed in blue.

RELATED DOCUMENTATION

About the Alert Definitions/Notifications Page | 449

Creating SD-WAN Alert Definitions

Alerts Overview

Alerts and notifications are used to notify administrators about significant events within the system. Notifications can also be sent through e-mail. You will be notified when a predefined network traffic condition is met. The alert trigger threshold is the number of network traffic events crossing a predefined threshold within a period of time.

Alerts and notifications provide options for:

- Defining alert criteria based on a set of predefined filters. You can use the filters defined in the advanced search to create an alert. You can also save filters and add them to security alert definitions.
- Generating an alert message and notifying you when alert criteria are met.
- Searching for specific alerts on the Generated Alerts page based on alert ID, description, or alert type.
- Supporting event-based alerts.

For example, If you are an administrator, you can define a condition such that if the number of firewall-deny events crosses a predefined threshold in a given time range for a specific device, you will receive an e-mail alert.

> **NOTE:** If a threshold is crossed and remains so for a long duration, new alerts are not generated. Alerts are generated again when the number of logs matching the alert criteria drops below the threshold and crosses the threshold again.

RELATED DOCUMENTATION

About the Generated Alerts Page | 447

About the Alert Definitions/Notifications Page | 449

About the Generated Alerts Page

To access this page, click **Monitor > Alerts & Alarms > Alerts**.

Use this page to view the system event-based alerts in response to a configured alert definition. The generated alerts help you to identify problems that appear in your monitored network environment and displays both security and SD-WAN alerts. You can view statistics such as the number of critical and non-critical alerts.

Tasks You Can Perform

You can perform the following tasks from this page:

- Select the generated alert and then right-click or click **More > Detail View**. The Alert Detail page appears displaying all the details of the alert.
- Select the generated alert and then right-click or click **More > Clear All Selections**.

Field Descriptions

Table 146 on page 448 provides information about the fields on the Generated Alerts page.

Table 146: Fields on the Generated Alerts Page

Field	Description
Severity	View the severity of the alert.
Time	View the date and time when the alert was generated.
Site	View the name of the tenant site.
Source	View the source of the alert. The source identifies whether an alert is a security alert or an SD-WAN alert.
Description	View the description of the alert.
Alert Type	View the type of alert.
ID	View the alert ID. Alert ID is an unique identification for each alert. For example, b4a3c027-7157-4861-8e3c-c872721cff2d.
Service Instance	View the service instance associated with the alert.
Object Type	View the object type.
Alert Name	View the name of the alert.
Tenant	View the name of the tenant.

RELATED DOCUMENTATION

About the Alert Definitions/Notifications Page | 449

Creating SD-WAN Alert Definitions

Editing and Deleting SD-WAN Alert Definitions

About the Alert Definitions/Notifications Page

To access this page, select **Monitor > Alerts & Alarms > Alert Definitions/Notifications** in the Administration Portal.

Use the Alert Definitions page to manage security alert definitions and enable or disable SD-WAN alarm notification. An alert definition consists of data criterion for triggering alerts about issues in the SD-WAN environment. Alert definitions also define the necessary action required to resolve issues based on the severity of the alert. An alert is triggered when the event threshold exceeds the data criteria that is defined. You can create an alert definition to monitor your data in real time and identify issues and attacks before they impact your network.

Tasks You Can Perform

You can perform the following tasks from this page:

- Manage security alert definitions. See "Managing Security Alerts Definitions" on page 449.
- Enable or disable the e-mail notification for alarms. See "Enable E-mail Notifications for SD-WAN Alarms" on page 456.
- View existing security alert definitions by clicking **Security**. See [Unresolved xref] for descriptions of the fields on the Security alert definitions pane.
- Show or hide columns that contain information about SD-WAN and Security alert definitions—Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for alert definitions using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Managing Security Alerts Definitions

Use the Security pane to generate alerts that warn you of problems in your monitored environment. An alert definition consists of data criteria for triggering an alert. An alert is triggered when the event threshold exceeds the data criteria that is defined.

Tasks You Can Perform

You can perform the following tasks from this pane:

- Create security alert definition. See "Creating Security Alert Definitions" on page 451.
- Edit, clone, and delete security alert definition. See "Editing, Cloning, and Deleting Security Alert Definitions" on page 452.

Field Descriptions

Table 147 on page 450 provides guidelines on using the fields on the Security alert definitions pane.

Table 147: Fields on the Security Alert Definitions Pane

Field	Description
Alert Name	View the name of the alert.
Alert Description	View the description for the alert.
Filter	View filter values of the alert.
Recipients	View recipients' e-mail addresses where alert notifications are sent.
Status	View the status of the alert.
Alert Type	View the type of alert. Example: Event-based

RELATED DOCUMENTATION

Alerts Overview

Creating Security Alert Definitions

You can create an alert definition to monitor your data in real time. You can identify issues and attacks before they impact your network.

For example, if you are an administrator, you can define a condition such that if the number of firewall deny events crosses a predefined threshold in a given time frame for a specific device, you receive an e-mail alert.

To create a security alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

   The Security alert definitions page appears.

2. Click the create icon (+) or add icon (+).

   The Create an Alert Definition page appears.

3. Complete the configuration according to the guidelines provided in Table 148 on page 451.

4. Click **OK**. If you want to discard the changes, click **Cancel** instead.

A new alert definition with the configured alert triggering condition is created. You can view the generated alerts from the alert definition to troubleshoot the issues with your system.

Table 148: Fields on the Security Alert Definitions Page

Field	Description
General	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Alert Description	Enter a description for the alerts; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system-based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: info, minor, major, critical.
Trigger	

Table 148: Fields on the Security Alert Definitions Page *(continued)*

Field	Description
Use Data Criteria from Filters	Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer. To add saved filters: • Click the **Use data criteria** from filters link. The Add Saved Filters page appears. • Select the filters to be added. • Click **OK**.
Add Data Criteria	Specifies the data criteria based on the Time Span period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.
Recipient(s)	
E-mail Address(es)	Specify the e-mail addresses for the recipients of the alert notification.
Custom Message	Enter a custom string for identifying the type of alert in the alert notification e-mail.

RELATED DOCUMENTATION

Managing Security Alerts Definitions | 449
Editing, Cloning, and Deleting Security Alert Definitions | 452

Editing, Cloning, and Deleting Security Alert Definitions

IN THIS SECTION

Editing Security Alert Definitions | 453
Cloning Security Alert Definitions | 453
Deleting Security Alert Definitions | 454

You can edit, clone, and delete security alert definitions.

Editing Security Alert Definitions

To edit the security alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

   The Security Alerts Definition page appears.

2. Select the check box of the security alert definition that you want to modify, and click the edit icon.

   The Edit Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Update the configuration as needed.

4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

Cloning Security Alert Definitions

You can clone an alert definition when you want to quickly create a copy of an alert definition and modify its parameters including the name of the alert.

To clone an alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

   The Security Alert Definitions page appears.

2. Select the alert definition that you want to clone, and click **More > Clone** at the top right corner of the page.

   The Clone Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Click **OK** to save the configuration.

   A new alert definition is created.

Deleting Security Alert Definitions

You can click the delete icon (X) to delete one or more alert definitions.

To delete the alert definition:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications > Security Alerts Definitions**.

   The Security Alerts Definition page appears.

2. Select the alert definition that you want to delete and click the delete icon (X icon).

   The Confirm Delete page appears.

3. Click **Yes** to delete the alert definition or **No** to cancel the deletion.

   If you click **Yes**, then the alert definition is deleted from the main page.

RELATED DOCUMENTATION

Managing Security Alerts Definitions | 449
Creating Security Alert Definitions | 451

About the Alarms Page

To access this page, select **Monitor > Alerts & Alarms > Alarms** in the Administration Portal.

Use this page to view system generated alarms. Alarms alert you to conditions that might prevent the device from operating normally. System alarm conditions are preset based on fault monitoring and performance monitoring (FMPM) being performed on a device. For example, conditions such as hardware issues, drop in throughput and latency of data, temperature variations, and capacity optimization issues automatically trigger an alarm.

NOTE: To generate alarms correctly, ensure that CSO and the devices are NTP enabled, and in sync. The time set on CSO must match with the time set on the devices.

The difference between alerts and alarms lies in the type of events that are being monitored. An alert is used to notify administrators about significant events within the system. For example, when a predefined network traffic condition is met. For more information about alerts, see "Alerts Overview" on page 446.

Tasks You Can Perform

You can perform the following tasks from this page:

- View alarm activity within a specific time range:
  - You can select the time range by clicking on the options provided—2 hours (2h), 4 hours (4h), 8 hours (8h), 16 hours (16h), 24 hours (24h), or 1 week (1w). By default, alarm activity is displayed for 1 week.
  - You can view alarm activity for a custom time range by clicking on **Custom** and providing the time range.
- View details about the alarm. See Table 149 on page 455 for more information.
- Select the generated alarm and then right-click or click **More > Detail View** to view the details of the alarm.

Field Descriptions

Table 149 on page 455 provides information about the fields on the Alarms page.

Table 149: Fields on the Alarms Page

Field	Description
Severity	View the severity of the alarm.
Time	View the date and time when the alarm was generated.
Tenant	View the name of the tenant.
Site	View the site for which the alarm was generated.
Source	View the source of the alarm.
Description	View the description of the alarm.
ID	View the alarm ID.

Table 149: Fields on the Alarms Page *(continued)*

Field	Description
Link Name	View the name of the link that generated the alarm.
Service Instance	View the service instance associated with the alarm..
Object Type	View the type of alarm. Example: Event-based
POP	View the point of presence (POP) of the alarm.

RELATED DOCUMENTATION

About the Generated Alerts Page | 447

About the Alert Definitions/Notifications Page | 449

Enable E-mail Notifications for SD-WAN Alarms

Starting from CSO Release 5.1.1, you now notify the user (tenant administrators and tenant operators) about SD-WAN alarms. You can also specify the minimum severity level of alarms that must be notified to the users. Alarm notifications enable users to take action to ensure that the network runs smoothly.

NOTE: You can enable or disable the e-mail notification for SD-WAN alarms if you are an SP administrator, or OpCo administrator, or tenant administrator.

To enable e-mails notifications for SD-WAN alarms:

1. Select **Monitor > Alerts & Alarms > Definitions/Notifications**.

   The Definitions/Notifications page appears.

2. Select the **SD-WAN Alarm Notifications** tab.

   The SD-WAN Alarm Notifications page appears.

3. Complete the configuration according to the guidelines provided in Table 150 on page 457.

NOTE: Fields marked with an asterisk (*) are mandatory.

4. Click **Save** to save the changes.

If you have enabled e-mail notifications, an e-mail will be sent to the user based on the severity level that you specified for an alarm.

If you have disabled e-mail notifications, the users will not receive e-mail notifications in case of alarms.

Table 150: SD-WAN Alarm Notifications Settings

Field	Description
Send Email Notifications	Click the toggle button to enable or disable the e-mail notifications of alarms to users. By default, e-mail notifications are disabled. After enabling this field, you must specify the minimum severity level of the alarm and select the e-mail addresses of the users.
Minimum Severity to Report	Select the minimum severity level (critical, major, minor) of the alarms to users through an e-mail. • Critical—If you select this option, e-mail notifications are sent to users only for alarms with the severity level critical. • Major—If you select this option, e-mail notifications are sent to users only for alarms with the severity levels major or critical. • Minor—If you select this option, e-mail notifications are sent to users only for alarms with the severity levels minor, major, or critical.
Recipients	Select one or more e-mail addresses of the users from the list. Only users with tenant administrator or tenant operator roles are listed. The e-mail addresses listed are based on the users that are listed in the Administration > Users page.

Release History Table

Release	Description
5.1.1	Starting from CSO Release 5.1.1, you now notify the user (tenant administrators and tenant operators) about SD-WAN alarms. You can also specify the minimum severity level of alarms that must be notified to the users. Alarm notifications enable users to take action to ensure that the network runs smoothly.

RELATED DOCUMENTATION

About the Alert Definitions/Notifications Page

Rogue Device Detection

Starting in Release 6.1.0, CSO detects any unauthorized device that attempts to access the network. On detection, CSO immediately rejects the connection request from the device and generates an alarm so that administrators can take remedial actions promptly.

CSO generates an alarm indicating unauthorized access in the following scenarios:

- **Scenario 1:** An unauthorized device attempts to connect using the configuration of a device that is modeled but not yet provisioned on CSO.

  Users might create (model) a site and provision (activate) the site later. In such a case, the device (for example, device A) at the site is not connected to the CSO network. If a rogue device attempts to connect to the CSO network by using the configuration of device A, CSO rejects the connection request and generates an alarm.

  Users can clear the alarm in the **Monitor > Alerts & Alarms** page after taking the necessary actions such as blocking the traffic originating from the rogue device.

  CSO clears the alarm automatically when the original device is provisioned and connected to CSO.

  The alarm message that is displayed for this scenario is as follows:

  ```
  Rejected connection from an unauthorized device! A device with serial number
  serial number of rogue device attempted to connect to CSO as device A registered
   with CSO with serial number serial number of device A. Verify the serial number
   in the stage 1 configuration applied on the device or if the device is an
  unauthorized one, take immediate action to block the device.
  ```

- **Scenario 2:** An unauthorized device attempts to connect using the configuration of a device that is provisioned on the CSO network.

  If a device attempts to connect to the CSO network using the configuration of a provisioned device, CSO identifies the device as a rogue device and rejects the connection. CSO also raises an alarm to notify the users. Users can clear the alarm in the **Monitor > Alerts & Alarms** page after taking the necessary actions to block the device from accessing the network again.

  The alarm message that is displayed for this scenario is as follows:

```
Rejected connection request from an unauthorized device! A device with serial
number serial number of rogue device and device ID device id of rogue device
attempted to connect to CSO. A device with the same device ID and serial number
 serial number of provisioned device is already provisioned on CSO. Take immediate
 action to prevent the unauthorized device from accessing your network again.
```

Multitenancy

Multitenancy enables provider hub devices to serve departments across multiple tenants. Each department of a tenant can have its own Layer 3 VPNs if network segmentation is enabled for the tenant. Traffic from all the Layer 3 VPNs are carried over to the provider hub using a shared overlay. The overlay tunnel [generic routing encapsulation (GRE) or GRE over IPsec] is used to carry traffic from all departments in a site through MPLS-based traffic separation.

Multitenancy is a cost-effective approach where the cost of a device and its maintenance is shared among multiple tenants. With multitenant device support, a dedicated share of the device is allocated to each tenant, and the data is kept private among the tenants that access the same device.

A service provider administrator or an OpCo administrator can perform the following tasks:

- Create tenants.
- Manage applications for each tenant.
- Create SD-WAN and security policies for each tenant and monitor the dashboard at the tenant level or at the department level.
- Add traffic type profiles.
- Configure steering based SD-WAN or security services for each tenant.
- View the services and networks configured for each tenant.

RELATED DOCUMENTATION

About the SLA Performance of a Single Tenant Page | 463

Viewing the SLA Performance of a Site | 469

About the SLA Performance of All Tenants Page

To access this page, select **Monitor > Tenants SLA Performance** in the Administration Portal.

You can use the Tenants SLA Performance page to view the SLA performance of all tenants. This page displays the list of tenants with low, medium, and high SLA performance during a specified time range. By default, the data is shown for the previous one day. You can change the time range for which the data is displayed. Tenants with low and medium SLA performance are grouped together. The SLA performance classification is done based on the **Performance Threshold** value you set. You can customize the view by selecting the card or grid view.

Tasks You Can Perform

You can perform the following tasks from this page:

- Specify performance threshold values based on which tenants can be classified as tenants with low, medium, or high SLA performance.
- View the SLA performance of all tenants that have low or medium SLA performance in the specified time period.
- View the SLA performance of all tenants that have high SLA performance in the specified time period.
- Select grid or card view for tenant SLA performance.

  Select the **Card** view or the **Grid** view at the top right of the page to switch between views. By default, the card view is selected.
- You can customize the time range to view the SLA performance of all tenants.

  Select the time range for which you want to view SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.

Field Descriptions

Table 151 on page 461 describes the fields on the Tenants SLA Performance page.

Table 151: Fields on the Tenants SLA Performance Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance. You can choose between card and grid views. By default, card view is selected.
Performance Threshold	Specify the performance threshold, in percentage, based on which tenants can be classified as tenants with low, medium, or high SLA performance. To set the performance threshold, click **More** > **Performance Threshold**. From the **Performance Threshold** dialog box, move the slider button to set the low and high thresholds. Tenants that have a performance score below the low threshold are marked as having low SLA performance and tenants that exceed the high threshold are marked as having high SLA performance. Tenants that have a performance score between the low and high are considered as having medium SLA performance.
Tenants with Low and Medium Performance	View tenants that have low and medium SLA performance in the selected time period. The low and medium performance classification is done based on the performance threshold you specify. Click each tenant to view information about the SLA performance of the sites in the tenant. See "About the SLA Performance of a Single Tenant Page" on page 463.
Tenants with High Performance	View the tenants that have high SLA performance in the selected time range. Click each tenant to view information about the SLA performance of the sites in the tenant. See "About the SLA Performance of a Single Tenant Page" on page 463.

Table 152 on page 461 describes the fields in the card and grid views.

Table 152: Fields in the Card and Grid Views of Tenants SLA Performance Page

Field	View	Description
Name	Card and Grid	Name of the tenant.
Sites	Card and Grid	Number of sites associated with the tenant.

Table 152: Fields in the Card and Grid Views of Tenants SLA Performance Page *(continued)*

Field	View	Description
SLA Performance	Card and Grid	Displays the SLA performance score on a scale of 100. Scores that exceed the high performance threshold are displayed in green. Scores that are below the low performance threshold are displayed in red, and the medium scores that are between the low and high performance threshold are displayed in orange. For information about SLA performance score, see "Understanding SLA Performance Score for Applications, Links, Sites, and Tenants" on page 476.
Sites with Low Performance	Card and Grid	Number of sites with low SLA performance.
SLA Not Met Events	Grid	Number of events that failed to meet the SLA.
Total Sessions	Card and Grid	Total number of sessions during the specified period.
Session Switch Count	Grid	Number of instances when a session switch occurred because of non-compliance with SLA. Note that the session switch count may have a value higher than the total sessions if multiple SLA violations occur for all the sessions.
Total Tenant Traffic	Card and Grid	Total traffic across all sites and links for the specified tenant.
Transmitted Bytes	Card and Grid	Total outgoing traffic from the tenant.
Received Bytes	Card and Grid	Total incoming traffic to the tenant.

RELATED DOCUMENTATION

- About the SLA Performance of a Single Tenant Page | 463
- Viewing the SLA Performance of a Site | 469
- Viewing the SLA Performance of an Application or Application Group | 474
- Adding SLA-Based Steering Profiles | 357
- Adding Path-Based Steering Profiles | 369

About the SLA Performance of a Single Tenant Page

To access this page from the Administration Portal, select **Monitor** > **Tenant SLA Performance** and then, click the name of the tenant for which you want view the site-level SLA performance information.

> **NOTE:** Sites with the Secure SD-WAN Essentials service do not support SLA performance monitoring and are displayed in the **Unsupported Sites** section on the *Tenant Name* SLA Performance page.

You can use the *Tenant-Name* SLA Performance page to view SLA performance of all sites in a tenant. This page displays the list of sites with low, medium, and high SLA performance during the specified time range. By default, the data is shown for the previous one day. You can change the time range for which the data is displayed. Sites with low and medium SLA performance are grouped together. The SLA performance classification is done based on the **Performance Threshold** value you set. You can customize the view by selecting card or grid views

Tasks You Can Perform

You can perform the following tasks from this page:

- Specify performance threshold values based on which sites can be classified as sites with low, medium, or high SLA performance.
- View the SLA performance of all sites that have low or medium SLA performance in the specified time period.
- View the SLA performance of all sites that have high SLA performance in the specified time period.
- View the SLA performance for all sites in a tenant in grid or card views.

  Select the **Card** view or the **Grid** view at the top right of the page. By default, the card view is selected.
- Customize the time range to view the SLA performance for all sites in a tenant.

  Select the time range for which you want to view SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.

Field Descriptions

Table 153 on page 464 describes the fields on the SLA Performance of a Single Tenant page.

Table 153: Fields on the SLA Performance of a Single Tenant Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance for all sites in the tenant. You can choose between card and grid views. By default, card view is selected.
Performance Threshold	Specify the performance threshold based on which sites can be classified as sites with low, medium, or high SLA performance. The performance threshold is specified in percentage terms. To set the performance threshold, click **More** > **Performance Threshold**. From the **Performance Threshold** dialog box, move the slider button to set the low and high thresholds. Site that have a performance score below the low threshold are marked as having low SLA performance and sites that exceed the high threshold are marked as having high SLA performance. Sites that have a performance score between the low and high are considered as having medium SLA performance.
Sites with Low and Medium Performance	View sites that have low and medium SLA performance in the selected time period. The low and medium performance classification is done based on the performance threshold you specify. Click each site to view information about application-level SLA performance. See "Application and Link Level SLA Performance" on page 465.
Sites with High Performance	View the sites that have high SLA performance in the selected time range. Click each site to view information about the application-level SLA performance. See "Application and Link Level SLA Performance" on page 465.

Table 154 on page 465 describes the fields in the card and grid views.

Table 154: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views

Field Name	Card or Grid View	Description
Site name	Card and Grid	Name of the tenant.
AppQoE Function	Card and Grid	Shows whether AppQoE is enabled or not. AppQoE is enabled only when the SD-WAN mode is set to Real time-Optimized.
SLA Performance	Card and Grid	Displays the SLA performance score on a scale of 100. Scores that exceed the high performance threshold are displayed in green. Scores that are below the low performance threshold are displayed in red, and the medium scores that are between the low and high performance threshold are displayed in orange. For information about SLA performance score, see "Understanding SLA Performance Score for Applications, Links, Sites, and Tenants" on page 476.
Total sessions	Card and Grid	Total number of sessions during the specified period.
Total Bytes	Card and Grid	Total traffic across all links for the specified tenant.
Transmitted Bytes	Card and Grid	Total outgoing traffic from the site.
Received Bytes	Card and Grid	Total incoming traffic to the site.

Application and Link Level SLA Performance

When AppQoE is enabled, you can view SLA performance of all applications in the site. You can also customize your view by selecting graph view or grid view. In the graph view, you can further select scatter plot or tree map views.

Table 155 on page 466 describes the fields on the SLA Performance of a Single Tenant page.

Table 155: Fields on the SLA Performance of a Single Tenant Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance. You can choose between graph and grid views. By default, graph view is selected.
View App Names	Select this check box to view the names of the applications in the graph view.
Top 10 applications	Select this check box to see the top 10 applications.
Application SLA Performance	
Departments	Select All Departments to view application SLA data for all departments, or select one department to view application SLA data specific to that department. By default, All Departments is selected.
SLA Parameters	Choose one of the following SLA parameters based on which you want to view the application SLA performance data: • Throughput • Latency metric • Packet loss • Jitter metric By default, Throughput is selected. The data for the selected parameter is displayed in the y-axis in the scatter plot view.
Group by	Select whether you want to group the applications based on the SLA Profile or the Traffic Type. By default, the SLA Profile option is selected.
SLA Profile	If you selected **SLA Profile** for **Group by**, select the SLA Profile for which you want to view the SLA performance information. This option is available only if you selected **SLA Profile** for **Group by**.
Traffic Type	If you selected **Traffic Type** for **Group by**, select the **Traffic Type** for which you want to view the SLA performance information. This option is available only if you selected **Traffic Type** for **Group by**.

Table 155: Fields on the SLA Performance of a Single Tenant Page *(continued)*

Field	Description
Graph	Select whether you want to view the SLA performance information for applications in the **Scatter Plot** view or in **Tree Graph** view. By default, **Scatter Plot** is selected.
Link SLA Performance	
Traffic Type	Select the traffic type for which you want to view the link SLA performance. You can choose either **All Traffic Type** or one of the available traffic types.
Links	Select the links for which you want to view the SLA performance. You can choose either **All Links** or one of the available links.

RELATED DOCUMENTATION

- About the SLA Performance of All Tenants Page | **460**
- Viewing the SLA Performance of a Site | **469**
- Viewing the SLA Performance of an Application or Application Group | **474**
- Adding SLA-Based Steering Profiles | **357**
- Adding Path-Based Steering Profiles | **369**

Monitoring Application-Level SLA Performance for Secure SD-WAN-Advanced

CSO uses the system log information from SRX devices to monitor application-level SLA performance and displays the relevant information on the **Monitor** > **Tenant SLA Performance** page of the Admin Portal and the **Monitor** > **Application SLA Performance** page of the Customer Portal.

For Tenants with Secure SD-WAN Advanced service, CSO uses the class-of-service values and the probe results to assign each application, site, and tenant scores that indicate the SLA performance. For more

information about the SLA performance scores, see "Understanding SLA Performance Score for Applications, Links, Sites, and Tenants" on page 476.

The following sections explain how you can view the SLA performance information at tenant level, site level, and application level:

1. Viewing SLA Performance of Tenants | **468**
2. Viewing SLA Performance of Sites | **468**

Viewing SLA Performance of Tenants

Service provider administrators and OpCo administrators can view the SLA performance of all the tenants from the **Monitor** > **Tenant SLA Performance** page.

To view the SLA performance of all tenants:

1. From the administration portal, click **Monitor** > **Tenant SLA Performance**.

   The "Tenant SLA Performance" on page 460 page appears.

2. Customize the view to your specific requirements.

   For customization options, see Table 151 on page 461

   The Tenants SLA Performance page displays the SLA performance information for all the tenants in the format and for the time range you specified. For each of the tenant, you can view the details as described in Table 152 on page 461

Viewing SLA Performance of Sites

Service provider administrators and OpCo administrators can view SLA performance information for all the sites associated with a tenant.

To view SLA performance information for the sites associated with a tenant:

1. From the administration portal, click **Monitor** > **Tenant SLA Performance**, and then click the name of the tenant for which you want view the site-level SLA performance information.

   The *Tenant Name* SLA Performance page appears. For more information, see "About the SLA Performance of a Single Tenant Page" on page 463.

> **NOTE:** On the *Tenant Name* SLA Performance page, sites with the Secure SD-WAN Essentials service are displayed in the **Unsupported Sites** section, because SD-WAN Essentials service does not support SLA performance monitoring.

2. Customize the view as required. For more information about the customization options, see Table 153 on page 464

   The *Tenant Name* SLA Performance page displays the information in the format and for the time range you specified. For each of the sites, you can view the information as explained in Table 154 on page 465.

3. Click the name of the site to view more details about application-level and link-level SLA performance. A new page appears with graphical representation of SLA performance information for the site as well as the applications and links available in the site.

   You can customize the view as described in Table 155 on page 466.

Viewing the SLA Performance of a Site

IN THIS SECTION

- SLA Not Met by SLA Profiles | **470**
- Applications SLA Performance by Throughput | **471**
- SLA Performance for ALL | **473**

You can use the **Monitor > *Tenant-Name* SLA Performance > *Site-Name* SLA Performance** page in the Administration Portal to view SLA performance for all applications and application groups in a site. You can view the SLA performance for all applications and application groups in a site for a specified time range and in graph or grid views.

The ***Site-Name* SLA Performance** page is divided into the following three sections:

SLA Not Met by SLA Profiles

You can use the **SLA Not Met by SLA Profiles** section on the ***Site_name* SLA Performance** page to view the SLA profiles for which SLA requirements were not met and the time at which they were not met. The y-axis represents the SLA profiles and the x-axis represents the specified time range. The **SLA Not Met by SLA Profiles** section can be viewed and remains the same in both graph and grid views.

To view a graphical representation of SLA profiles for which SLA target values were not met:

1. Select the time range for which you want to view the SLA profiles for which SLA target values were not met. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.

   The graphical representation of SLA profiles for which SLA target values were not met is displayed for the selected time range.

2. (Optional) You can use the sliders at the sides of the graph to further customize the time range.

   The graphical representation of SLA profiles for which SLA target values were not met is refreshed and displayed for the customized time range. The graphical representation of SLA performance data in the subsequent sections on the page is also refreshed and displayed for the customized time range.

Applications SLA Performance by Throughput

You can view average throughput performance of all applications and application groups in a site. You can also customize your view by selecting graph view or grid view. In the graph view, you can further select scatter plot or tree map views.

To view a graphical representation of average throughput performance of all applications and application groups in a site:

1. Select **Graph View** at the top right of the page. By default, Graph View is selected.

   A graphical representation of average throughput performance of all applications and application groups in a site against the target throughput is displayed in the **Scatter Plot** view. The y-axis represents the average throughput. 0% on the x-axis represents the target throughput (in %) defined in the SLA profiles, while the regions on the left and right of the target represent percentages below and above the target throughput, respectively.

   A carousel at the bottom of the section also displays the list of all applications and application groups with their SLA profiles, target throughput, and average throughput values.

2. Click **Legend** at the bottom right of the section to view the plotting legend.

   The items described in the **Legend** are:

   - A single application is represented by a blue circle.
   - An application group is represented by a blue square.
   - An application or application group whose target throughput value in the SLA profile was modified during runtime is represented by an uncolored circle or uncolored square, respectively.
   - The SLA profiles are represented by their priority numbers within the colored or uncolored circles and squares.

3. (Optional) You can use the sliders at the sides of the graph further to customize the time range.

   The carousel is refreshed for the customized time range.

4. Click the circles or squares to view more information about the application or application groups. See "Viewing the SLA Performance of an Application or Application Group" on page 474.

> **NOTE:** You can also select **Tree Map** at the top right of the section to view a list of all applications and application groups in a site and their average throughput values.
>
> A list of all applications and application groups in a site along with their associated SLA profiles and the average throughput values is displayed.

To view a tabular representation of average throughput performance of all applications and application groups in a site:

1. Select **Grid View** at the top right of the page.

   A list of all applications and application groups along with their SLA profiles, average throughput, and target throughput values is displayed in a tabular format.

   Table 156 on page 472 describes the fields on the Applications SLA Performance by Throughput grid view.

   Table 156: Fields on the Applications SLA Performance by Throughput Grid View

Field	Description
Name	View name of the application or application group.
SLA Profile	View the SLA profile associated with the application or application group.
Type	View the type—application or application group
Category	View the category of the application or application group. The value of category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on.
Sessions	View the number of sessions consumed by the application or application group.
Throughput Avg. Performance	View the average throughput performance value (in %) of the application or application group. The upward triangle on the left of the average throughput performance value indicates that the average throughput is higher than the target throughput configured in the SLA profile of the application or application group. The value (in %) denotes the percentage above the target throughput value. Similarly, the downward triangle on the left of the average throughput performance value indicates that the average throughput is lower than the target throughput configured in the SLA profile of the application or application group. The value (in %) denotes the percentage below the target throughput value.

2. (Optional) Click the details icon to the left of the application or application group name to view more details about the application or application group. See "Viewing the SLA Performance of an Application or Application Group" on page 474.

SLA Performance for ALL

View a graphical representation of the performance of the SLA parameters such as round-trip time (RTT), latency, packet loss, and jitter for the specified time range for MPLS and Internet WAN links for all SLA profiles. The y-axis represents the SLA parameters and the x-axis represents the specified time range. You can also view the respective target SLA parameters in the graphs.

> **NOTE:** The graphical representation of the performance of all SLA parameters for the WAN links is available only in the graph view.

To view a graphical representation of the performance of all SLA parameters for the WAN links:

- Select **All** at the top right of the section. By default, **All** is selected.

  A graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range for all WAN links is displayed.

- Select **wan_0**, **wan_1**, and so on at the top right of the section to view the performance of the SLA parameters for the MPLS and Internet WAN links. You can enable and configure **wan_0**, **wan_1**, and so on and map them to MPLS or Internet links when you create a site.

  The graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range is refreshed and only the performance for the selected WAN link is displayed.

- (Optional) Click **Legend** at the bottom right of the section to view the plotting legend for the horizontal dotted lines parallel to the x-axis in the graphs. The horizontal dotted lines represent the respective target SLA parameters of the SLA profiles.

> **NOTE:** RTT is represented as Delay on the "About the SLA-Based Steering Profiles Page" on page 354 and "About the Path-Based Steering Profiles Page" on page 366 page.

RELATED DOCUMENTATION

About the SLA Performance of All Tenants Page | 460

About the SLA Performance of a Single Tenant Page | 463

Viewing the SLA Performance of an Application or Application Group | 474

Viewing the SLA Performance of an Application or Application Group

You can use the **Monitor > *Tenant-Name* SLA Performance > *Site-Name* SLA Performance** page in the Administration Portal to view the SLA performance of individual applications and application groups in a site. You can also view the SLA performance of the associated SLA profile for all SLA parameters.

To view SLA performance of an application or application groups:

- Click one of the circles or squares in the **Applications SLA Performance by Throughput** section on the ***Site-Name* SLA Performance** page.

  The page that appears displays SLA performance details of the application or application group.

Table 157 on page 474 describes the fields on the application or application group SLA Performance details page.

Table 157: Fields on the Application or Application Group Details Page

Field	Description
Category and Description	View the category of the application or application group. The category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on. You can also view a description of the application or application group.
SLA	View the name of the SLA profile associated with the application or application group.
Target	View the current target throughput defined in the SLA profile associated with the application or application group. If the target throughput was modified during runtime, the date and time when the throughput was modified and the previously defined throughput value are also displayed.
Avg. Performance	View the average throughout performance (in %) above or below the configured target throughput. The average throughput (in Mbps) is displayed within parentheses.
SLA Metrics by Throughput	View a graphical representation of the SLA metrics by throughput during the specified time range for that application or application group. The y-axis represents the throughput (in Mbps). The x-axis represents the specified time range. Hover over the graph to view the throughput value and time at any specified point. You can also view the sessions consumed by the WAN links for the application or application group for the specified time range.

Table 157: Fields on the Application or Application Group Details Page *(continued)*

Field	Description
Global SLA Profile Performance	View the performance for all the SLA parameters of the SLA profile associated with the application or application group. The SLA performance is represented by a color-coded donut chart. The section in blue in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were met. The section in red in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were not met. Click the red colored section of the donut chart to view more information about when SLA requirements for the SLA profile were not met. The **SLA Profile Performance** page appears. The SLA Profile Performance page displays the following fields: • SLA Profile—SLA profile associated with the application or application group • Target—Target throughput configured in the SLA profile • SLAs Not Met—Percentage of time SLA requirements were not met for the SLA profile • Sessions—Number of sessions consumed by the application or application group • Start Time—Time at which the WAN links associated with the application or application groups started to fail meeting the SLA requirements • End Time—Time at which SLA profile requirements started to be met again • Avg Val—Average throughput (in Mbps) when the SLA requirements started to fail • Duration—Total duration (in seconds) during which SLA requirements were not met • From—Source WAN link • To—Destination WAN link

RELATED DOCUMENTATION

About the SLA Performance of All Tenants Page | **460**

About the SLA Performance of a Single Tenant Page | **463**

Viewing the SLA Performance of a Site | **469**

Understanding SLA Performance Score for Applications, Links, Sites, and Tenants

IN THIS SECTION

- Application Score | 476
- Site Score | 477
- Tenant Score | 477
- Link Score | 477

This topic explains the following SLA performance scores:

Application Score

CSO supports Application Quality of Experience (AppQoE) to improve the user experience at the application level. In real time-optimized SD-WAN networks, CSO monitors application traffic using passive probes, which are inline probes sent along with the application traffic. Based on various parameters collected from the passive probes, CSO assigns a score to each of the applications. Based on the sampling rate you specified as part of the traffic type profile, CSO sends passive probes to detect packet loss, jitter, and violations in RTT. If the probe detects any of these issues, a syslog is generated and a violation count is added for the session.

The following metrics are used to calculate the application score:

- Session Violation Count
- Sampling Percentage
- Total Session Count

NOTE: Application score is available only in real time-optimized SD-WAN networks.

Site Score

For AppQoE enabled (real time-optimized SD-WAN) networks, site score is calculated as an aggregate of individual parameters across all applications in the site. For information about application score calculation, see “Application Score” on page 476.

Tenant Score

Tenant score is calculated as the average value of site scores. For information about site score calculation, see “Site Score” on page 477.

Link Score

Link score is calculated based on the following SLA parameters collected using AppQoE active probes (in real time-optimized networks) or RPM probes:

- Latency
- Jitter
- Packet Loss

For VoIP traffic, the link score calculation also considers the R-Value and MOS.