

Contrail Service Orchestration Administration Portal User Guide

Published
2020-11-07

Release
5.0.3

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

5.0.3

Copyright © 2020 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 | xiv

Documentation and Release Notes | xiv

Documentation Conventions | xiv

Documentation Feedback | xvii

Requesting Technical Support | xvii

Self-Help Online Tools and Resources | xviii

Creating a Service Request with JTAC | xviii

1

Introduction

Contrail Service Orchestration Release 5.0.0 | 20

Accessing Administration Portal | 20

Administration Portal Overview | 23

Switching the Tenant Scope | 23

About the Administration Portal Dashboard | 24

Tasks You Can Perform | 24

Field Descriptions | 25

Changing the Administration Portal Password | 26

Resetting Your Password | 27

Resetting the Password for OpCo and Tenant Users | 29

Setting Password Duration | 29

Extending the User Login Session | 30

2

Managing E-Mail

Configuring SMTP Settings | 32

Customizing E-mail Templates | 33

3

Managing Authentication

Authentication Methods Overview | 37

About the Authentication Page | 37

Tasks You Can Perform | 38

Field Descriptions | 38

Configuring a Single Sign-On Server | 39

Editing and Deleting SSO Servers | 42

Editing SSO Server Configuration | 42

Delete SSO Server Configurations | 43

4

Managing Tenants

Tenant Overview | 45

Full Mesh Topology Overview | 45

Local Breakout in Full Mesh Topology | 46

About the Tenants Page | 47

Tasks You Can Perform | 47

Field Descriptions | 48

Adding a Single Tenant | 49

Importing Data for Multiple Tenants | 62

Creating a Tenant Data File | 62

Importing Tenant Data | 66

Viewing the History of Imported Tenant Data | 66

Viewing the History of Deleted Tenant Data | 68

Dynamic VPN Tunnels Overview | 71

Configuring Dynamic VPN Tunnels Threshold for all Tenants | 73

Updating the Terms of Use | 75

Managing Resources

About the POPs Page | 79

Tasks You Can Perform | 79

Field Descriptions | 79

About the Sites Page | 80

Tasks You Can Perform | 81

Field Descriptions | 81

Manually Importing Provider Hubs with OAM Capability | 82

About the Tenant Devices Page | 83

Tasks You Can Perform | 83

Field Descriptions | 84

About the Cloud Hub Devices Page | 87

Tasks You Can Perform | 87

Field Descriptions | 88

Adding a Provider Hub Device | 90

Managing a Tenant Device | 94

Managing an EX Series Switch | 95

Viewing the Chassis Information of an EX Series Switch | 96

Viewing Information about an EX Series Switch | 99

Viewing Information about Ports on an EX Series Switch | 101

Device Redundancy Support Overview | 105

Prerequisites for using SRX Series Devices for Device Redundancy | 105

Supported Connection Plans | 105

Create and Configure an SD-WAN Site | 106

Dual CPE Devices Logical Topology for NFX Network Services Platform | 106

Dual CPE Devices Logical Topology for SRX Series Gateway Devices | 107

Viewing the History of Tenant Device Activation Logs | 108

Secure OAM Network Overview | 110

- Topology of a Secure OAM Network | 110
- Workflow for Establishing a Secure OAM Network | 111
- Benefits of Secure OAM Network | 112

Secure OAM Network Redundancy Overview | 112

- Logical Topology | 113
- BGP Configuration | 114
- Adding and configuring provider hub devices | 114
- Adding and configuring an on-premise spoke site | 115
- Failure Detection and Recovery | 115
- Benefits of Secure OAM Network Redundancy | 115

Rebooting Tenant Devices and Provider Hub Devices | 116

- Rebooting a Tenant Device | 116
- Rebooting a Provider Hub Device | 117

Identifying Connectivity Issues by Using Ping | 118

Identifying Connectivity Issues by Using Traceroute | 122

Remotely Accessing a Device CLI | 124

Device Template Overview | 126

- Hybrid WAN CPE | 127
- SD-WAN CPE | 128
- Secure Internet CPE | 129
- Managed Internet CPE | 130

About the Device Template Page | 132

- Tasks You Can Perform | 132
- Field Descriptions | 133
- Supported Device Templates | 134

Cloning a Device Template | 137

Importing a Device Template | 138

- Creating a Device Template File | 138
- Importing a Device Template File | 139

Configuring Template Settings in a Device Template 	140
Updating Stage-2 Configuration Template in a Device Template 	174
Configuring Stage-2 Initial Configuration in a Device Template 	178
Modifying a Device Template Description 	181
Deleting a Device Template 	181
APN Overview 	182
Benefits of APN Configuration	183
Configuring APN Settings on CPE Devices 	183
Configuring APN Settings with SIM Change on CPE Devices	184
Configuring APN Settings without SIM Change on CPE Devices	186
Device Images Overview 	187
About the Device Images Page 	187
Tasks You Can Perform	188
Field Descriptions	188
Staging an Image 	189
Deploying Device Images to Devices 	191
Uploading a Device Image 	194
Deleting Device Images 	196
Network Services Overview 	197
About the Network Services Page 	197
Tasks You Can Perform	198
Field Descriptions	198
About the Service Overview Page 	200
Tasks You Can Perform	200
Field Descriptions	200
About the Service Instances Page 	202
Tasks You Can Perform	202
Field Descriptions	202

6

Managing Signatures

Signature Database Overview | 205

About the Signature Database Page | 205

Tasks You Can Perform | 206

Field Descriptions | 206

Downloading a Signature Database | 207

Download Locations for Signature Database | 209

Application Signatures Overview | 210

About the Application Signatures Page | 211

Tasks You Can Perform | 211

Field Descriptions | 212

Understanding Custom Application Signatures | 213

Adding Application Signatures | 214

Editing, Cloning, and Deleting Application Signatures | 219

Editing Application Signatures | 219

Cloning Application Signatures | 220

Deleting Application Signatures | 220

Creating Application Signature Groups | 221

Editing, Cloning, and Deleting Application Signature Groups | 222

Editing Application Signature Groups | 222

Cloning Application Signature Groups | 223

Deleting Application Signature Groups | 223

7

Managing Profiles

Application Quality of Experience (AppQoE) Overview | 226

Workflow | 227

About the Application Traffic Type Profiles Page | 227

Default Traffic Type Profiles | 228

Tasks You Can Perform | 229

Field Descriptions | 230

About the SLA-Based Steering Profiles Page | 231

Tasks You Can Perform | 231

Field Descriptions | 231

Adding SLA-Based Steering Profiles | 235

Editing and Deleting SLA-Based Steering Profiles | 242

Editing an SLA-Based Steering Profile | 242

Deleting SLA-Based Steering Profiles | 243

About the Path-Based Steering Profiles Page | 244

Tasks You Can Perform | 244

Field Descriptions | 244

Adding Path-Based Steering Profiles | 247

Editing and Deleting Path-Based Steering Profiles | 249

Editing a Path-Based Steering Profile | 249

Deleting a Path-Based Steering Profile | 250

8

Managing Licenses

About the Device License Files Page | 252

- Tasks You Can Perform | 252

- Field Descriptions | 252

Uploading a Device License File | 253

Editing and Deleting Device Licenses | 254

- Editing a Device License Entry | 255

- Deleting a Device License | 255

Pushing a License to Devices | 256

About the CSO Licenses Page | 257

- Tasks You Can Perform | 257

- Field Descriptions | 257

Assign CSO Licenses, and Update or Unassign CSO License Assignments | 259

- Assign CSO Licenses to Tenants | 259

- Update or Unassign CSO License Assignments | 261

9

Managing Users and Roles

Role-Based Access Control Overview | 264

About the Users Page in Administration Portal | 265

- Tasks You Can Perform | 265

- Field Descriptions | 265

Adding OpCo Users | 266

Editing and Deleting OpCo Users | 268

- Editing OpCo Users | 269

- Deleting OpCo Users | 269

Resetting the Password for OpCo and Tenant Users | 270

Roles Overview | 271

- Types of Roles | 271

- Role Scopes | 272

- Access Privileges | 272

Relationship Between Users, Roles, and Access Privileges | 273

Benefits of Roles in CSO | 273

About the Roles Page | 274

Tasks You Can Perform | 274

Field Descriptions | 274

Adding User-Defined Roles for OpCo, and Tenant Users | 275

Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users | 277

Editing Roles | 277

Cloning Roles | 278

Deleting Roles | 279

Access Privileges for Role Scopes (Operating Company and Tenant) | 279

10

Managing Jobs

About the Jobs Page | 289

Tasks You Can Perform | 289

Field Descriptions | 289

Field Descriptions | 290

Viewing Job Details | 291

Editing and Deleting Scheduled Jobs | 292

Editing Scheduled Jobs | 292

Deleting Scheduled Jobs | 293

Retrying a Failed Job on Devices | 294

11

Managing Audit Logs

Audit Logs Overview | 296

About the Audit Logs Page | 296

Tasks You Can Perform | 297

Viewing the Details of an Audit Log | 298

Exporting Audit Logs | 300

Purging Audit Logs (After Archiving or Without Archiving) | 302

Monitoring

About the Monitor Overview Page | 308

Tasks You Can Perform | 308

Field Descriptions | 308

Alerts Overview | 309

About the Generated Alerts Page | 310

Tasks You Can Perform | 310

Field Descriptions | 311

About the Alert Definitions Page | 312

Tasks You Can Perform | 312

Field Descriptions | 312

Creating SD-WAN Alert Definitions | 314

Editing and Deleting SD-WAN Alert Definitions | 315

Editing an SD-WAN Alert Definition | 316

Deleting SD-WAN Alert Definitions | 316

About the Alarms Page | 317

Tasks You Can Perform | 317

Field Descriptions | 317

About the Device Events Page | 318

Tasks You Can Perform | 319

Advanced Search | 319

Field Descriptions | 320

Multidepartment CPE Device Support | 323

About the SLA Performance of All Tenants Page | 324

Tasks You Can Perform | 324

Field Descriptions | 324

About the SLA Performance of a Single Tenant Page | 327

Tasks You Can Perform | 327

Field Descriptions | 327

Application and Link Level SLA Performance | 329

Monitoring Application-Level SLA Performance for real time-optimized SD-WAN | 331

Viewing SLA Performance of Tenants | 332

Viewing SLA Performance of Sites | 332

Viewing the SLA Performance of a Site | 333

SLA Not Met by SLA Profiles | 333

Applications SLA Performance by Throughput | 334

SLA Performance for ALL | 336

Viewing the SLA Performance of an Application or Application Group | 337

Understanding SLA Performance Score for Applications, Links, Sites, and Tenants | 339

Application Score | 339

Site Score | 340

Tenant Score | 340

Link Score | 340

About the Documentation

IN THIS SECTION

- Documentation and Release Notes | xiv
- Documentation Conventions | xiv
- Documentation Feedback | xvii
- Requesting Technical Support | xvii

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 xv](#) 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 xv 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
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>

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

Convention	Description	Examples
<i>Italic text like this</i>	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 <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">• 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 <i>metric</i>>;
(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 (<i>string1</i> <i>string2</i> <i>string3</i>)
# (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 [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

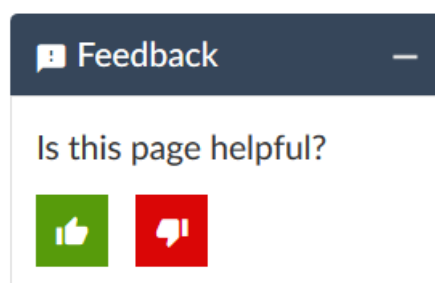
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> 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

[Contrail Service Orchestration Release 5.0.0 | 20](#)

[Accessing Administration Portal | 20](#)

[Administration Portal Overview | 23](#)

[Switching the Tenant Scope | 23](#)

[About the Administration Portal Dashboard | 24](#)

[Changing the Administration Portal Password | 26](#)

[Resetting Your Password | 27](#)

[Resetting the Password for OpCo and Tenant Users | 29](#)

[Setting Password Duration | 29](#)

[Extending the User Login Session | 30](#)

Contrail Service Orchestration Release 5.0.0

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

CSO Release 5.0.0 supports two types of accounts at the highest level:

- OpCo account—for multitenant service providers [also known as Operating Companies (OpCo)]; OpCo administrators can add tenants to the OpCo network and manage profiles and policies for traffic, SLA, breakout, and firewall management.
- Tenant account—for enterprise customers that want to use CSO for managing their sites; tenant administrators can add sites to the tenant network; configure SLA policies, firewall policies, and breakout policies; and apply the policies to the sites.

Based on the account type that you signed up for, you receive the link to the CSO portal along with the login credentials when the account is activated. OpCo account owners receive the account activation e-mail that contains the link to the OpCo portal and the login credentials from Juniper Networks. However, for tenant accounts, the account activation e-mail is sent by Juniper Networks or the OpCo from which the tenant has purchased the tenant account.

You can log in to the portal by using the link and credentials provided in the account activation e-mail.

You must reset the password when you first log in to the portal. After you reset the password, log in to the portal using the new credentials.

Accessing Administration Portal

To access Administration Portal:

1. If you are 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 3 on page 22](#).
- 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 to access the Contrail Service Orchestration (CSO) GUIs.

3. Enter your username and password.

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 4 on page 22](#).

Table 3: Fields on the Change Password Page

Field	Description
New Password	<p>Enter your new password.</p> <p>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.</p> <p>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.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select Show Password to view the password.</p>

Table 4: 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](#) | 23

Administration Portal Overview

Administration Portal offers OpCo administrators a convenient way to set up and manage resources, customers, and availability of network services through a graphical user interface (GUI).

When you use Administration Portal, you are actually creating and managing objects used by the following APIs in the Cloud CPE Centralized Deployment Model and Cloud CPE Distributed Deployment Model.

- Cloud CPE Tenant, Site, and Service Manager API, which manages customers (also called *tenants*), manages customer sites, and maps each customer's network services to the appropriate gateway resources, such as the Layer 2 access interfaces and routing instances.
- Identity and Access Manager API, which manages identifiers and roles for customers and users.
- Network Service Orchestration API, which manages network services and communicates with Contrail OpenStack, the virtualized infrastructure manager (VIM).
- Contrail OpenStack API, which manages network points of presence (POPs), service chains, and virtual machines (VMs) that contain service chains.

You can also set up and manage the Cloud CPE Centralized Deployment Model and Cloud CPE Distributed Deployment Model through API calls, either manually or from your operational support systems and business support systems (OSS/BSS). This method is more complex, especially if you use your own OSS/BSS, in which case you must perform development and integration work. Use of Administration Portal is particularly beneficial for companies who require a turnkey solution and do not want to expend effort on developing programs to set up and manage the deployment through APIs. Even if you plan to use your own OSS/BSS systems to set up and manage the Cloud CPE Centralized Deployment Model and Cloud CPE Distributed Deployment Model in a production environment, Administration Portal can prove useful for demonstrations and trials of the deployment.

RELATED DOCUMENTATION

| [Accessing Administration Portal](#) | 20

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

Unified Administration and Customer Portal Overview

[Role-Based Access Control Overview](#) | 264

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 5 on page 25](#) describes the dashboard widgets.

Table 5: Widgets on the Dashboard

Widget	Description
Tenant Sites: Total Alerts	<p>Displays the total number of alerts grouped by severity level.</p> <p>Click each alert name to view the total number of tenant sites receiving alerts that are critical, major, or minor.</p>
Top 5 POPs with Alerts	<p>Displays the top five POPs receiving alerts.</p> <ul style="list-style-type: none"> • 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 Alerts	<p>Displays the top five tenant sites receiving alerts.</p> <ul style="list-style-type: none"> • Name—Name of the tenant site. • Location—Location of the tenant site. • Status—Type of alerts received that are critical, major, or minor.

Table 5: Widgets on the Dashboard (*continued*)

Widget	Description
Top 5 Tenants with Alerts	<p>Displays the top five tenants receiving alerts.</p> <ul style="list-style-type: none"> • Name—Name of the tenant. • Sites—Number of sites in the tenant location. • Status—Type of alerts received that are critical, major, or minor.

RELATED DOCUMENTATION

[Administration Portal Overview](#) | 23

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 **Change Password**.

The Change Password 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. Enter the current password.

4. 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.

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

You can select the **Show Password** option to view the password.

6. Click **OK**.

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](#) | 23

[Accessing Administration Portal](#) | 20

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 6 on page 28](#).

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 6: Fields on the Set Password Page

Field	Description
Password	<p>Enter your new password.</p> <p>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.</p> <p>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.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select Show Password to view the password.</p>
Terms of Use	Select the check box to agree to the terms of use document.

RELATED DOCUMENTATION

[Accessing Administration Portal | 20](#)

[Changing the Administration Portal Password | 26](#)

[Changing the Password on First Login](#)

[Setting Password Duration | 29](#)

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 49](#).

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 | 20](#)

[Changing the Administration Portal Password | 26](#)

[Changing the Password on First Login](#)

[Resetting Your Password | 27](#)

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 | 26](#)

2

CHAPTER

Managing E-Mail

[Configuring SMTP Settings | 32](#)

[Customizing E-mail Templates | 33](#)

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 7 on page 32](#).

3. Click **Save**.

The status of the save operation is displayed.

Table 7: 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	<p>Enable this option if the e-mail server requires authentication before an e-mail can be sent.</p> <p>The Username and Password fields are displayed when you enable this option.</p> <p>Disable this option if you want to configure an unauthenticated e-mail server.</p> <p>The From Name and From E-Mail Address fields are displayed when you disable this option.</p>

Table 7: 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](#) | 37

[About the Authentication Page](#) | 37

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 | 37](#)

[About the Authentication Page | 37](#)

[Configuring a Single Sign-On Server | 39](#)

[Editing and Deleting SSO Servers | 42](#)

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 | 37](#)

[Configuring a Single Sign-On Server | 39](#)

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:

- Configure an SSO server. See [“Configuring a Single Sign-On Server” on page 39](#).
- Edit and delete an SSO server. See [“Editing and Deleting SSO Servers” on page 42](#).

Field Descriptions

[Table 8 on page 38](#) provides guidelines on using the fields on the Authentication page.

Table 8: Fields on the Authentication Page

Field	Description
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
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: <i>*@aaa-example.com</i>
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

Table 8: Fields on the Authentication Page (*continued*)

Field	Description
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 | 37](#)
[Configuring a Single Sign-On Server | 39](#)

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 a 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 9 on page 40](#).

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 9: 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: <ul style="list-style-type: none"> • 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 9: 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 10 on page 41 .

Table 10: 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 | 37](#)

[Editing and Deleting SSO Servers | 42](#)

Editing and Deleting SSO Servers

IN THIS SECTION

- [Editing SSO Server Configuration | 42](#)
- [Delete SSO Server Configurations | 43](#)

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

Editing 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 | 37](#)

[Configuring a Single Sign-On Server | 39](#)

4

CHAPTER

Managing Tenants

[Tenant Overview | 45](#)

[Full Mesh Topology Overview | 45](#)

[About the Tenants Page | 47](#)

[Adding a Single Tenant | 49](#)

[Importing Data for Multiple Tenants | 62](#)

[Viewing the History of Imported Tenant Data | 66](#)

[Viewing the History of Deleted Tenant Data | 68](#)

[Dynamic VPN Tunnels Overview | 71](#)

[Configuring Dynamic VPN Tunnels Threshold for all Tenants | 73](#)

[Updating the Terms of Use | 75](#)

Tenant Overview

A tenant in a Contrail Service Orchestration represents a customer who accesses virtualized network functions (VNFs) in an OpCos cloud through a Layer 3 VPN. You assign administrative users and sites to customers in the Administration Portal to 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.

RELATED DOCUMENTATION

[Administration Portal Overview | 23](#)

[About the Tenants Page | 47](#)

[Adding a Single Tenant | 49](#)

[Importing Data for Multiple Tenants | 62](#)

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.

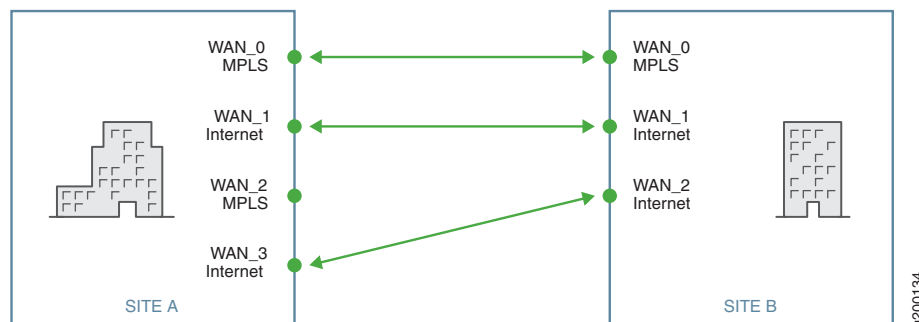
For more information about mesh tags, see *Mesh Tags Overview*.

The full mesh topology supports the following:

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

Contrail Service Orchestration 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 46](#)). 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.

RELATED DOCUMENTATION

Traffic-Based Steering Profiles and SD-WAN Policies Overview

[About the Tenants Page | 47](#)

Breakout and Breakout Profiles Overview

About the Tenants Page

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

A tenant in Contrail Service Orchestrator is a customer who can use one or more services (SD-WAN, Hybrid-WAN, Next Gen firewall, or LAN). You can use this page to add tenants, view tenant details, delete tenants, and add CSO license to a tenant. You can add tenants by importing tenant-related data through a JSON file. See [“Tenant Overview” on page 45](#).

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**. See *Viewing Object Details*.
- Add a single tenant. See [“Adding a Single Tenant” on page 49](#).
- Delete a tenant. Select the tenant that you want to delete and click the delete icon.
- Import multiple tenants. See [“Importing Data for Multiple Tenants” on page 62](#).
- Assign Network Services. See *Allocating Network Services to a Tenant*.
- View tenant import history. See [“Viewing the History of Imported Tenant Data” on page 66](#).
- View tenant delete history. See [“Viewing the History of Deleted Tenant Data” on page 68](#).

Field Descriptions

Table 11 on page 48 provides guidelines on using the fields on the Tenants page.

Table 11: Fields on the Tenants Page

Field	Description
Name	<p>Name of the tenant.</p> <p>Click the name to view full information about a tenant.</p>
Deployment Type	Displays the SD-WAN mode (real-time optimized or bandwidth-optimized) of the tenant. A hyphen (-) is displayed if the site type is Hybrid WAN, or Next Gen Firewall, or LAN.
Site Types	Displays one or more site capabilities (SD-WAN, Hybrid WAN, Next Gen Firewall, LAN) that the tenant can add.
Sites	Total number of sites that are available for the tenant.
Assigned Services	<p>Number of services that are assigned to the tenant.</p> <p>To assign services to the tenant:</p> <ol style="list-style-type: none"> 1. Click the Allocate Network Services link in Assigned Service column. The Allocate Network Services to <i>Tenant-Name</i> 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).
Administrator	Administrative user for the tenant.
Last Modified	Date and time when the tenant was last modified.

RELATED DOCUMENTATION

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:

- SD-WAN service
- Hybrid WAN service
- Next Gen Firewall service
- LAN service

TIP: A single tenant with SD-WAN service supports both full mesh or hub-and-spoke topologies.

To connect sites in hub-and-spoke topology,

- Select the SD-WAN mode as bandwidth-optimized in the Add Tenant page, or
- Select the SD-WAN mode as real-time optimized, and do not enable the **Enable Meshing** toggle button in the Configure Site page.

To connect sites in full mesh topology,

- Select the SD-WAN mode as real-time optimized (or you must have selected both real-time optimized and bandwidth-optimized) in the Add Tenant page, and
- Select the **Enable Meshing** toggle button for at least one WAN link in the Configure Site page.

In earlier versions of CSO, when a tenant user logs in to the Customer Portal for the first time, the user is assigned the Tenant Administrator role by default. With the introduction of object-based custom roles, the tenant user that logs in to Customer Portal for the first time might have customized roles and the role is not restricted to Tenant Administrator.

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 enter only the username.

To add a tenant:

1. Select **Tenants > All Tenants > +**.

The Add Tenant page appears.

2. Update the tenant information. Complete the configuration according to the guidelines provided in [Table 12 on page 50](#).

3. Click **OK** to add a tenant. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the tenant that you configured appears on the Tenants page. 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 12: Fields on the Add Tenant Page

Field	Description
<i>Tenant Info</i>	
Name	Enter a unique name for the tenant. You can use alphanumeric characters and hyphen (-); the maximum length is 15 characters. Example: test-tenant
<i>Admin user</i>	
First Name	Enter the first name of the user.
Last Name	Enter the last name of the user.
Username (Email)	Enter the e-mail ID of the user. The e-mail ID is also the username for the user. This field is automatically populated after you enter the tenant name. Example: test-tenant_admin@test-tenant.com

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Roles	<p>Select one or more roles (both predefined and custom roles) that you want to assign to the tenant user.</p> <p>NOTE: In the Available column, all tenant scope roles are listed.</p> <p>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.</p> <p>To preview the access privileges assigned to a role, click the role name.</p>
<i>Password Policy</i>	
Password Expiration Days	<p>Specify the duration (in days) after which the password expires and must be changed.</p> <p>The range is from 1 through 365. The default value is 180 days.</p>
Deployment Info	

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Service for Tenant	<p>Select one or more services for the tenant:</p> <ul style="list-style-type: none"> • 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. • Hybrid WAN—Select this option if you want the tenant to add Hybrid WAN sites. The Hybrid WAN sites can have up to two WAN links. You cannot apply intent policies for Hybrid WAN sites. • Next Gen Firewall—Select this option if you want the tenant to add a standalone firewall site for the CPE device. • LAN—Select this option if you want the tenant to provision and monitor switches to optimize performance and maintain SLAs in a LAN. The switch can be provisioned as a standalone device or connected to a CPE device. <p>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 SD-WAN and LAN for a tenant, in Customer portal > Resources > Sites Management > Add > On-Premise Spoke, only the following capabilities are listed:</p> <ul style="list-style-type: none"> • SD- WAN • LAN

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
SD-WAN Mode	<p>NOTE: This field appears only if you selected the SD-WAN sites check box in the Deployment Type field.</p> <p>Select the SD-WAN mode:</p> <ul style="list-style-type: none"> • Bandwidth-optimized—CSO uses link-level probes to switch traffic from links that do not meet SLA criteria to links that meet SLA. This is selected by default. If you select the bandwidth-optimized option, all sites in the tenant are connected to the hub (hub-and-spoke topology). • Real time-optimized—CSO monitors application-level traffic and delegates the application-level probes and link switching to CPE. Select this mode if you want to implement AppQoE. If you select the real time-optimized option, all sites in the tenant are connected in full mesh or hub-and-spoke topology. <p>NOTE: The Dynamic VPN page and Mesh Tags page appears in the Customer Portal only if you have selected the Real time-optimized option.</p>
Tenant Properties	
<i>SSL Settings</i>	
NOTE: This setting is applicable only to the SD-WAN deployment scenario.	

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Default SSL Forward Proxy Profile	<p>Click the toggle button to enable a default SSL proxy profile for the tenant.</p> <p>If you enable this option, the following items are created when a tenant is added:</p> <ul style="list-style-type: none">• 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 <p>This option is disabled by default.</p> <p>NOTE: You use this option to create a tenant-wide default profile; enabling or disabling this option does <i>not</i> mean that SSL is enabled or disabled.</p> <p>If you enable this option, you must add a root certificate.</p>

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Root Certificate	<p>You can add a root certificate (X.509 ASCII format) by importing the certificate content from a file or by pasting the certificate content:</p> <ul style="list-style-type: none"> To import the certificate content directly from a file: <ol style="list-style-type: none"> Click Browse. The File Upload dialog box appears. 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. <p>After the tenant is successfully added, a default root certificate, a default SSL proxy profile, and a default SSL proxy profile intent are created.</p> <p>NOTE:</p> <ul style="list-style-type: none"> 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 deployment scenario.

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Authentication Type	

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
	<p>Select the VPN authentication method to establish a secure IPsec tunnel:</p> <ul style="list-style-type: none"> • Preshared Key—Select this option if you want CSO to establish IPsec tunnels using keys. <p>NOTE: Preshared Key is the default VPN authentication method.</p> <ul style="list-style-type: none"> • PKI Certificate—Select this option if you want CSO to establish IPsec tunnels using public key infrastructure (PKI) certificates. Specify the following: <ul style="list-style-type: none"> • CA Server URL—Specify the Certificate Authority (CA) Server URL. For example, <code>http://CA-Server-IP-Address/certsrv/mscep/mscep.dll/pkiclient.exe</code>. 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. • Revocation List Server URL—Specify the CRL server URL. For example, <code>http://Revocation-List-Server-IP-Address/certservices/abc.crl</code>. CSO retrieves the list of revoked certificates from the CRL server. • Auto Renew—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. <p>NOTE: If the certificate is expired before the renewal, CSO might not be able to reach the device.</p> • Renew before expiry—This field appears only if you have enabled the Auto Renew toggle button.

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
	<p>Select the number of days, weeks, or months before the expiration date when the certificates get automatically renewed.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> • 3 Days • 1 Week • 2 Weeks • 1 Month <p>NOTE: The default value is 2 weeks. You can also change the duration value in the Customer Portal > Administration > Certificate Management > VPN Authentication page.</p>
Overlay Tunnel Encryption	
NOTE: This is applicable only to the SD-WAN deployment scenario.	
Encryption Type	<p>For security reasons, all data that passes through the VPN tunnel must be encrypted. Select the encryption type:</p> <ul style="list-style-type: none"> • 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. <p>The default encryption type is AES-256-GCM.</p> <p>NOTE: The MX Series routers do not support encryption types, AES-128-GCM and AES-256-GCM. The default encryption type for MX Series routers is, AES-256-CBC.</p>
Network Segmentation	
Network Segmentation	Enable network segmentation on the tenant.

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Dynamic VPN Threshold	
Note: This is applicable only to the SD-WAN deployment scenario in real-time optimized mode.	
Threshold for Creating a Tunnel	
Set a threshold value, above which a tunnel is created between two sites.	
Sessions closed	<p>Specify the maximum number of sessions closed (for a time duration of 2 minutes) between two spoke sites.</p> <p>The dynamic VPN tunnel is created between two spoke 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.</p> <p>The default threshold value (the number of sessions for 2 minutes) is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes exceeds 5.</p>
Threshold for Deleting a Tunnel	
Set a threshold value, below which a tunnel is deleted between two sites.	
Sessions closed	<p>Specify the minimum number of sessions closed (for a time duration of 15 minutes) between two spoke sites.</p> <p>The dynamic VPN tunnel is deleted between two spoke 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.</p> <p>The default threshold value (the number of sessions for 15 minutes) is 2.</p> <p>For example, if you specify the number of sessions as 2, the dynamic VPN tunnels are deleted if the number of sessions closed is lesser than or equal to 2.</p>
Maximum DVPN Tunnels	

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
Max tunnels allowed per CSO	<p>Displays the maximum number of DVPN tunnels that can be created in CSO. The total number of DVPN tunnels that can be created by all tenants in CSO is limited to 125000.</p> <p>A major alarm is raised if the number of DVPN tunnels created by all tenants reaches seventy percent of the maximum value.</p> <p>A critical alarm is raised if the number of DVPN tunnels created by all tenants reaches ninety percent of the maximum value.</p> <p>To view alarms, see Monitor > Alerts & Alarms > Alarms in the Administration Portal.</p> <p>For more information about alarms, see “About the Alarms Page” on page 317.</p>
Max tunnels allowed per tenant	<p>Specify the maximum number of DVPN tunnels that the tenant can create.</p> <p>Range: 0 through 50000.</p> <p>A major alarm is raised if the number of DVPN tunnels created by all sites in a tenant reaches seventy percent of the maximum value.</p> <p>A critical alarm is raised if the number of DVPN tunnels created by all sites in a tenant reaches ninety percent of the maximum value.</p> <p>To view alarms, see Monitor > Alerts & Alarms > Alarms in the Customer Portal.</p> <p>For more information about alarms, see <i>About the Alarms Page</i>.</p>

Table 12: Fields on the Add Tenant Page (*continued*)

Field	Description
VIM Name	<p>If you use a dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment, then select the virtualized infrastructure manager (VIM) for the tenant. A tenant can be associated with multiple VIMs.</p> <p>Example: test-vim</p>
Service Profile Name	<p>If you use a dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment, then select the service profile that specifies the authentication information for the tenant. You configure the service profile when you create the VIM.</p> <p>Example: service-profile-for-test-vim</p>
<i>Tenant-specific Attributes</i>	<p>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.</p>
Name	<p>Specify any information about the site that you want to pass to a third-party router.</p> <p>Example: Location</p>
Value	<p>Specify a value for the information about the site that you want to pass to a third-party device.</p> <p>Example: Boston</p>

RELATED DOCUMENTATION

[Tenant Overview](#) | 45

Importing Data for Multiple Tenants

IN THIS SECTION

- [Creating a Tenant Data File | 62](#)
- [Importing Tenant Data | 66](#)

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 13 on page 63](#) as a reference.
7. Save the customized tenant data file.

You can add tenants using the customized tenant data file.

Table 13: Tenant Configuration Fields

Field	Description
tenant_name	Specify the name of the tenant. You can only use alphanumeric characters and hyphens; the maximum length allowed is 15 characters. Example: tenant-a
password_expiration_radio	Specify the duration (in days) after which the password expires and must be changed.
tenant_admin	
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, or Hybrid WAN, or both)
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	

Table 13: Tenant Configuration Fields (*continued*)

Field	Description
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
<i>router_info (cloud_site_info)</i>	
router_name	Specify the router name that connects to the tenant site. This value matches the interface that you configure for the MX Series router physical network element (PNE). Example: PNE-MX10
route_target	Specify the route target of the transit network for the tenant. Example: 8888:889
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
<i>pop_info (cloud_site_info)</i>	
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

Table 13: Tenant Configuration Fields (*continued*)

Field	Description
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
<i>pop_info (data_center_site_info)</i>	
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 History of Imported Tenant Data](#) | 66

Viewing the History of Imported Tenant Data

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

To view the history of imported tenant data:

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

The Import History page is displayed. [Table 14 on page 67](#) describes the fields on the Import History page.

2. Click the task name.

The Import Tenants Task page appears. [Table 15 on page 67](#) 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 16 on page 68](#) describes the fields on the Job Status page for imported tenant data.

Table 14: 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 15: 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 16: 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](#) | 62

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 17 on page 69](#) describes the fields on the Delete History page.

2. Click the task name.

The Delete Tenants Tasks page appears. [Table 18 on page 69](#) 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 19 on page 69](#) describes the fields on the Job Status page for deleted tenant data.

Table 17: 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.
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 18: 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 19: 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.

Table 19: Fields on the Job Status Page for Deleted Tenant Data (*continued*)

Field	Description
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 | 62](#)[Viewing the History of Imported Tenant Data | 66](#)

Dynamic VPN Tunnels Overview

In releases earlier than CSO 4.1.0, all static tunnels are established between spoke sites during the Zero Touch Provisioning (ZTP) process.

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

- Between an on-premise spoke site and the corresponding enterprise hub (primary enterprise hub or secondary enterprise hub)
- Between an on-premise spoke site and the provider hub (primary provider hub or secondary provider hub)
- Between two enterprise hubs

Therefore, the communication between two on-premise spoke sites is established only through the enterprise hub or the provider hub.

CSO dynamically create or delete a VPN tunnel (without passing through an enterprise hub or a provider hub) between two spoke sites, if:

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

NOTE: The dynamic VPN feature is applicable only for SD-WAN sites in real-time optimized mode (Full mesh).

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

- The **Administration > Dynamic VPN** page of Administration portal (Global Level)

NOTE: Only the OpCo administrator can modify the default threshold value on this page.

- The Add Tenant page (Tenant-level)
- The **Administration > Dynamic VPN** page of Customer portal (Global Level)
- The Add On-Premise Spoke Site page (Site-level)
- The Add Enterprise page (Site-level)

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 VPN 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 VPN page and Add Tenant page.

NOTE: Changes that OpCo administrators make at global level do not apply to already-created tenants. The changes are applied only to tenants created after the changes have been made at the global level.

CSO allows you to manually create or delete dynamic VPN tunnels between a source site and a destination site by using Add On-Demand VPN Tunnel or Delete On-Demand VPN Tunnel pages in Customer Portal.

RELATED DOCUMENTATION

| [Configuring Dynamic VPN Tunnels Threshold for Tenants](#) | 73

Configuring Dynamic VPN Tunnels Threshold for all Tenants

CSO can dynamically create or delete a VPN tunnel (that does not pass through an enterprise hub or a provider hub) between two spoke sites , if the following conditions are met:

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

For more information on dynamic VPN tunnels, see [“Dynamic VPN Tunnels Overview” on page 71](#).

NOTE: Changes to the DVPN threshold settings are not applied to already-created tenants. Changes are applicable only to tenants that created after the settings have been modified.

To modify threshold values at the global-level (for all tenants):

1. Select **Administration > Dynamic VPN**.

The Dynamic VPN page appears.

2. Complete the configuration according to the guidelines in [Table 20 on page 74](#).

NOTE: Fields marked with * are mandatory.

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

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

The threshold values that you specify here are applicable for all tenants that you add after modifying the threshold value.

NOTE: You can also modify the threshold values while adding a tenant. The threshold value that you specify on the Add Tenant page for a specific tenant overrides the threshold value that you specified on the Dynamic VPN page of the Administration Portal at the global level (for all tenants).

Table 20: Fields on the Dynamic VPN page

Field	Description
Threshold for Creating a Tunnel	
Sessions Closed	<p>Specify the number of sessions closed (for a duration of 2 minutes) between two spoke sites.</p> <p>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 VPN tunnel is created between two spoke sites.</p> <p>The default threshold value (the number of sessions closed for 2 minutes) is 5.</p> <p>For example, if you specify the number of sessions closed as 10, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes is greater than or equal to 10.</p>
Threshold for Deleting a Tunnel	

Table 20: Fields on the Dynamic VPN page (*continued*)

Field	Description
Sessions Closed	<p>Specify the number of sessions closed (for a duration of 15 minutes) between two spoke sites.</p> <p>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 VPN tunnel is deleted between two spoke sites.</p> <p>The default threshold value (the number of sessions for 15 minutes) is 2.</p> <p>For example, if you specify the number of sessions closed as 20, dynamic VPN tunnels are deleted if the number of sessions closed between two spoke sites in 15 minutes is less than or equal to 20.</p>

RELATED DOCUMENTATION

[Dynamic VPN Tunnels Overview](#) | 71

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 21 on page 76](#).

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 21: 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	<p>If there is an update to the Terms of Use document, you can schedule a date to notify tenants about the change.</p> <p>Select the date from which the Terms of Use document is effective. The format is, YYYY-MM-DD.</p> <p>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.</p>

RELATED DOCUMENTATION

| [Accessing Administration Portal](#) | 20

5

CHAPTER

Managing Resources

- About the POPs Page | **79**
- About the Sites Page | **80**
- Manually Importing Provider Hubs with OAM Capability | **82**
- About the Tenant Devices Page | **83**
- About the Cloud Hub Devices Page | **87**
- Adding a Provider Hub Device | **90**
- Managing a Tenant Device | **94**
- Managing an EX Series Switch | **95**
- Device Redundancy Support Overview | **105**
- Viewing the History of Tenant Device Activation Logs | **108**
- Secure OAM Network Overview | **110**
- Secure OAM Network Redundancy Overview | **112**
- Rebooting Tenant Devices and Provider Hub Devices | **116**
- Identifying Connectivity Issues by Using Ping | **118**
- Identifying Connectivity Issues by Using Traceroute | **122**

[Remotely Accessing a Device CLI | 124](#)

[Device Template Overview | 126](#)

[About the Device Template Page | 132](#)

[Cloning a Device Template | 137](#)

[Importing a Device Template | 138](#)

[Configuring Template Settings in a Device Template | 140](#)

[Updating Stage-2 Configuration Template in a Device Template | 174](#)

[Configuring Stage-2 Initial Configuration in a Device Template | 178](#)

[Modifying a Device Template Description | 181](#)

[Deleting a Device Template | 181](#)

[APN Overview | 182](#)

[Configuring APN Settings on CPE Devices | 183](#)

[Device Images Overview | 187](#)

[About the Device Images Page | 187](#)

[Staging an Image | 189](#)

[Deploying Device Images to Devices | 191](#)

[Uploading a Device Image | 194](#)

[Deleting Device Images | 196](#)

[Network Services Overview | 197](#)

[About the Network Services Page | 197](#)

[About the Service Overview Page | 200](#)

[About the Service Instances Page | 202](#)

About the POPs Page

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

You can use the POPs page to view the list of available POPs in the OpCo network. You can also view information about each POP in the network.

Tasks You Can Perform

You can perform the following tasks from this page:

- 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.

Field Descriptions

[Table 22 on page 79](#) describes the fields on the POPs page.

Table 22: Fields on the POPs Page

Field	Description
Name	Name of the POP. Example: AWS
Location	Location of the POP. Example: Sunnyvale, CA

Table 22: Fields on the POPs Page *(continued)*

Field	Description
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)

About the Sites Page

IN THIS SECTION

- [Tasks You Can Perform | 81](#)
- [Field Descriptions | 81](#)

To access this page, click **Resources > Site Management > Sites**.

Use the Sites page to view or manually import provider hubs with OAM_ONLY capability, view device activation logs, view add and delete history of provider hubs, and view detailed information about each provider hub in the network.

Operating Company (OpCo) administrator can onboard provider hub devices with the DATA_ONLY capability.

The provider hub devices that are owned by the OpCo administrator are shared with the tenants within the OpCo.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add provider hub sites—See [“Manually Importing Provider Hubs with OAM Capability” on page 82](#)
- View details of a provider hub site—Hover over the site name and click the Detailed View icon or click **More > Detail View**.

The Detailed View pane appears on the right side of the sites page, displaying information about the cloud hub site. Click the close icon (X) to close the pane.

View details about a cloud hub device. See [Viewing Object Details](#)

- View device activation logs. See [“Viewing the History of Tenant Device Activation Logs” on page 108](#).
- View the jobs executed to add and delete provider hub sites. see [Viewing the Sites History](#).
- Search for a provider hub site—Click the Search icon in the top right corner of the page to search for a particular cloud hub site. 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 23 on page 81](#) describes the fields on the **Sites** page.

Table 23: Fields on the Sites Page

Field	Description
Alert Icon	Alert associated with the site. The alert can be critical (indicated by a red icon), major (indicated by an orange icon), or minor (indicated by a yellow icon). NOTE: The alert icon is displayed only if there is an alert associated with the site. If there is no alert, no icon is displayed.
Site Name	Name of the provider hub site. Click the name of the provider hub site to go to the <i>Site-Name</i> page where you can view the site details and configure parameters related to the site.
Location	Location of the provider hub site.
Operational Status	Operational status (Up or Down) of the site.
Devices	Displays the number of devices. By default, the value is always 1.

Table 23: Fields on the Sites Page (*continued*)

Field	Description
Type	Displays the site type (provider hub).
Site Status	<p>The current status of the site:</p> <ul style="list-style-type: none"> • Created—Indicates that the site is added but not configured. • Configured—Indicates that the site is configured but not activated. • Provisioned—Indicates that the site is provisioned (activated). • Upgrade-Required—Indicates that the site needs to be upgraded. • Maintenance—Indicates that the site upgrade is in progress; any deployments that might occur because of other jobs are skipped when the site status is Maintenance.
Version	Contrail Service Orchestration (CSO) version in which the provider hub site was added.

RELATED DOCUMENTATION

[Manually Importing Provider Hubs with OAM Capability](#) | 82

Manually Importing Provider Hubs with OAM Capability

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). You 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 24 on page 83](#).

NOTE: Fields marked with * are mandatory.

4. Click **OK**.

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

Table 24: 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. The provider hub devices that are listed supports only the OAM_ONLY capability.

RELATED DOCUMENTATION

[About the Sites Page](#) | 80

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:

- Quickly view activation data created for CPEs in the widgets that appear at the top of the page. See [Table 25 on page 85](#).
- View the history of tenant device activation logs. See [“Viewing the History of Tenant Device Activation Logs” on page 108](#).
- Reboot a CPE device. See [“Rebooting Tenant Devices and Provider Hub Devices” on page 116](#).

- 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 256](#).

- 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**. See *Viewing Object Details*.
- Deleting a CPE. See *Deleting Objects*.
- Show or hide columns about the CPE. See *Sorting Objects*.
- Search an object about the CPE device. See *Searching for Text in an Object Data Table*.

Field Descriptions

- [Table 25 on page 85](#) describes widgets on the Tenant Devices page.
- [Table 26 on page 85](#) describes the fields on the Tenant Devices page.

Table 25: Widgets on the Tenant Devices Page

Widget	Description
Cloud CPEs by Status	<p>Displays the management status of the CPE devices deployed in the cloud.</p> <ul style="list-style-type: none"> • Pending Activation—Number of CPE devices that are yet to connect to the regional server. • Activation Failed—Number of CPE devices that could not connect to the regional server. • Expected—Number of CPE devices that have yet to connect to the regional server. • Active—Number of CPE devices that have downloaded images, but are not yet configured. • Provisioned—Number of CPE devices on which IPsec tunnels are fully operational. • Provision Failed—Number of CPE devices failed if the vSRX was not instantiated properly.

Table 26: Fields on the Tenant Devices Page

Field	Description
Device Name	<p>Displays the name of the device.</p> <p>Example: sunny-NFX-250</p>
Tenant	<p>Displays the name of the tenant.</p> <p>Example: tenant-blue</p>
Site Name	<p>Displays the name of the tenant site.</p> <p>Example: site-blue-white</p>
Location	<p>Displays the name of the location.</p> <p>Example: San Jose, CA</p>
Status Message	<p>Displays the latest status message.</p> <p>Example: IPsec provision success</p>
WAN Links	<p>Displays the number of WAN links.</p> <p>Example: 2</p>

Table 26: Fields on the Tenant Devices Page *(continued)*

Field	Description
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. <ul style="list-style-type: none"> • 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.
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_fmfm_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](#) | 108

About the Cloud Hub Devices Page

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

Use the Cloud Hub Devices page to view the list of cloud 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 cloud hub device in the network.

CSO uses the cloud 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 Cloud Hub Devices page:

- Add a cloud hub device with DATA_ONLY capability. See [“Adding a Provider Hub Device” on page 90](#).
- View details of a cloud 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 Cloud Hub Devices page, displaying information (such as hardware and software) about the cloud hub device.

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

- Delete a cloud 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 cloud 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 cloud hub device—Click the Search icon in the top right corner of the page to search for a particular cloud 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 27 on page 88](#) describes the fields on the Cloud Hub Devices page.

Table 27: Fields on the Cloud Hub Devices Page

Field	Description
Device Name	Name of a cloud hub device. Example: srx-cloud-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 cloud hub device. Example: OAM

Table 27: Fields on the Cloud Hub Devices Page *(continued)*

Field	Description
Management Status	<p>Management status of the cloud hub devices deployed in the cloud:</p> <ul style="list-style-type: none"> • 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 cloud hub device. If the activation process is successful, then the management status changes to Provisioned. • Active—Cloud hub device is yet to be configured. • Provisioned—Cloud hub device is ready to be used. • Provision Failed—Cloud 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 cloud hub device was added.
Model	<p>Name of the device model.</p> <p>Example: MX</p>
OS Version	<p>Junos OS Release version.</p> <p>Example: 15.1X49-D40</p>
Serial Number	<p>Serial number of the device.</p> <p>Example: DD0416AA0117</p>

RELATED DOCUMENTATION

[About the Tenant Devices Page](#) | 83

Adding a Provider Hub Device

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

The device template that is currently supported for provider hub devices is SRX as SD-WAN Hub.

To add a provider hub device with DATA_ONLY capability:

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 28 on page 90](#).

4. Click **Ok**. If you want to discard your changes, click **Cancel** instead.

If you click **Ok**, the provider hub device is added. The information about the new provider hub device appears on the Provider Hub Devices page.

Table 28: Fields on the Add Provider Hub Device Page

Field	Description
Name	<p>Enter the name of the provider hub device.</p> <p>You can use alphanumeric characters, including special character(-). The maximum length is 15 characters.</p> <p>Example: MX-cloud-hub</p>
Management Region	<p>Displays the regional server with which the device communicates. The management region name is populated based on the information from the device template.</p> <p>Example: regional</p>
POP	<p>Select the POP where the hub device needs to be added.</p> <p>Example: pop_blue</p>

Table 28: Fields on the Add Provider Hub Device Page (*continued*)

Field	Description
Site Capability	<p>Select the site capability of the provider hub device as DATA_ONLY, which indicates that the hub transmits only the data traffic.</p> <p>A secure connection is established between the provider hub with data capability and the provider hub (with OAM capability) that is owned and managed by the Juniper Network team that hosts the cloud-based CSO.</p>
Authentication Type	Select the authentication method—Preshared Key (PSK) or Public Key Infrastructure (PKI).
Advanced Configuration	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on.</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
Device Template	
Device Series	Select the device series to which the provider hub belongs—vSRX or SRX.
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
Device Information	

Table 28: Fields on the Add Provider Hub Device Page (*continued*)

Field	Description
Serial Number	<p>Enter the serial number of the provider hub device.</p> <p>The serial number is a 12-digit number present on the rear panel of the device. Serial numbers are case-sensitive.</p>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the provider hub device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the provider hub device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the provider hub device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>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. .</p>
Management Connectivity	
Loopback IP Prefix	<p>By default, CSO assigns the IPv4 address prefix for the loopback interface on the device. If you prefer to use a specific loopback address contact the Juniper Networks team.</p>
WAN Links	

Table 28: Fields on the Add Provider Hub Device Page (*continued*)

Field	Description
WAN_0	Select a WAN link to enable it. After selecting the link, specify the following information: <ul style="list-style-type: none"> • WAN Interface—Displays the interface name configured in the device template. You cannot modify this field. Example: ge-0/0/0 • Link Type—Select the link type (MPLS or Internet) configured in the device template. Example: Internet • Address Assignment—Select STATIC to assign a static IP address. • Static IP Prefix—Enter a private IPv4 address from the subnet • Gateway IP Address—Enter the gateway IP address of the default route. • Data VLAN ID—(Optional) Enter the VLAN ID that is associated with the data link. A data VLAN identifier is an integer in the range 0–65,535. Example: 201
WAN_1	
WAN_2	
WAN_3	

After you add the provider hub device:

- If you have enabled the Auto Activate field, the provider hub device is automatically activated.
- If you have disabled the Auto Activate field, select the provider hub device on the **Resources > Provider Hub Devices** page and click **Activate Device**.

During activation, the provider hub device is discovered and the required details are stored in CSO.

RELATED DOCUMENTATION

[About the Cloud Hub Devices Page](#) | 87

Managing a Tenant Device

You can use the Tenant Devices page to view and manage a single customer premises equipment (CPE) device and an EX Series switch 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 stage-2 configuration template for the device.
- Deploy the stage-2 configuration template for the device.
- Rollback to the previous stage-2 configuration template for the device.
- View the deployment history of the stage-2 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.

For information about managing an EX Series switch, see [“Managing an EX Series Switch” on page 95](#).

RELATED DOCUMENTATION

Managing an EX Series Switch

IN THIS SECTION

- [Viewing the Chassis Information of an EX Series Switch](#) | 96
- [Viewing Information about an EX Series Switch](#) | 99
- [Viewing Information about Ports on an EX Series Switch](#) | 101

You can use the *Device-Name* page to view and manage an EX Series switch.

To access this page:

1. Click **Resources > Tenant Devices**.

The Tenant Devices page appears.

2. Click an EX Series switch in the Device Name column of the Devices List.

The *Device-Name* page appears.

You can perform the following actions from this page:

Viewing the Chassis Information of an EX Series Switch

The chassis view displays the device model and all the ports on an EX Series switch.

You can perform the following actions from the chassis view dashlet that appears on this page:

NOTE: The chassis view is refreshed after every 60 seconds.

- View information about ports—Hover over a port on the chassis view to view general information (such as administrative status, link status, and link mode) about the port.

See [Table 29 on page 97](#) for more details.

NOTE: The ports on the chassis view are color coded depending on the admin and link statuses:

- Green—If the admin status and link status are up.
- Red—If the admin status is up and the link status is down.
- Dark Gray—If the admin status and link status are down.
- Light Gray—If the port is not configured as part of any LAN segment.

- View additional details of a port—Click a port to view additional details of the port.

The Port Overview tab appears. [Table 34 on page 103](#) describes the fields on the Port Overview tab.

- View details of system meters—Hover over a system meter to view more information from the trays that appear. See [Table 30 on page 98](#) for more details.
- Perform various actions on an EX Series switch—Click **Actions** on the chassis view dashlet.

A list of all actions that you can perform on the switch is displayed. See [Table 31 on page 98](#) for more details.

[Table 29 on page 97](#) describes the fields on the port view pane.

Table 29: Fields on the Port View Pane

Field	Description
Admin Status	<p>Administrative status of the port:</p> <ul style="list-style-type: none"> • Green—Indicates that the admin status is up (enabled). • Gray—Indicates that the admin status is down (disabled).
Link Status	<p>Operational status of the link or connection to the port:</p> <ul style="list-style-type: none"> • Green—Indicates that the connection to the port is up. • Red—Indicates that the connection to the port is down.
Port Mode	<p>Indicates the mode in which the port operates:</p> <ul style="list-style-type: none"> • Access (default)—Only one VLAN is configured on the port. <p>Trunk and Tagged-access modes are not supported as port modes in CSO Release 5.0.2 as multiple VLAN IDs are not supported in this release.</p> <p>NOTE: The chassis view displays Trunk as the port mode only if the ports of the EX Series switch are connected to a CPE or NGFW.</p>
Link Mode	Mode in which the link to the port operates—Half-duplex or Full-duplex.
Power Consumption	Power consumed by the port, in watts (W).
PoE Status	Indicates whether the port is configured to transmit electrical power through an Ethernet cable (ON) or not (OFF).
Negotiated Speed	Current negotiated speed (in Kbps, Mbps, and Gbps) of the port.
VLAN	<p>ID of the VLAN configured on the port.</p> <p>Range: 1 through 4094.</p>
Input Bandwidth Utilization	Bandwidth (in %) consumed by the incoming packets on the port.
Output Bandwidth Utilization	Bandwidth (in %) consumed by the outgoing packets on the port.
Input Drops	Number of incoming packets dropped by the port due to congestion.
Output Drops	Number of outgoing packets dropped by the port due to congestion.
Input Errors	Number of errors in the incoming packets.
Output Errors	Number of errors in the outgoing packets.

[Table 30 on page 98](#) describes the system meters available on the chassis view dashlet. The system meters display current data.

NOTE: The UI polls the database every 30 seconds and the database polls the devices every five minutes.

Table 30: System Meters on the Chassis View Dashlet

System Meter	Description
CPU	CPU utilization (in %) in the switch.
Memory	Memory (in %) utilized in the switch.
Storage	Storage space (in %) allocated to the logical partitions of the switch.
Fan	Details of the fan used on the switch.
Temperature	Temperature details of the components in the available FPC.
LEDs	Severity level of the Alarms, System, and Primary LEDs.
Power	Details of the power supplies for the switch.

[Table 31 on page 98](#) describes the actions that you can perform on an EX Series switch.

Table 31: Options on the Actions List

Action	Description
Ping	<p>Select this option to ping a remote host to verify the connectivity between the EX Series switch and the remote host.</p> <p>See “Identifying Connectivity Issues by Using Ping” on page 118 for more information.</p>
Traceroute	<p>Select this option to execute the traceroute command from the EX Series switch, to view the path a packet travels to reach the remote host.</p> <p>See “Identifying Connectivity Issues by Using Traceroute” on page 122 for more information.</p>
Reboot Device	<p>Select this option to reboot the switch.</p> <p>See “Rebooting Tenant Devices and Provider Hub Devices” on page 116 for more information.</p>

Table 31: Options on the Actions List (*continued*)

Action	Description
View ARP Table	<p>The switch uses the ARP table to map MAC addresses to IP addresses of the ports on the switch.</p> <p>If you select this option, the View ARP Details page appears with details, such as MAC addresses, IP addresses, Interface names, and flags associated with the switch.</p>
View MAC Table	<p>The switch uses the MAC table to map MAC addresses to specific ports on the switch.</p> <p>If you select this option, the View MAC Details page appears with details, such as MAC addresses, Interface names, and flags associated with the switch.</p>

Viewing Information about an EX Series Switch

Click the **Overview** tab to view information about an EX Series switch.

You can select one of the following options as the time span to view details about the recent alarms, PoE, resource utilization, and physical box storage:

- Past 1 hour
- Past 8 hours
- Past 1 day
- Past 1 week
- Past 1 month

[Table 32 on page 99](#) describes the dashlets on the Overview tab. The graphical representations on this tab display trends based on historical data.

Table 32: Dashlets on the Overview Tab

Dashlet	Description
Port Link Status	<p>Graphical representation (Donut chart) of the link status.</p> <p>Hover over the chart to view the number and percentage of links that are up and down. You can click the chart to view all the ports on the switch, on the Port Details page.</p> <p>You can also search for a port or filter the list based on port name and link status (up or down).</p>

Table 32: Dashlets on the Overview Tab (*continued*)

Dashlet	Description
Recent Alarms	<p>Recent alarms (Critical, Major, and Minor) generated on the switch.</p> <p>Click the <i>View All Alarms</i> link to view information about all the alarms, on the Alarms page.</p> <p>See “About the Alarms Page” on page 317 for more information.</p>
Details	Details (such as serial number, management IP address, OS version, and device template) of the switch.
Resource Utilization	Graphical representation of memory and CPU utilized in the switch, for the selected time span.
Current System Users	<p>Details (such as name, duration, and login time) of the system users who are currently logged in to the switch.</p> <p>Click the <i>More Details</i> link on this dashlet to view additional information (such as username and session type) about the current users, on the View Details page.</p> <p>You can search and sort the information on this page as per your requirement, by using the Search and Filter icons, respectively.</p>
PoE	<p>Graphical representation of the power consumed by each PoE interface, in Watts (W).</p> <p>NOTE: This graph is displayed only for P models of EX Series switches.</p>
Top Ports by Input Bandwidth	Graphical representation of the top 10 ports on which the incoming packets consume the maximum bandwidth.
Top Ports by Output Bandwidth	Graphical representation of the top 10 ports on which the outgoing packets consume the maximum bandwidth.
Top Ports with Input Errors	Graphical representation of the top 10 ports with the highest number of errors in incoming packets.
Top Ports with Input Errors	Graphical representation of the top 10 ports with the highest number of errors in outgoing packets.
Top Ports with Input Packet Loss	Graphical representation of the top 10 ports that drop the highest number of incoming packets.
Top Ports with Output Packet Loss	Graphical representation of the top 10 ports that drop the highest number of outgoing packets.

Table 32: Dashlets on the Overview Tab (*continued*)

Dashlet	Description
Licenses	<p>Details of licenses (such as license name and description) installed on the switch.</p> <p>Click the <i>More Details</i> link on this dashlet to view additional information about the licenses, on the Device License Files page. .</p> <p>See “About the Device License Files Page” on page 252 for more information.</p>
Physical Box Storage	Graphical representation of the storage space (in %) allocated to the logical partitions of the switch.

Viewing Information about Ports on an EX Series Switch

Click the **Ports** tab to view information about each port on an EX Series switch.

[Table 33 on page 102](#) describes the fields on the Ports tab.

You can perform the following tasks on this tab:

- Search for a specific port by using keywords—Click the Search icon to search for a port by entering partial or full text of the keyword in the text box.
The search results are displayed on the same tab.
- Filter the data displayed on the tab—Click the Filter icon to apply a quick filter. The filtered results are displayed on the same tab.
- Show or hide columns that contain information about the ports—Click the Show or Hide Columns icon to select or clear columns that you want to display or hide on the tab.
- View additional details of a port—Click a port in the Port column to view additional details of the port, on the Port Overview tab that appears.

[Table 34 on page 103](#) describes the fields on the Port Overview tab.

Table 33: Fields on the Ports Tab

Field	Description
Interface List	
Port	<p>Name of the port.</p> <p>Click each port to view additional information about the port, on the Port Overview page.</p> <p>See Table 34 on page 103 for details of dashlets that appear on the Port Overview page.</p>
Admin Status	<p>Indicates the administrative status of the port:</p> <ul style="list-style-type: none"> • Up—if the port is enabled. • Down—If the port is disabled.
Link Status	<p>Indicates the status of the link or connection to the port:</p> <ul style="list-style-type: none"> • Up—If the connection to the port is up. • Down—If the connection to the port is down.
MTU	<p>Maximum transmission unit (MTU) size (in bytes) on the ports.</p> <p>Default: 1500 bytes.</p>
Negotiated Speed	Current negotiated speed (in Kbps, Mbps, and Gbps) of the port.
Link Mode	Mode in which the port operates—Half-duplex or Full-duplex.
Media Type	Type of transmission medium—Copper or Fiber.
Power Consumption	Power consumed by the port, in Watts (W).
VLAN ID	<p>ID of the VLAN configured on the port.</p> <p>Range: 1 through 4094.</p>
Input Bandwidth Utilization	Bandwidth (in %) consumed by the incoming packets on the port.
Output Bandwidth Utilization	Bandwidth (in %) consumed by the outgoing packets on the port.
Input Drops	Number of incoming packets dropped by the port due to congestion.
Output Drops	Number of outgoing packets dropped by the port due to congestion.

Table 33: Fields on the Ports Tab (*continued*)

Field	Description
Interface List	
Input Errors	Number of errors in the incoming packets.
Output Errors	Number of errors in the outgoing packets.
PoE (Power Over Ethernet)	Indicates whether the port is configured to transmit electrical power through an Ethernet cable (ON) or not (OFF).
Auto Negotiation	Indicates whether the interface speed is auto-negotiated (Enabled) or is fixed based on an explicitly configured value (Disabled).

Table 34 on page 103 describes the dashlets available on the Port Overview tab.

You can select one of the following options as the time span for which you want to view the graph for these dashlets:

- Past 1 hour
- Past 8 hours
- Past 1 day
- Past 1 week
- Past 1 month

NOTE: The dashlets on the Port Overview tab are refreshed after every 30 seconds. The date and time of the last refresh appear at the bottom-left corner on each dashlet.

Table 34: Dashlets on the Port Overview Tab

Dashlet	Description
Details	Details (such as port number, admin status, and link mode) of the port that you selected.
Utilization	Graphical representation of CPU utilized by the selected port (in terms of input and output) for the selected time span.

Table 34: Dashlets on the Port Overview Tab (*continued*)

Dashlet	Description
Errors	<p>Graphical representation of the number of errors in the incoming (input) and outgoing (output) packets for the selected time span.</p> <p>You can select either the past 1 hour, 8 hours, 1 day, 1 week, or 1 month as the time span for which you want to view the graph.</p>
Packet Loss	<p>Graphical representation of packet loss in incoming (input) and outgoing (output) packets for the selected time span.</p> <p>You can select either the past 1 hour, 8 hours, 1 day, 1 week, or 1 month as the time span for which you want to view the graph.</p>
Bytes	<p>Graphical representation of the MTU (in bytes) for incoming (input) and outgoing (output) packets for the selected time span.</p> <p>You can select either the past 1 hour, 8 hours, 1 day, 1 week, or 1 month as the time span for which you want to view the graph.</p>
Packets	<p>Graphical representation of the number of incoming (input) and outgoing (output) packets for the selected time span.</p> <p>You can select either the past 1 hour, 8 hours, 1 day, 1 week, or 1 month as the time span for which you want to view the graph.</p>

RELATED DOCUMENTATION

Managing a Tenant Device | 94

Device Redundancy Support Overview

Contrail Service Orchestration (CSO) supports spoke redundancy for large enterprise SD-WAN on-premise spokes. 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.

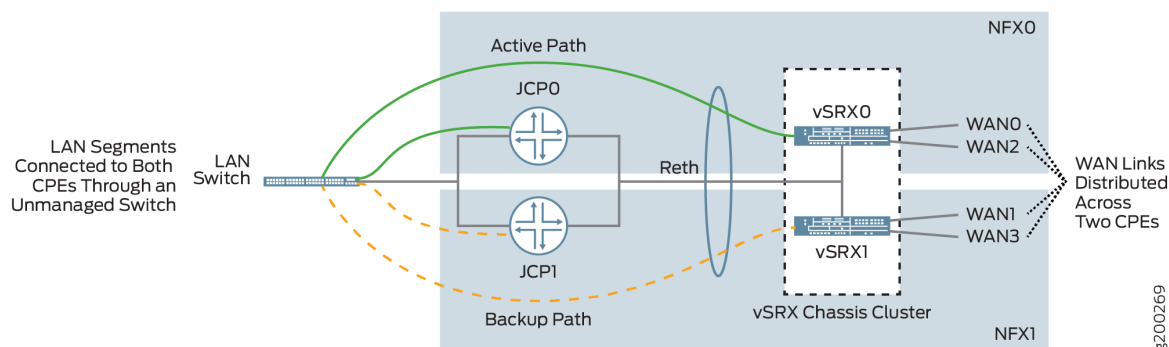
Create and Configure an SD-WAN Site

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 *Adding an On-Premise Spoke Site with SD-WAN Capability* and *Configuring a Single Site*.

Dual CPE Devices Logical Topology for NFX Network Services Platform

Figure 2 on page 106 shows the logical topology of the NFX Series dual CPE devices.

Figure 2: Dual CPE Device Topology - NFX Network Services Platform



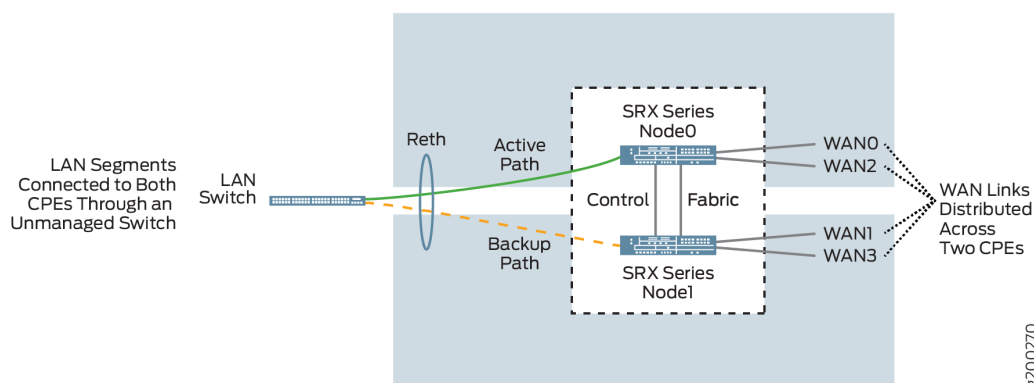
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

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 3 on page 107 shows the logical topology of the SRX Series dual CPE devices.

Figure 3: 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

Adding an On-Premise Spoke Site with SD-WAN Capability

Configuring a Single Site

Activating Dual CPE Devices (Device Redundancy)

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 35 on page 108](#) describes the fields on the Activation Logs page.

3. Click a task name.

The ZTP Logs page appears. [Table 36 on page 109](#) describes the fields on the ZTP Logs page.

4. Click the Task Name.

The Job Status page appears. [Table 37 on page 109](#) describes the fields on the Job Status page.

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

Table 35: 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 35: 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 36: 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 37: 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](#) | 83

Secure OAM Network Overview

IN THIS SECTION

- [Topology of a Secure OAM Network | 110](#)
- [Workflow for Establishing a Secure OAM Network | 111](#)
- [Benefits of Secure OAM Network | 112](#)

The management and control plane traffic between a customer premises equipment (CPE) device associated with an SD-WAN on-premise spoke 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 on-premise spoke 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.

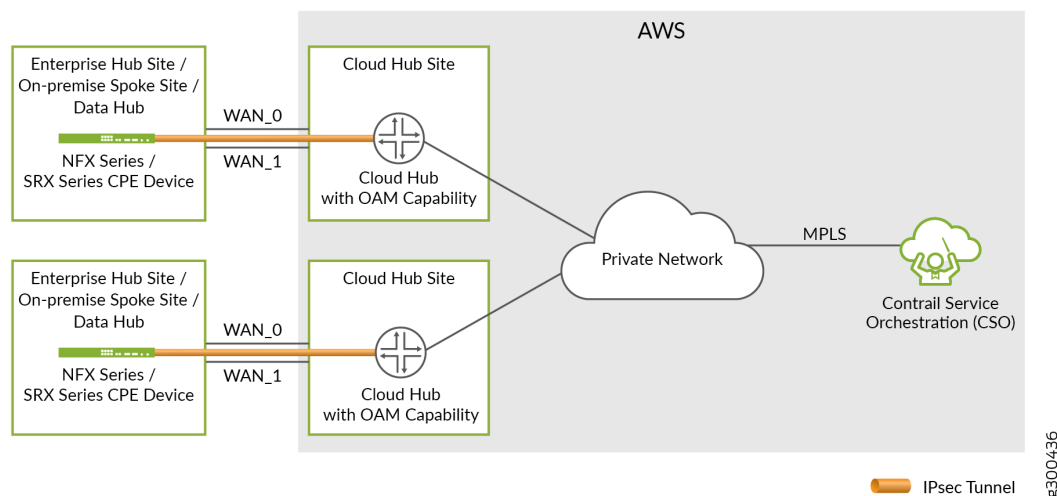
Topology of a Secure OAM Network

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 on-premise spoke sites. The provider hub device is located in the service provider's point of presence (POP). A provider hub device can be an MX Series router, 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 4 on page 111 shows the connections between the SD-WAN on-premise spoke site, provider hub, and CSO.

Figure 4: 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 on-premise spoke 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 on-premise spoke 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 on-premise spoke 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 an on-premise spoke 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 on-premise spoke 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 spoke sites, each CPE device at the site is connected to two provider hubs, and the IPsec tunnels are established from the SD-WAN on-premise spoke 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.

Secure OAM Network Redundancy Overview

IN THIS SECTION

- [Logical Topology | 113](#)
- [BGP Configuration | 114](#)
- [Adding and configuring provider hub devices | 114](#)
- [Adding and configuring an on-premise spoke site | 115](#)

- Failure Detection and Recovery | 115
- Benefits of Secure OAM Network Redundancy | 115

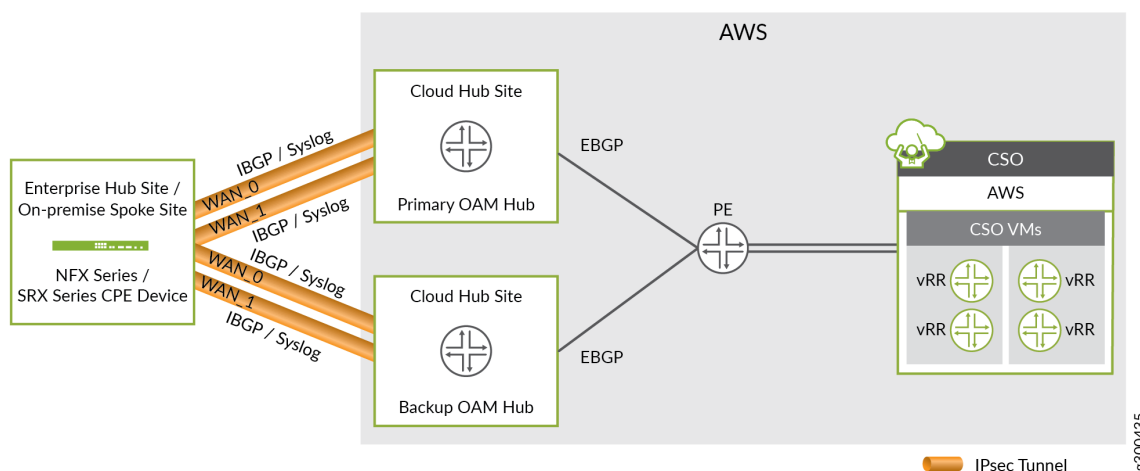
Contrail Service Orchestration (CSO) supports secure Operation, Administration, and Maintenance (OAM) network redundancy for provider hub devices in an SD-WAN deployment. You can configure two provider hub devices to act as the primary and secondary OAM hub devices and protect the site against device 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 5 on page 113 shows the topology for secure OAM network redundancy.

Figure 5: Secure OAM Network Redundancy



The CPE device at the on-premise spoke 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 on-premise spoke 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 loses 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 on-premise spoke site and the OAM hub device. During this session the OAM hub device advertises the learned CSO route to the CPE device at the on-premise spoke 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 *Adding Provider Hub Sites for SD-WAN Deployment*.

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 an on-premise spoke site

The workflow to configure an on-premise spoke site to support redundant secure OAM network is similar to adding a single on-premise spoke site. For more information about adding and configuring an on-premise spoke site, see *Adding an On-Premise Spoke 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.
- In bandwidth-optimized deployments, you must enable the **Use for OAM Traffic** option on at least one WAN link 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 propagates 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 switch 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

Rebooting Tenant Devices and Provider Hub Devices

IN THIS SECTION

- [Rebooting a Tenant Device | 116](#)
- [Rebooting a Provider Hub Device | 117](#)

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 Cloud Hub Devices Page | 87](#)

[About the Tenant Devices Page | 83](#)

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, EX switch, 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 5.0, the following devices support ping:

- EX Series: EX2300, EX3400, EX4300
- MX Series
- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, 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 38 on page 119](#).

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 39 on page 121](#).

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 38: 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 38: Fields on the Ping page (*continued*)

Field	Description
Source Interface	<p>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.</p> <p>To clear the selected interface, click Clear All and select another interface.</p>
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	<p>Click the toggle button to enable or disable (default) sending ping requests rapidly.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. <p>NOTE: The ping results are displayed in a single consolidated message instead of individual messages for each ping request packet sent.</p>
Packet Fragmentation	<p>Click the toggle button to enable or disable (default) the fragmenting of ping request packets.</p> <p>If packet fragmentation is disabled, ping packets with the maximum transmission unit (MTU) greater than 1500 bytes are dropped.</p>
Packet Size (bytes)	<p>Enter the size (in bytes) of the ping request packet.</p> <p>Default: 56 bytes.</p> <p>Range:</p> <ul style="list-style-type: none"> • 1 through 1,472 bytes, if packet fragmentation is disabled. • 1 through 65,468 bytes, if packet fragmentation is enabled.
Wait Time (seconds)	<p>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.</p> <p>Default: 10 seconds.</p> <p>Range: 0 through 600 seconds.</p>

Table 38: 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	<p>Select a specific routing instance that the ping request packets can use to reach the remote host.</p> <p>The ping result displays the information about the connectivity between the source device and the remote host based on the selected routing instance.</p> <p>To clear the selected routing instance, click Clear All and select another routing instance.</p>

Table 39: 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 μ s)	<p>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.</p> <p>Displays the following:</p> <ul style="list-style-type: none"> • 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	<p>Interface on the source device on which the responses are received for the ping requests.</p> <p>This data appears if you have enabled the Incoming Interface option on the Ping page.</p>
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, EX switch, 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 5.0, the following devices support traceroute:

- EX Series: EX2300, EX3400, EX4300
- MX Series
- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, 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 40 on page 123](#).

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 41 on page 124](#).

If the traceroute operation fails, the Traceroute Result page displays an appropriate error message (such as **No response** or **No route to host**).

Table 40: Fields on the Traceroute page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Maximum Hops	<p>Specify the maximum number of network devices that a packet can pass through to reach the remote host.</p> <p>Default: 30.</p> <p>Range: 1 through 255.</p> <p>If the number of hops to reach the remote host exceeds the set value, the traceroute packet is dropped.</p>
Advanced	
Source Interface	<p>Select a source interface on the device from which you want to send the packets to the remote host.</p> <p>Click Clear All to remove the selected interface and select another interface.</p>
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)	<p>Enter the time until which the device waits for a response from the remote host to a packet sent before considering timeout.</p> <p>Default: 10 seconds.</p> <p>Range: 0 through 86,399 seconds.</p>
Routing Instance	<p>Select a routing instance that the traceroute request packets can use to reach the remote host.</p> <p>The trace result displays the route information based on the configured routing instance type.</p> <p>To clear the selected routing instance, click Clear All and select another routing instance.</p>

[Table 41 on page 124](#) lists the parameters on the Traceroute Result page when the traceroute operation is successful.

Table 41: 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	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.
Time Taken by Packet 2	
Time Taken by Packet 3	

Remotely Accessing a Device CLI

You can use the Devices page to remotely access the CLI of a CPE device and EX Series switch, 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**.

A list of actions that you can perform on the device appears.

NOTE: For dual CPE devices, the **Remote Console** option is disabled for a parent cluster device. Only member devices can select this option to access the device CLI.

4. Select the **Remote Console** option to access the device CLI.

The Remote Terminal browser window appears, displaying the **CONNECTING TO DEVICE. PLEASE WAIT FOR PROMPT** message.

NOTE: You can automatically log in to the device through the Remote Terminal browser window, without entering a username and password. If you access the device CLI through the remote terminal, root user log in is disabled.

- If the connection is successfully established, the CLI prompt appears on the browser window. Proceed to Step 5.
 - If the connection is not established, the **Remote console connection was closed. Please close this window and open the remote console again** message appears on the browser window.
5. Enter the **show** operational command to view information about current system configuration, log files, routing tables, and so on.

The output for the show command that you entered, appears on the same browser window.

6. Close the Remote Terminal browser window to disconnect from the device.

The Devices page appears.

NOTE: The session times out if the session remains idle for more than two 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 on the browser window.

RELATED DOCUMENTATION

[About the Cloud Hub Devices Page | 87](#)

[About the Tenant Devices Page | 83](#)

Device Template Overview

IN THIS SECTION

- [Hybrid WAN CPE | 127](#)
- [SD-WAN CPE | 128](#)
- [Secure Internet CPE | 129](#)
- [Managed Internet CPE | 130](#)

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: Hybrid WAN CPE, SD-WAN CPE, Secure Internet CPE, and Managed Internet CPE.

Hybrid WAN CPE

You can use the **NFX Hybrid WAN CPE** or **SRX Hybrid WAN CPE** device template for a CPE device in hybrid WAN deployment.

Figure 6 on page 127 shows the topology for a hybrid WAN CPE deployment model.

Figure 6: Hybrid WAN CPE

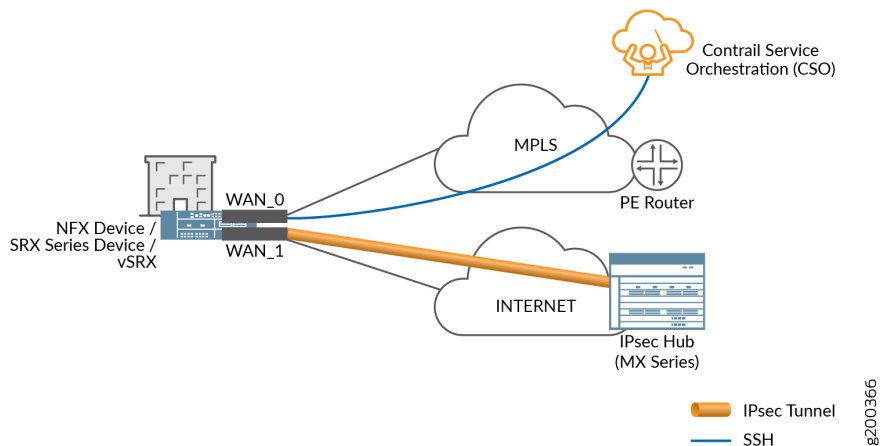


Table 42 on page 127 lists the connectivity details for hybrid WAN CPE.

Table 42: Connectivity Details for Hybrid WAN CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	MPLS	ge-1/0/1 (NFX150) ge-0/0/8 (NFX250) ge-0/0/0 (SRX)	Static	—	Data, OAM
WAN_1(Optional)	Internet	ge-1/0/2 (NFX150) ge-0/0/9 (NFX250) ge-0/0/1 (SRX)	DHCP	IPsec	Backup data path

Table 42: Connectivity Details for Hybrid WAN CPE (continued)

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_2		ge-1/0/3 (NFX150)			
WAN_3		ge-1/0/4 (NFX150)			

SD-WAN CPE

You can use the **NFX SDWAN CPE** or **SRX SDWAN CPE** device template for a CPE device in an SD-WAN deployment.

Figure 7 on page 128 shows the topology for an SD-WAN CPE deployment model.

Figure 7: SD-WAN CPE

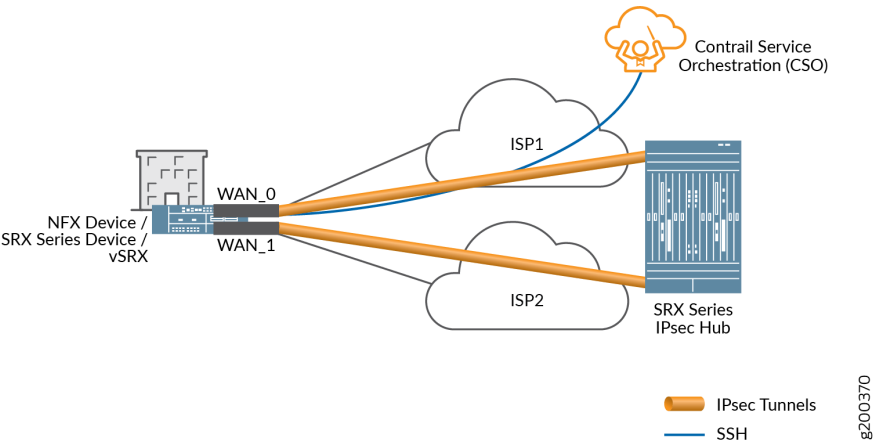


Table 43 on page 129 lists the connectivity details for an SD-WAN CPE.

Table 43: Connectivity Details for SD-WAN CPE

Link Name	Type	Default Interface	IP Assignment	Overlay	Traffic
WAN_0	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	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
WAN_2		ge-1/0/3 (NFX150) (NFX1250) ge-0/0/2 (SRX) xe-0/0/0 (SRX4x00)			
WAN_3		ge-1/0/4 (NFX150) (NFX250) ge-0/0/3 (SRX) xe-0/0/0 (SRX4x00)			

Secure Internet CPE

You can use the **NFX Secure Internet CPE** device template to provide a secure Internet connection through the CPE device.

[Figure 8 on page 130](#) shows the topology for a secure Internet CPE deployment model.

Figure 8: Secure Internet CPE

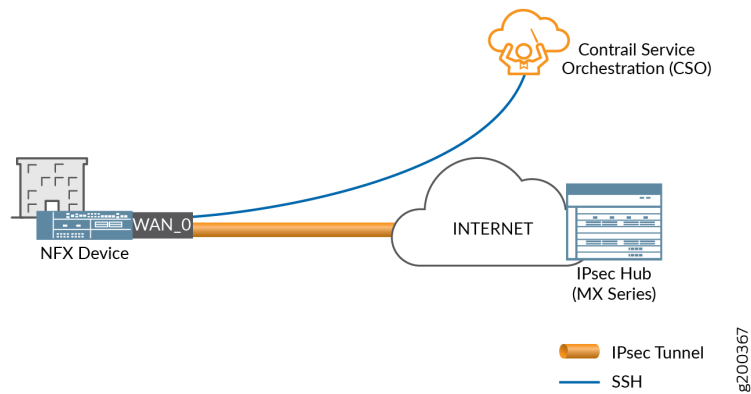


Table 44 on page 130 lists the connectivity details for secure Internet CPE.

Table 44: 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
WAN_1	—	ge-1/0/12 (NFX150)	—	—	Not Used
WAN_2		ge-1/0/3 (NFX150)			
WAN_3		ge-1/0/4 (NFX150)			

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 131 shows the topology for a managed Internet CPE deployment model.

Figure 9: Managed Internet CPE

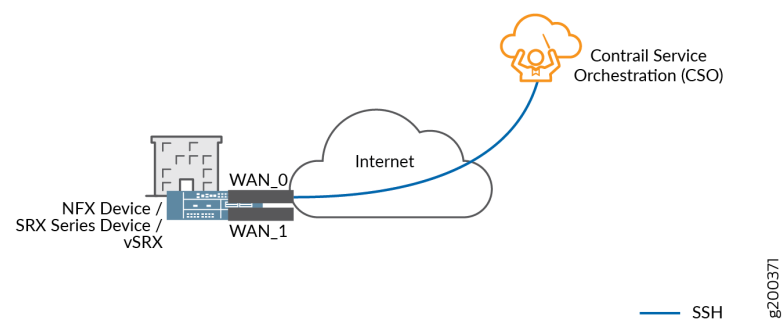


Table 45 on page 131 lists the connectivity details for a managed Internet CPE deployment model.

Table 45: 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
WAN_1	—	ge-1/0/2 (NFX150)	—	—	Not Used
WAN_2		ge-1/0/3 (NFX150)			
WAN_3		ge-1/0/4 (NFX150)			

RELATED DOCUMENTATION

About the Device Template Page | 132

About the Device Template Page

IN THIS SECTION

- [Tasks You Can Perform | 132](#)
- [Field Descriptions | 133](#)
- [Supported Device Templates | 134](#)

To access this page, click **Resources > 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 137](#).
- Import a device template from a file. See [“Importing a Device Template” on page 138](#).
- Configure device template settings. See [“Configuring Template Settings in a Device Template” on page 140](#).
- Update stage-2 configuration template. See [“Updating Stage-2 Configuration Template in a Device Template” on page 174](#).
- Configure stage-2 initial configuration. See [“Configuring Stage-2 Initial Configuration in a Device Template” on page 178](#).
- Modify a device template description. See [“Modifying a Device Template Description” on page 181](#).
- Delete a device template. See [“Deleting a Device Template” on page 181](#).
- 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 46 on page 133 describes the fields on the Device Templates page.

Table 46: Fields on the Device Templates Page

Field	Description
Name	Name of the device template
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 (<i>OpCo Name</i> 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 47 on page 134 describes the list of supported device templates.

Table 47: List of Supported Device Templates

No.	Device Template Name	Device Template Description
1	MX as SD-WAN Hub	Device template for an MX Series router acting as a hub device in an SD-WAN deployment(in hub-and-spoke topology).
2	MX as Hybrid WAN IPsec Hub	Default template for an MX Series router acting as an hub device in hybrid WAN topology. Select this option for MX Series routers in centralized and distributed deployments.
3	NFX250 as Hybrid WAN CPE	<p>Device template for an NFX250 device acting as a CPE device in a distributed deployment. This template supports port-forwarding with a CSO-initiated connection.</p> <p>This device template supports the NFX250 device as a CPE device with MPLS WAN link and optional Internet WAN link as backup</p>
4	NFX250 as Secure Internet CPE	<p>Device template for an NFX250 device acting as a CPE device in a distributed deployment. This template supports outbound SSH, which is device-initiated connection, with port-forwarding capability.</p> <p>This device template supports the NFX250 device as CPE with one Internet WAN link that has IPsec encryption(DHCP IP address configuration).</p>
5	NFX250 as Managed Internet CPE	<p>Device template for an NFX250 device acting as a CPE for a managed Internet service.</p> <p>This device template supports managed Internet Service with one Gigabit Ethernet WAN link.</p>
6	NFX250 as SD-WAN CPE	<p>Device template for an NFX250 device acting as a CPE in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>

Table 47: List of Supported Device Templates (*continued*)

No.	Device Template Name	Device Template Description
7	Dual NFX250 as SD-WAN CPEs	<p>Device template for NFX250 devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports device redundancy in SD-WAN deployment with up to four WAN links.</p>
8	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.
9	NFX150 as Hybrid WAN CPE	Device template for an NFX150 device as CPE in a distributed deployment. This device template supports port-forwarding with a CSO-initiated connection, MPLS WAN links, and optional Internet WAN link as backup.
10	NFX150 as Secure Internet CPE	Device template for an NFX150 device as CPE in a distributed deployment. This device template supports port-forwarding with device-initiated connection, one Internet WAN link with IPsec encryption (DHCP IP address configuration) and outbound SSH.
11	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.
12	SRX as Hybrid WAN CPE	Device template for an SRX Series Services Gateway or a vSRX instance acting as a CPE device in a distributed hybrid WAN deployment.
13	SRX as SD-WAN CPE	<p>Device template for an SRX Series Services Gateway acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
14	SRX as SDWAN Hub	<p>Device template for an SRX Series Services Gateway acting as a hub device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>

Table 47: List of Supported Device Templates (*continued*)

No.	Device Template Name	Device Template Description
15	Dual SRX as SD-WAN CPEs	<p>Device template for SRX Series Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
16	vSRX as SD-WAN spoke in AWS	<p>Device template for a vSRX instance acting as spoke in AWS for SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
17	SRX-4x00 as SD-WAN CPE	<p>Device template for an SRX 4000 line Services Gateways acting as a CPE device in an SD-WAN deployment with hub-and-spoke topology.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
18	Dual SRX4x00 as SD-WAN CPEs	<p>Device template for SRX 4000 line Services Gateways acting as CPE devices in device redundancy mode in an SD-WAN deployment.</p> <p>This device template supports SD-WAN deployment with up to four WAN links.</p>
19	SRX_Standalone_Pre_Staged_NonZTP	Device template for pre-staged SRX Services Gateways acting as a Standalone CPE device without ZTP.
20	SRX_Standalone_Pre_Staged_ZTP	Device template for pre-staged SRX Services Gateways acting as a Standalone CPE device with ZTP.
21	EX_Single_ZTP	Device template for EX devices acting as a single switch with ZTP.
22	EX_VC_Pre_Staged_NonZTP	Device template for pre-staged EX device acting as a virtual chassis system without ZTP.
23	EX_VC_ZTP	Device template for pre-staged EX device acting as a virtual chassis system with ZTP.

RELATED DOCUMENTATION

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 > 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.

You can also clone the device template by performing the following procedure:

1. Select **Resources > 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 | 138](#)

Importing a Device Template

IN THIS SECTION

- [Creating a Device Template File | 138](#)
- [Importing a Device Template File | 139](#)

Use the [Resources > Device Templates](#) page 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 > 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 cloud CPE 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 > 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 > Device Template**.
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 48 on page 140](#).
The configurable settings supported and default values for different device templates are as follows:

- MX Series: [Table 49 on page 147](#)
- NFX250 devices: [Table 50 on page 148](#)
- NFX150 devices: [Table 51 on page 155](#)
- SRX Series: [Table 52 on page 157](#)
- SRX4100 and SRX4200: [Table 53 on page 160](#)

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 48: Fields on the Template Settings Page for All Device Templates

Field Name	Description	Applicable To (Device Templates)
SSH Settings		

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
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
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

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
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		NFX250
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
ADSL_VPI	Enter the Virtual Path Identifier (VPI) setting to connect to the asymmetric digital subscriber line (ADSL) service provider.	NFX250

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
ADSL_ENCAP	Enter the encapsulation that is used to connect to the ADSL service provider.	NFX250
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
ADSL_VCI	Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider.	NFX250
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
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

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
GWR_VSRX_IMAGE_LOCAL_FILE_PATH	<p>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.</p> <p>For example, <code>./var/third-party/images/*vsrx*-15.1X*.qcow2</code>. 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.</p>	NFX250
GWR_VSRX_IMAGE_CNAME_IN_CSO	<p>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.</p>	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 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
OOB_MGMT_ENABLED	<p>Specify whether the out-of-band (OOB) management port of the device is being used for management connectivity or not.</p> <p>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.</p>	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 Virtual Private Network (DVPN) 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 DVPN tunnels at the tenant site after which the DVPN tunnels are dynamically deleted.	NFX150 NFX250 SRX Series
WAN_PORT_NAMES	Specify the mapping of the physical port names used for WAN side connectivity	NFX250
LAN_PORT_NAMES	Specify the mapping of the physical port names used for LAN side connectivity	NFX250

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
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 <i>do not</i> 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
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

Table 48: Fields on the Template Settings Page for All Device Templates (*continued*)

Field Name	Description	Applicable To (Device Templates)
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
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

Table 49: Configurable Settings Supported (and Their Defaults) on MX Series Device Template

Field Name	MX as SD-WAN Hub
AUTO_DEPLOY_STAGE2_CONFIG	Disabled
ZTP_ENABLED	Disabled
ACTIVATION_CODE_ENABLED	Disabled

Table 49: Configurable Settings Supported (and Their Defaults) on MX Series Device Template (continued)

Field Name	MX as SD-WAN Hub
OOB_OAM_Port	fxp0
AUTO_INSTALL_LICENSE_TO_DEVICE	Disabled
WAN Port Names	WAN_0 ge-0/0/0 WAN_1 ge-0/0/1 WAN_2 ge-0/0/2 WAN_3 ge-0/0/3

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
SSH Settings					
Prevent root login via SSH?	—	—	—	Disabled	Disabled
Restrict SSH access to be from CSO only	—	—	—	Disabled	Disabled
Max number of SSH connections allowed at any time	—	—	—	50	50
Max number of SSH connections allowed per minute	—	—	—	50	50
Max number of sessions per SSH connection	—	—	—	50	50
Policer Settings					
Bandwidth limit for ICMP traffic towards the device	—	—	—	1m	1m

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (*continued*)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
Burst-size limit for ICMP traffic towards the device	—	—	—	2k	2k
Bandwidth limit for trace-route traffic towards the device	—	—	—	1m	1m
Burst-size limit for trace-route traffic towards the device	—	—	—	15k	15k
Bandwidth limit for DHCP traffic towards the device	—	—	—	1m	1m
Burst-size limit for DHCP traffic towards the device	—	—	—	15k	15k
Bandwidth limit for DNS traffic towards the device	—	—	—	1m	1m
Burst-size limit for DNS traffic towards the device	—	—	—	15k	15k
Log Rotation Settings					
Max size (MB) for log files	—	—	—	10	10
Max number of log files	—	—	—	10	10
Customer Parameters					
S2_MODEL_HUGEPAGE_COUNT	21	21	21	13	13

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (continued)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
ADSL_VPI	—	—	—	8	8
ADSL_ENCAP	—	—	—	llcsnap-bridged-802.1q	llcsnap-802.1q
VNF_OAM_TRANSLATED_PORT_START	49152	49152	49152	49152	49152
ADSL_VCI	—	—	—	36	36
AUTO_INSTALL_LICENSE_TO_DEVICE	Disabled	Disabled	Disabled	Disabled	Disabled
AUTO_INSTALL_DEFAULT_TRUSTED_CERTS_TO_DEVICE	Enabled	Enabled	Enabled	Enabled	Enabled
USE_SINGLE_SSH_TO_NFX	Enabled	—	—	Enabled	—
ENC_ROOT_PASSWORD	juniper123	juniper123	juniper123	juniper123	juniper123
GWR_VSRX_IMAGE_CNAME_IN_CSO	vsrx-vmdisk-15.1.qcow2	vsrx-vmdisk-15.1.qcow2	vsrx-vmdisk-15.1.qcow2	vsrx-vmdisk-15.1.qcow2	vsrx-vmdisk-15.1.qcow2
ACTIVATION_CODE_ENABLED	Enabled	Enabled	Enabled	Enabled	Enabled
GWR_VSRX_IMAGE_LOCAL_FILE_PATH	—	—	—	—	—
INTERNAL_OAM_SUBNET	10.10.10.0/24	10.10.10.0/24	10.10.10.0/24	10.10.10.0/24	10.10.10.0/24
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled	Disabled	Disabled	Disabled
OOB_MGMT_ENABLED	Enabled	Enabled	Enabled	Enabled	Enabled

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (*continued*)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
S1_MODEL_HUGEPAGE_COUNT	9	9	9	9	9
CONTROL_LINK_PORT_NAME	—	—	—	—	xe-0/0
FAB_LINK_PORT_NAME	—	—	—	—	xe-0/0
MAX_DVPN_TUNNELS_ON_SITE	—	—	—	nfx250_s1e: 750 nfx250_10_t: 750 nfx250_ls1_10_t: 750 nfx250_att_s1_10_t: 300 nfx250_s2_10_t: 750 nfx250_att_ls1_10_t: 300 nfx250_att_s2_10_t: 300	nfx250_s1e: 750 nfx250_10_t: 750 nfx250_ls1_10_t: 750 nfx250_att_s1_10_t: 300 nfx250_s2_10_t: 750 nfx250_att_ls1_10_t: 300 nfx250_att_s2_10_t: 300
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE	—	—	—	nfx250_s1e: 250 nfx250_10_t: 250 nfx250_ls1_10_t: 250 nfx250_att_s1_10_t: 100 nfx250_s2_10_t: 250 nfx250_att_ls1_10_t: 100 nfx250_att_s2_10_t: 100	nfx250_s1e: 250 nfx250_10_t: 250 nfx250_ls1_10_t: 250 nfx250_att_s1_10_t: 100 nfx250_s2_10_t: 250 nfx250_att_ls1_10_t: 100 nfx250_att_s2_10_t: 100

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (*continued*)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
WAN_PORT_NAMES	WAN_0 ge-0/0/8 WAN_1 ge-0/0/9	WAN_0 ge-0/0/8	WAN_0 ge-0/0/8	WAN_0 ge-0/0/10 WAN_1 ge-0/0/11 WAN_2 xe-0/0/12 WAN_3 xe-0/0/13	WAN_0 ge-0/0/10 WAN_1 ge-0/0/11 WAN_2 xe-0/0/12 WAN_3 xe-0/0/13 WAN_4 ge-0/0/14 WAN_5 ge-0/0/15 WAN_6 ge-0/0/16 WAN_7 ge-0/0/17 WAN_8 ge-0/0/18 WAN_9 ge-0/0/19
LAN_PORT_NAMES	—	—	—	LAN_0 ge-0/0/0 LAN_1 ge-0/0/1 LAN_2 ge-0/0/2 LAN_3 ge-0/0/3 LAN_4 ge-0/0/4 LAN_5 ge-0/0/5 LAN_6 ge-0/0/6 LAN_7 ge-0/0/7 LAN_8 ge-0/0/8 LAN_9 ge-0/0/9	—

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (continued)

[illegible]

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (continued)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
GWR_CPU_PIN	nfx250_s2_10_t: 4, 10 nfx250_s1e: 4, 10 nfx250_10_t: 4,10 nfx250_ls1_10_t: 2,6 nfx250_att_s1_10_t: 4, 10 nfx250_att_ls1_10_t: 2,6 nfx250_att_s2_10_t: 4,10	nfx250_s2_10_t: 4, 10 nfx250_s1e: 4, 10 nfx250_10_t: 4,10 nfx250_ls1_10_t: 2,6 nfx250_att_s1_10_t: 4, 10 nfx250_att_ls1_10_t: 2,6 nfx250_att_s2_10_t: 4,10	nfx250_s2_10_t: 4, 10 nfx250_s1e: 4, 10 nfx250_10_t: 4,10 nfx250_ls1_10_t: 2,6 nfx250_att_s1_10_t: 4, 10 nfx250_att_ls1_10_t: 2,6 nfx250_att_s2_10_t: 4,10	nfx250_s2_10_t: 4, 10 nfx250_s1e: 4, 10 nfx250_10_t: 4,10 nfx250_ls1_10_t: 2,6 nfx250_att_s1_10_t: 4, 10 nfx250_att_ls1_10_t: 2,6 nfx250_att_s2_10_t: 4,10	nfx250_s2_10_t: 4, 10 nfx250_s1e: 4, 10 nfx250_10_t: 4,10 nfx250_ls1_10_t: 2,6 nfx250_att_s1_10_t: 4, 10 nfx250_att_ls1_10_t: 2,6 nfx250_att_s2_10_t: 4,10
AUX_Subnets	AUX_0 10.10.0.0/24 AUX_1 10.10.12.0/24 AUX_2 10.10.13.0/24	AUX_0 10.10.0.0/24 AUX_1 10.10.12.0/24 AUX_2 10.10.13.0/24	AUX_0 10.10.0.0/24 AUX_1 10.10.12.0/24 AUX_2 10.10.13.0/24	AUX_0 10.10.0.0/24 AUX_1 10.10.12.0/24 AUX_2 10.10.13.0/24	AUX_0 10.10.0.0/24 AUX_1 10.10.12.0/24 AUX_2 10.10.13.0/24
LAN_Subnets	LAN_0 10.10.1.0/24 LAN_1 10.10.2.0/24	LAN_0 10.10.1.0/24 LAN_1 10.10.2.0/24	LAN_0 10.10.1.0/24 LAN_1 10.10.2.0/24	LAN_0 10.10.1.0/24 LAN_1 10.10.2.0/24	LAN_0 10.10.1.0/24 LAN_1 10.10.2.0/24
Login Security Settings					
Login idle timeout (minutes)	—	—	—	10	10
Login attempts before locking out	—	—	—	3	3
Login lockout period in minutes	—	—	—	5	5

Table 50: Configurable Settings Supported (and Their Defaults) on NFX250 Device Templates (*continued*)

Field Name	NFX250 as Hybrid WAN CPE	NFX250 as Managed Internet CPE	NFX250 as Secure Internet CPE	NFX250 as SD-WAN CPE	Dual NFX250 as SD-WAN CPE
Login backoff factor in seconds	—	—	—	5	5
Login backoff threshold	—	—	—	2	2
Maximum time to enter password in seconds	—	—	—	20	20
Maintenance user account	—	—	—	juniper	juniper
Login Announcement	—	—	—	This system is private property.	This system is private property.
Login Message	—	—	—	Unauthorized access will be reported.	Unauthorized access will be reported.

Table 51: Configurable Settings Supported on NFX150 Device Templates

Field Name	NFX150 as Hybrid WAN CPE	NFX150 as Managed Internet CPE	NFX150 as Secure Internet CPE	NFX150 as SD-WAN CPE
VNF_OAM_TRANSLATED_PORT_START	49152	49152	49152	49152
AUTO_INSTALL_LICENSE_TO_DEVICE	Disabled	Disabled	Disabled	Disabled
ZTP_ENABLED	Enabled	Enabled	Enabled	Enabled
INTERNAL_OAM_SUBNET	10.10.10.0/24	10.10.10.0/24	10.10.10.0/24	10.10.10.0/24
ENC_ROOT_PASSWORD	Specified	Specified	Specified	Specified
ACTIVATION_CODE_ENABLED	Enabled	Enabled	Enabled	Enabled
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled	Disabled	Disabled
USE_SINGLE_SSH_TO_NFX	Enabled	—	—	Enabled

Table 51: Configurable Settings Supported on NFX150 Device Templates (continued)

Field Name	NFX150 as Hybrid WAN CPE	NFX150 as Managed Internet CPE	NFX150 as Secure Internet CPE	NFX150 as SD-WAN CPE
ADSL_VPI	—	—	—	8
ADSL_ENCAP	—	—	—	llcsnap-bridged-802.1q
ADSL_VCI	—	—	—	36
MAX_DVPN_TUNNELS_ON_SITE	—	—	—	300
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE	—	—	—	100
WAN Port Names for SKU with single slot	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-0-2 WAN_3 ge-1/0/4 heth-0-3	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-0-2 WAN_3 ge-1/0/4 heth-0-3	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-0-2 WAN_3 ge-1/0/4 heth-0-3	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-0-2 WAN_3 ge-1/0/4 heth-0-3
WAN Port Names for SKU with EM-6T2SFP expansion module.	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-1-6 WAN_3 ge-1/0/4 heth-1-7	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-1-6 WAN_3 ge-1/0/4 heth-1-7	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-1-6 WAN_3 ge-1/0/4 heth-1-7	WAN_0 ge-1/0/1 heth-0-4 WAN_1 ge-1/0/2 heth-0-5 WAN_2 ge-1/0/3 heth-1-6 WAN_3 ge-1/0/4 heth-1-7

Table 52: Configurable Settings Supported on SRX Series Device Templates

Field Name	SRX as Managed Internet CPE	SRX as Hybrid WAN CPE	SRX as SD-WAN CPE	SRX as SD-WAN Hub	Dual SRX as SD-WAN CPEs	vSRX as SD-WAN spoke AV
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
ZTP_ENABLED	Enabled	Disabled	Enabled	Enabled	Disabled	—
PRE-STAGED-CPE	Disabled	—	—	—	—	—
ACTIVATION_CODE_ENABLED	Disabled	Disabled	Enabled	Enabled	Disabled	—
OOB_OAM_Port	fxp0	fxp0	fxp0	fxp0	ge-0/0/0	—
ENC_ROOT_PASSWORD	Specified	Specified	Specified	Specified	Specified	Sp
AUTO_INSTALL_LICENSE_TO_DEVICE	Disabled	Disabled	Disabled	Disabled	Disabled	Dis
CLUSTER_OFFSET	—	—	—	—	5	—
MAX_DVPN_TUNNELS_ON_SITE	—	—	300	—	300	30
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE	—	—	100	—	100	10
LTE_SETTINGS						
MINI_PIM_SLOT	—	—	1	—	—	—
NOTE: If you have powered on an SRX Series services gateway device with the LTE Mini-PIM installed in slot 1 (default), the dialer interface is triggered to dial automatically. If you have installed the Mini-PIM in any other slot and want the phone-home process to be triggered through the LTE interface, you must configure the cl and dl interfaces that are required to reach the redirect server.						

Table 52: Configurable Settings Supported on SRX Series Device Templates (continued)

Field Name	SRX as Managed Internet CPE	SRX as Hybrid WAN CPE	SRX as SD-WAN CPE	SRX as SD-WAN Hub	Dual SRX as SD-WAN CPEs	vS SD sp AW
WAN Port Names	WAN_0 ge-0/0/0	WAN_0 ge-0/0/0 WAN_1 ge-0/0/1	WAN_0 ge-0/0/0 WAN_1 ge-0/0/1 WAN_2 ge-0/0/2 WAN_3 ge-0/0/3	WAN_0 ge-0/0/0 WAN_1 ge-0/0/1 WAN_2 ge-0/0/2 WAN_3 ge-0/0/3	WAN_0 ge-0/0/3 WAN_1 ge-{ {CLUSTER_ OFFSET.value}}/0/3 WAN_2 ge-0/0/4 WAN_3 ge-{ {CLUSTER_ OFFSET.value}}/0/4	W ge W ge
OAM CE Port Names	—	—	—	OAM_CE_0 ge-0/0/0 OAM_CE_1 ge-0/0/1 OAM_CE_2 ge-0/0/2 OAM_CE_3 ge-0/0/3	—	—
FAB Port Names	—	—	—	—	FAB_0 ge-0/0/2 FAB_1 ge-{ {CLUSTER_ OFFSET.value}}/0/2	—

Table 52: Configurable Settings Supported on SRX Series Device Templates (continued)

Field Name	SRX as Managed Internet CPE	SRX as Hybrid WAN CPE	SRX as SD-WAN CPE	SRX as SD-WAN Hub	Dual SRX as SD-WAN CPEs	vSRX as SD-WAN spoke AV
LAN Port Names	—	—	LAN_0 ge-0/0/0 LAN_1 ge-0/0/1 LAN_2 ge-0/0/2 LAN_3 ge-0/0/3 LAN_4 ge-0/0/4 LAN_5 ge-0/0/5 LAN_6 ge-0/0/6 LAN_7 ge-0/0/7 LAN_8 ge-0/0/8 LAN_9 ge-0/0/9 LAN_10 ge-0/0/10	—	LAN_0_0 ge-0/0/7 LAN_0_1 ge-0/0/8 LAN_0_2 ge-0/0/9 LAN_0_3 ge-0/0/10	LAN_0_0 ge-0/0/7 LAN_0_1 ge-0/0/8 LAN_0_2 ge-0/0/9 LAN_0_3 ge-0/0/10
RESERVED_MEMBER_PORT_NAMES	—	—	—	—	PORT_0_0 ge-0/0/5 PORT_0_1 ge-0/0/6	—
RESERVED_SUBNETS	—	—	—	—	NODE_0 10.10.12.0/24 NODE_1 10.10.13.0/24	—

Table 52: Configurable Settings Supported on SRX Series Device Templates (continued)

Field Name	SRX as Managed Internet CPE	SRX as Hybrid WAN CPE	SRX as SD-WAN CPE	SRX as SD-WAN Hub	Dual SRX as SD-WAN CPEs	vS SD sp AW
AUTO_INSTALL_DEFAULT _TRUSTED_CERTS_ TO_DEVICE	—	—	—	—	—	En
AMI_vSRX_BYOL	—	—	—	—	—	Sp

Table 53: Configurable Settings Supported on SRX4x00 Series Device Templates

Field Name	SRX-4x00 as SD-WAN CPE	Dual SRX4x00 as SD-WAN CPEs
SSH Settings		
Prevent root login via SSH?	Disabled	Disabled
Restrict SSH access to be from CSO only	Disabled	Disabled
Max number of SSH connections allowed at any time	50	50
Max number of SSH connections allowed per minute	50	50
Max number of sessions per SSH connection	50	50
Policer Settings		
Bandwidth limit for ICMP traffic towards the device	1m	1m
Burst-size limit for ICMP traffic towards the device	2k	2k
Bandwidth limit for trace-route traffic towards the device	1m	1m
Burst-size limit for trace-route traffic towards the device	15k	15k
Bandwidth limit for DHCP traffic towards the device	1m	1m
Burst-size limit for DHCP traffic towards the device	15k	15k

Table 53: Configurable Settings Supported on SRX4x00 Series Device Templates (continued)

Field Name	SRX-4x00 as SD-WAN CPE	Dual SRX4x00 as SD-WAN CPEs
Bandwidth limit for DNS traffic towards the device	1m	1m
Burst-size limit for DNS traffic towards the device	15k	15k
Log Rotation Settings		
Max size (MB) for log files	10	10
Max number of log files	10	10
Feature Level Access Settings		
Allow TACACS access	Disabled	Disabled
Allow SNMP Access	Disabled	Disabled
Customer Parameters		
AUTO_INSTALL_LICENSE_TO_DEVICE	Disabled	—
AUTO_INSTALL_DEFAULT_TRUSTED_CERTS_TO_DEVICE	Enabled	Enabled
ZTP_ENABLED	Disabled	Disabled
ENC_ROOT_PASSWORD	Specified	Specified
ACTIVATION_CODE_ENABLED	Disabled	Disabled
CLUSTER_OFFSET	—	7
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled
OOB_OAM_PORT	fxp0	fxp0
MAX_DVPN_TUNNELS_ON_SITE		
default-value	1500	1500
WAN_PORT_NAMES		

Table 53: Configurable Settings Supported on SRX4x00 Series Device Templates (*continued*)

Field Name	SRX-4x00 as SD-WAN CPE	Dual SRX4x00 as SD-WAN CPEs
WAN_0	xe-0/0/0	xe-0/0/0
WAN_1	xe-0/0/1	xe-{{CLUSTER_OFFSET.value}}/0/0
WAN_2	xe-0/0/2	xe-0/0/1
WAN_3	xe-0/0/3	xe-{{CLUSTER_OFFSET.value}}/0/1
MIN_DVPN_TUNNELS_TO_START_DEACTIVATE		
default-value	500	500
LAN_PORT_NAMES		
LAN_0	xe-0/0/0	LAN_0_0— xe-0/0/2
LAN_1	xe-0/0/1	LAN_0_1— xe-0/0/3
LAN_2	xe-0/0/2	LAN_0_2— xe-0/0/4
LAN_3	xe-0/0/3	LAN_0_3— xe-0/0/5
LAN_4	xe-0/0/4	
LAN_5	xe-0/0/5	
LAN_6	xe-0/0/6	
LAN_7	xe-0/0/7	
Login Security Settings		
Idle timeout (minutes)	10	10
Attempts before locking out	3	3
Lockout period in minutes	5	5
Backoff factor in seconds	5	5
Backoff threshold	2	2

Table 53: Configurable Settings Supported on SRX4x00 Series Device Templates *(continued)*

Field Name	SRX-4x00 as SD-WAN CPE	Dual SRX4x00 as SD-WAN CPEs
Maximum time to enter password in seconds	20	20
Maintenance user account	juniper	juniper
Announcement	This system is private property.	This system is private property.
Message	Unauthorized access will be reported.	Unauthorized access will be reported.
RESERVED_MEMBER_PORT_NAMES		
PORT_0_1	—	xe-0/0/7
PORT_0_0	—	xe-0/0/6
RESERVED_SUBNETS		
NODE_1	—	10.10.13.0/24
NODE_0	—	10.10.12.0/24

Table 54: 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

Table 54: Fields on the Template Settings Page (continued)

Name	Description
ZTP_ENABLED	<p>Specify whether to enable ZTP for the device.</p> <p>NOTE: This option is supported on SRX Series Services Gateways only.</p> <p>Example: Enabled</p>
PRE_STAGED_CPE	<p>Specify whether the CPE device is pre-staged with WAN configuration.</p> <p>NOTE: This option is supported on SRX Series Services Gateways only.</p> <p>Example: Enabled</p>
ACTIVATION_CODE_ENABLED	<p>Specify whether the customer must use an activation code to activate the CPE device.</p> <p>Example: Enabled</p>
OOB_OAM_Port	<p>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.</p> <p>NOTE: This option is supported on SRX Series Services Gateways only.</p> <p>Example: fxp0</p>
S2_MODEL_HUGEPAGE_COUNT	<p>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.</p> <p>Example: 21</p>
USE_SINGLE_SSH_TO_NFX	<p>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.</p> <p>Example: Enabled</p>

Table 54: Fields on the Template Settings Page (continued)

Name	Description
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.
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

Table 54: Fields on the Template Settings Page (continued)

Name	Description
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.
GWR_VSRX_IMAGE_LOCAL_FILE_PATH	<p>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.</p> <p>Example: <code>./var/third-party/images/*vsrx*-15.1X*.qcow2</code></p>
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	<p>Enter the Virtual Path Identifier (VPI) setting to connect to the ADSL service provider through PPPoE.</p> <p>Example: 8</p>
ADSL_ENCAP	<p>Enter the encapsulation that is used to connect to the ADSL service provider through PPPoE.</p> <p>Example: <code>llcsnap-bridged-802.1q</code></p>
ADSL_VCI	<p>Enter the VCI (Virtual Channel Identifier) setting to connect to the ADSL service provider through PPPoE.</p> <p>Example: 36</p>

Table 54: Fields on the Template Settings Page (*continued*)

Name	Description
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
CLUSTER_OFFSET	Enter the cluster slot number for designated secondary node.

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 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

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)

Field Name	Description
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
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

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)

Field Name	Description
Log Rotation Settings	
Max size (MB) for log files	Enter the maximum size of the log file, in megabytes (MB). Default: 10
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	
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
ZTP_ENABLED	Specify whether to enable ZTP for the device.
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

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)

Field Name	Description
CLUSTER_OFFSET	Enter the cluster slot number for designated secondary node.
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 Virtual Private Network (DVPN) 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 DVPN tunnels that must be present at a site to start deactivating the inactive site-to-site tunnels.
WAN_PORT_NAMES	Enter the name of the physical interfaces for the ports that are used for WAN side connectivity. WAN_0 WAN_1 WAN_2 WAN_3

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)

Field Name	Description
WAN_MEMBER_PORT_NAMES	<p>In case of dual-CPE devices, enter the name of the physical interfaces for the ports that are used for WAN side connectivity.</p> <p>WAN_0</p> <p>WAN_1</p> <p>WAN_2</p> <p>WAN_3</p>
LAN_PORT_NAMES	<p>Enter the name of the physical interfaces for the ports that are used to connect to LAN side devices.</p> <p>LAN_0— xe-0/0/0</p> <p>LAN_1— xe-0/0/1</p> <p>LAN_2— xe-0/0/2</p> <p>LAN_3— xe-0/0/3</p> <p>LAN_4— xe-0/0/4</p> <p>LAN_5— xe-0/0/5</p> <p>LAN_6— xe-0/0/6</p> <p>LAN_7— xe-0/0/7</p>
LAN_MEMBER_PORT_NAMES	<p>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..</p> <p>LAN_0_0— xe-0/0/2</p> <p>LAN_0_1— xe-0/0/3</p> <p>LAN_0_2— xe-0/0/4</p> <p>LAN_0_3— xe-0/0/5</p>
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.

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)

Field Name	Description
Attempts before locking out	<p>Enter the maximum number of unsuccessful login attempts allowed before the account is locked.</p> <p>Range: 3 to 10</p>
Lockout period in minutes	<p>Enter the number of minutes an account must remain locked after the maximum number of unsuccessful login attempts.</p> <p>Range: 1 to 43,200</p>
Backoff factor in seconds	<p>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.</p> <p>Range: 5 to 10</p>
Backoff threshold	<p>Enter the threshold for the number of failed login attempts before the user experiences a delay when attempting to reenter a password.</p> <p>Range: 1 to 3</p>
Maximum time to enter password in seconds	<p>Enter the maximum time allowed (in seconds) to enter a password to log in to the device after entering your username.</p> <p>Range: 20 to 300.</p>
Maintenance user account	<p>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.</p>
Announcement	<p>Enter the system login announcement, which is displayed after a user successfully logs in to the device.</p>
Message	<p>Enter the system login message, which is displayed when a user logs into the device.</p>

Table 55: Fields on the Template Settings Page for SRX4100 and SRX4200 Device Templates (*continued*)


Field Name	Description
RESERVED_MEMBER_PORT_NAMES	<p>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.</p> <ul style="list-style-type: none"> • PORT_0_0— xe-0/0/6 • PORT_0_1— xe-0/0/7
RESERVED_SUBNETS	<p>Enter the IP address of reserved subnets that is used for System logs.</p> <ul style="list-style-type: none"> • NODE_0— 10.10.12.0/24 • NODE_1— 10.10.13.0/24

RELATED DOCUMENTATION

| [About the Device Template Page](#) | 132

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 > 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 56 on page 174](#) 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 57 on page 175](#).

4. Click **Save**.

The new stage-2 configuration template is included in the device template.

Table 56: Fields on the Stage-2 Configuration Templates Page

Name	Description
Name	View the name of the stage-2 configuration template. Example: LAN side config

Table 56: Fields on the Stage-2 Configuration Templates Page (*continued*)

Name	Description
Component Name	<p>View the name of the component through which the settings are configured. The components that are currently supported are:</p> <ul style="list-style-type: none"> • 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. <p>Example: JUNOS</p>
Hide	<p>Displays whether the template is hidden on Customer Portal.</p> <ul style="list-style-type: none"> • true—Template is not visible on Customer Portal. • false—Template is visible on Customer Portal. <p>Example: false</p>
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.
Enable for	Displays whether the stage-2 configuration template is enabled for all tenants, no tenants, or specific tenants.

Table 57: Fields on the Add New Template Page

Name	Description
Template	<p>Select the configuration template from the drop-down list. The configuration templates are designed in the Configuration Designer tool.</p> <p>Example: srx-basic-sdwan-cpe-config</p>

Table 57: Fields on the Add New Template Page (*continued*)

Name	Description
Display Name	<p>Specify the name of the template that you want to display on the configuration interface.</p> <p>Example: SDWAN Config</p>
Component Name	<p>Specify the component name through which the settings are configured. The components that are currently supported are:</p> <ul style="list-style-type: none"> • 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. <p>Example: JUNOS</p>
Hide	<p>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.</p> <ul style="list-style-type: none"> • hide—White dot on right with blue background. • show—White dot on left with gray background. <p>Example: hide</p>
Copy From Template	<p>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.</p> <p>Example: srx-mis-lan-to-wan-config</p>
Auto Deploy	<p>Specify whether the stage-2 configuration must be automatically pushed to the device during ZTP process. The available options are</p> <ul style="list-style-type: none"> • Same as global settings • Yes • No

Table 57: Fields on the Add New Template Page (*continued*)

Name	Description
Enabled for	<p>You can enable the stage-2 configuration template for all tenants, specific tenants, an SP administrator or an OpCo administrator.</p> <p>NOTE: Only users with SP administrator or OpCo administrator role can enable stage-2 configuration templates.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • 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. <p>When you select the Selective Tenants option, the Tenants section is displayed.</p> <p>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.</p> <p>The default option is All Tenants.</p>

To remove a stage-2 configuration template:

1. Select **Resources > 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 > 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 58 on page 179](#), [Table 59 on page 179](#), and [Table 60 on page 179](#) and [Table 61 on page 180](#).

4. Click **Ok**.

Table 58: 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
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 59: 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 60: 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

Table 60: Fields for the SRX Basic SD-WAN Settings on the Stage-2 Initial Configuration Page *(continued)*

Field	Description
Application SLA Profile	Specify the application SLA profile for the rule. Example: critical-apps

Table 61: 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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](#) | 132

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](#) | 132

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 > 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 | 132](#)

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 | 184](#)
- [Configuring APN Settings without SIM Change on CPE Devices | 186](#)

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 > 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 62 on page 185](#).

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 62: 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. <ul style="list-style-type: none"> • 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: <p>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.</p> <ul style="list-style-type: none"> • (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.
Authentication Method	Select the authentication method for the APN configuration: <ul style="list-style-type: none"> • (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 .

Table 62: Fields for the APN Configuration Settings on the Stage-2 Initial Configuration Page (*continued*)

Field	Description
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 > 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 62 on page 185](#).

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 Series, MX Series, 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](#) | 187

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 187](#).

Tasks You Can Perform

You can perform the following tasks from this page:

- Stage device images. See [“Staging an Image” on page 189](#)
- Deploy device images. See [“Deploying Device Images to Devices” on page 191](#).
- 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**. See *Viewing Object Details*.
- Show or hide columns that contain information about the device image. See *Sorting Objects*.
- Search an object for a device image. See *Searching for Text in an Object Data Table*.

Field Descriptions

[Table 63 on page 188](#) shows the fields on the Device Images page.

Table 63: 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
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

RELATED DOCUMENTATION

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 64 on page 189](#) 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 64: 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

Table 64: Fields on the Deploy Image: Select Devices Page (continued)

Field	Description
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
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. <ul style="list-style-type: none"> ● 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.

Table 64: Fields on the Deploy Image: Select Devices Page (continued)

Field	Description
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 | 187](#)
- [Deploying Device Images to Devices | 191](#)

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 64 on page 189](#) 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 65: 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
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. <ul style="list-style-type: none"> ● 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

Table 65: Fields on the Deploy Image: Select Devices Page (continued)

Field	Description
Stage Image	<p>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.</p> <p>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.</p> <p>If you disable the Stage Image option without manually staging the image onto the device, the deploy operation fails.</p>
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 | 187](#)
[Staging an Image | 189](#)

Uploading a Device Image

On the Images page, you can upload image files for CPE and VNF devices that you use in a distributed, centralized, or combined deployment from the Images page. 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 66 on page 195](#).

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 66: Fields on the Upload Device Image Page

Field	Description
Name	<p>Specify the filename for the device image that you are uploading.</p> <p>Example: juniper_nfx_250_v1_img.tgz</p> <p>You must use the following filename format for device images of VNFs as listed below:</p> <ul style="list-style-type: none"> • Riverbed—riverbed-img • vSRX—vsrx-vmdisk-15.1.qcow2 • NFX—juniper_nfx_1.5_img.tgz
Image Type	<p>Specify the type of device image.</p> <ul style="list-style-type: none"> • 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. <p>Yes</p> <ul style="list-style-type: none"> • 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.
File Location	Click Browse to navigate to the file location in your local system and select an image file to upload.
Vendor	<p>Specify the vendor name of the device.</p> <p>Example: Juniper Networks.</p>
Family	<p>Specify the name of the device family.</p> <p>Example: NFX</p>

Table 66: Fields on the Upload Device Image Page (continued)

Field	Description
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 | 187](#)
- [About the Device Images Page | 187](#)

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](#) | 187

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](#) | 197

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 197.

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 67 on page 198](#).
- 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 202](#).

Field Descriptions

[Table 67 on page 198](#) shows the descriptions of the widgets that appear at the top of the Services page.

Table 67: Widgets on the Services Page

Widget	Description
Top Network Services Used	<p>View the numbers of instances of the three services that are most used by tenants in the network.</p> <p>This view might help you to identify trends for network services, especially when you introduce a new service.</p>
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 68 on page 198](#) shows the descriptions of the fields on the Network Services page.

Table 68: Fields on the Services Page

Field	Description
Name	<p>View the name of the network service.</p> <p>Click the name to view full information about a service.</p>

Table 68: Fields on the Services Page (*continued*)

Field	Description
Tenants	<p>View the number of tenants and the names of the tenants that have access to this network service.</p> <ul style="list-style-type: none"> • 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 69 on page 199 shows the descriptions of the fields on the Detail for *Service-Name* page.

Table 69: Fields on the Service Detail Page

Field	Description
<i>General Information</i>	
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	<p>View the status of the network service.</p> <p>Example: Published</p>
Performance Goals	View performance of the network service which include bandwidth, number of sessions, and latency.

RELATED DOCUMENTATION

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 70 on page 200](#).
 - View resources required for the service and its performance specification. See *Service Requirements* and *Service Performance* in [Table 70 on page 200](#).
 - View the service chain, with its constituent VNFs. See *Service Configuration* in [Table 70 on page 200](#).

Field Descriptions

[Table 70 on page 200](#) provides guidelines on using the fields on the Service Overview page.

Table 70: Fields on the Service Overview Page

Field	Description
<i>General Information</i>	
Description	View a summary about the service’s capabilities. The network service designer provides this summary.

Table 70: Fields on the Service Overview Page (*continued*)

Field	Description
State	View the state of the network service: <ul style="list-style-type: none"> • 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.
<i>Service Requirements</i>	
CPU	View the number of CPUs that the service needs (cores).
Memory	View the amount of RAM that the service needs in gigabytes (GB).
<i>Service Performance</i>	
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.
<i>Service Configuration (graphic of the service chain)</i>	
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	<p>Click to view settings for the VNF.</p> <p>The service designer can configure the VNF settings in Network Service Designer and the administrative user can configure the VNF settings in Customer Portal.</p> <p>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.</p>

RELATED DOCUMENTATION

| [About the Network Services Page](#) | 197

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 72 on page 203](#).
- 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 or VNF in a centralized deployment. By default, automatic recovery of a network service or VNFs is enabled.

Field Descriptions

[Table 71 on page 202](#) shows the descriptions of the fields on the Service Instances page.

Table 71: 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: <ul style="list-style-type: none"> • 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 71: 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 72 on page 203 shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

Table 72: Fields on the Service Instance Details Page

Field	Description
<i>General</i>	
Description	View information about this service instance. This information is generated from data in Customer Portal.

RELATED DOCUMENTATION

[Network Services Overview](#) | 197

[About the Network Services Page](#) | 197



Managing Signatures

[Signature Database Overview | 205](#)

[About the Signature Database Page | 205](#)

[Downloading a Signature Database | 207](#)

[Download Locations for Signature Database | 209](#)

[Application Signatures Overview | 210](#)

[About the Application Signatures Page | 211](#)

[Understanding Custom Application Signatures | 213](#)

[Adding Application Signatures | 214](#)

[Editing, Cloning, and Deleting Application Signatures | 219](#)

[Creating Application Signature Groups | 221](#)

[Editing, Cloning, and Deleting Application Signature Groups | 222](#)

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 | 205](#)

[Downloading a Signature Database | 207](#)

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 207](#).
- 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 73 on page 206](#) describes the fields on this page.

Table 73: 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 <i>detector-versions</i> link to view the detector details. The Detector Details for <i>Signature-Database-Version</i> 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 73: Fields on the Signature Database Page (*continued*)

Field	Description
<i>Latest List of Signatures</i>	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	<p>Displays the summary of changes from the previous version of the signature database; for example, 6 new signatures, 1 updated signature, 1 renamed signature.</p> <p>Click the hyperlinked text to view the details of the updates. The Signature Update Details for Database <i>Version</i> 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.</p>
Detectors	<p>Version numbers of the detector engines associated with the signature database.</p> <p>Click the <i>detector-versions</i> link to view the detector details. The Detector Details for <i>Signature-Database-Version</i> 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.</p>
Action	<p>Click the Full Download link to download the complete signature database; the download might take a while to complete.</p> <p>NOTE: This field is displayed only for users with the SP administrator role.</p>

RELATED DOCUMENTATION

[Signature Database Overview](#) | 205

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 74 on page 208](#).

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 74: Fields on the Signature Download Settings Page

Field	Description
Download URL	<p>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.</p> <p>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.</p> <p>For more information, see “Download Locations for Signature Database” on page 209.</p>
Signature Version	<p>NOTE: This field is enabled only when you change the download URL from https://signatures.juniper.net/.</p> <p>Enter the numeric value of the signature database version. The value must only contain numbers and not have any special characters or negative values.</p>

Table 74: Fields on the Signature Download Settings Page (*continued*)

Field	Description
Type	<p>You can chose to download the signature database immediately or schedule the download for later.</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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. <p>NOTE: The time-zone is picked-up based on the time-zone specified when CSO is installed.</p>

RELATED DOCUMENTATION

[Signature Database Overview | 205](#)

[About the Signature Database Page | 205](#)

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 | 211](#)

| [Creating Application Signature Groups | 221](#)

| [Editing, Cloning, and Deleting Application Signature Groups | 222](#)

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 214](#).
- Modify, clone, or delete an application signature. See [“Editing, Cloning, and Deleting Application Signatures” on page 219](#).
- 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 75 on page 212 describes the fields on the **Application Signatures** page.

Table 75: 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 | 210](#)

[Creating Application Signature Groups | 221](#)

[Editing, Cloning, and Deleting Application Signature Groups | 222](#)

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 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 | 214](#)

[Editing, Cloning, and Deleting Application Signatures | 219](#)

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 76 on page 215](#).
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 intents.

[Table 76 on page 215](#) provides guidelines on using the fields on the **Create Application Signature** page.

Table 76: Fields on the Create Application Signature Page

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.
Order	<p>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.</p> <p>Range is 1-50000.</p>
Priority	Specify the application signature priority (high or low) over other application signatures.
Select one or more Application Identification match criteria	<p>Select one or more applications matching criteria from the following list:</p> <ul style="list-style-type: none"> • ICMP Mapping • IP Protocol Mapping • Address Mapping • L7 Signature
<i>ICMP Mapping</i>	<p>Specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification.</p> <p>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.</p>
ICMP Type	<p>Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name.</p> <p>Range is 0-254.</p>
ICMP Code	<p>Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field.</p> <p>Range is 0-254.</p>
<i>IP Protocol Mapping</i>	Specify the IP protocol value for an application to match. This parameter is used to identify an application based on IP and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.

Table 76: Fields on the Create Application Signature Page (*continued*)

IP Protocol	<p>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.</p> <p>Range is 0-254.</p> <p>You can find a complete list of industry standard protocol numbers at the IANA website.</p> <p>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.</p>
Address Mapping	<p>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.</p> <p>Address mapping provides efficiency and accuracy while handling traffic from a known application.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • 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.
Name	<p>Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p>
Dst. IP Address	<p>Enter an IPv4 or IPv6 address for the application.</p>
CIDR	<p>Enter a CIDR value for the IP Address that you assign to the application.</p> <p>Range for IPv4 address is 1-32.</p> <p>Range for IPv6 address is 1-128.</p>
Dst. TCP Port range (Optional)	<p>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.</p> <p>The range is 0-65535.</p> <p>Example: 80-82 443.</p>
Dst. UDP port range (Optional)	<p>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.</p> <p>Example: 160-162 260.</p>

Table 76: Fields on the Create Application Signature Page (*continued*)

<i>L7 Signature</i>	Specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols.
Cacheable	<p>Select True to enable caching of application identification results on the device.</p> <p>Set 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.</p>
Name	Displays the name of the L7 signature.
Port range	Displays the port range for the application.
Over Protocol	Displays the L7 application protocol that matches the signature..
Members	Displays the member name for L7 signature.
<i>Add L7 Signature</i>	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.
Over Protocol	<p>Displays the signature to match the application protocol.</p> <p>Example: HTTP.</p>
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	<p>Enter the port range for the application.</p> <p>Range is 0-65535</p> <p>Example: 80-82,443</p>
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 76: Fields on the Create Application Signature Page (*continued*)

Direction	<p>Select the direction of the packet flow to which the signature must be matched.</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Context (<i>Over HTTP</i>)	<p>Select the service-specific context from the following list:</p> <ul style="list-style-type: none"> • 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 <p>For possible combinations of context and direction for L7 application creation, refer context (Application Identification).</p>
Context (<i>Over SSL</i>)	<p>Select the service-specific context as ssl-server-name.</p>
Context (<i>Over TCP</i>)	<p>Select the service-specific context as stream.</p>
Context (<i>Over UDP</i>)	<p>Select the service-specific context as stream.</p>

RELATED DOCUMENTATION

[Understanding Custom Application Signatures | 213](#)
[Editing, Cloning, and Deleting Application Signatures | 219](#)
[Adding SLA-Based Steering Profiles | 235](#)
[Adding Path-Based Steering Profiles | 247](#)

Editing, Cloning, and Deleting Application Signatures

IN THIS SECTION

- [Editing Application Signatures | 219](#)
- [Cloning Application Signatures | 220](#)
- [Deleting Application Signatures | 220](#)

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 214](#).
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 214](#)

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 appears to 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

Creating 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 77 on page 221](#).
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 77 on page 221](#) provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 77: 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 | 210](#)[About the Application Signatures Page | 211](#)[Editing, Cloning, and Deleting Application Signature Groups | 222](#)

Editing, Cloning, and Deleting Application Signature Groups

IN THIS SECTION

- [Editing Application Signature Groups | 222](#)
- [Cloning Application Signature Groups | 223](#)
- [Deleting Application Signature Groups | 223](#)

You can edit, clone, and delete application signature groups from the **Application Signatures** page.

Editing Application Signature Groups

To modify the parameters configured for a cloned user-created (custom) 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 click on the edit icon (pencil symbol), 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 group.

3. Modify the parameters according to the guidelines provided in [“Creating Application Signature Groups” on page 221](#).
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 a custom 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 a custom 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 clone, and then select **More > Clone**, or right-click the application signature group and then select **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 a cloned user-created (custom) 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.

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 | 210](#)

[About the Application Signatures Page | 211](#)

[Creating Application Signature Groups | 221](#)

7

CHAPTER

Managing Profiles

[Application Quality of Experience \(AppQoE\) Overview | 226](#)

[About the Application Traffic Type Profiles Page | 227](#)

[About the SLA-Based Steering Profiles Page | 231](#)

[Adding SLA-Based Steering Profiles | 235](#)

[Editing and Deleting SLA-Based Steering Profiles | 242](#)

[About the Path-Based Steering Profiles Page | 244](#)

[Adding Path-Based Steering Profiles | 247](#)

[Editing and Deleting Path-Based Steering Profiles | 249](#)

Application Quality of Experience (AppQoE) Overview

IN THIS SECTION

- [Workflow | 227](#)

Application Quality of Experience (AppQoE) aims to improve the user experience at the application level by constantly monitoring the class-of-service parameters and SLA compliance of application traffic and ensuring that the application data is sent over the most SLA-compliant link available. AppQoE is supported on both hub-and-spoke and full mesh topologies when the SD-WAN mode is set to Real Time-Optimized. AppQoE is implemented as a book-ended solution, where both the ends have SRX series devices or vSRX instances that run the same version of Junos OS with the same configuration.

AppQoE is enabled only when the SD-WAN mode for the tenant is set to Real Time-Optimized. In the default mode, which is Bandwidth-Optimized, CSO uses RPM probes to monitor link-level traffic.

On SD-WANs in the real time-optimized mode, CSO monitors the application traffic for SLA compliance. The CPE device uses this data to move the application traffic from links that fail to meet the SLA requirements to links that meet SLA.

To monitor the SLA compliance of the link on which the application traffic is sent, CSO sends inline probes, called as passive probes, along with the application traffic. To identify the best available link for an application in case the active link fails to meet the SLA criteria, CSO constantly monitors and collects SLA compliance data for other available links. The probes that CSO sends over the other links to check the SLA compliance are called as active probes. The active probes are carried out based on the probe parameters that you configure.

Link switching is done at the application level by the CPE device. That is, only the traffic corresponding to the application that reported the SLA violation is moved to a link that meets the specified SLA. The remaining traffic remains on the same link until those applications report an SLA violation.

You can configure traffic type profiles to specify the class-of-service parameters and the probe parameters for each traffic type. When you create an application SLA profile, you can link that with a traffic type profile and specify the SLA parameters and SLA sampling criteria for the SLA profile. The Application SLA profile is then linked to an SD-WAN policy intent, which can be deployed to implement AppQoE.

From the **Application SLA Performance** page, you can view the application-level SLA performance information and whether AppQoE is enabled. You can also view applications-level SLA performance details such as packet loss, RTT, jitter, and the number of probes.

The following sections describe the prerequisites, limitations, and workflow for configuring AppQoE.

Workflow

This section provides a sequential list of tasks that you need to perform to configure and monitor AppQoS:

1. OpCo administrators review the [“Default Traffic Type Profiles” on page 228](#), enable the required profiles, *modify the default profiles, or create new profiles*.
2. Add a tenant with the SD-WAN mode set to real time-optimized. For information about adding a tenant, see [“Adding a Single Tenant” on page 49](#).
3. Service provide administrator or tenant administrator can create an SLA-based steering profile or a path-based steering profile and associate a traffic type profile with that. For more information about creating an SLA-based steering profile or a path-based steering profile, see *Adding SLA-Based Steering Profiles*, and *Adding Path-Based Steering Profiles*.
4. Service provide administrator or tenant administrator can associate the SLA-based steering profile or a path-based steering profile with an SD-WAN Policy and deploy the policy. For more information see *Creating SD-WAN Policy Intents* and *Deploying Policies*.
5. OpCo administrator or tenant administrator can view application-level SLA performance details from the Application SLA Performance page. For more information, see [“Monitoring Application-Level SLA Performance for real time-optimized SD-WAN” on page 331](#).

About the Application Traffic Type Profiles Page

IN THIS SECTION

- [Default Traffic Type Profiles | 228](#)
- [Tasks You Can Perform | 229](#)
- [Field Descriptions | 230](#)

To access this page from the Administration portal, select **Configuration > Application Traffic Type Profiles**.

You can use the **Traffic Type Profiles** page 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. Traffic type profiles enable you to assign priority and service level criteria for traffic types. This topic contains the following sections:

Default Traffic Type Profiles

By default, CSO provides the following traffic type profiles:

- High-Priority-Video
- Premium-Internet
- Internet
- Hosted-AV
- Voice-Video

NOTE: By default, these traffic type profiles are disabled. Juniper SRE team can enable the profiles on a need-basis.

Table describes the default parameters for each of these traffic types.

Table 78: Default Traffic Type Profiles and Parameters

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
High Priority Video	Low	20%	Minimum of 20% and Maximum of 25%	Data size (bytes)	64	af31
				Probe interval (seconds)	30	
				Probe count	10	
				Burst size	1	
Premium-Internet	Low	10%	Minimum of 12% and Maximum of 15%	Data size (bytes)	64	af12
				Probe interval (seconds)	20	
				Probe count	10	
				Burst size	2	

Table 78: Default Traffic Type Profiles and Parameters (*continued*)

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
Internet	Low	5%	Minimum of 15% and Maximum of 20%	Data size (bytes)	64	af11
				Probe interval (seconds)	10	
				Probe count	5	
				Burst size	1	
Hosted-AV	Low	10%	Minimum of 16% and Maximum of 20%	Data size (bytes)	64	af32
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	
Voice-Video	Low	5%	Minimum of 20% and Maximum of 20%	Data size (bytes)	64	af41
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	

You can use the default traffic type profiles as is or request the Juniper SRE team to modify the parameters based on your specific requirements. Juniper SRE team can also create additional traffic type profiles. However, note that you can only have a maximum of six traffic type profiles enabled at a time. The total buffer allocation of the enabled traffic type profiles must not exceed 100%.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of the traffic type profiles configured for the tenant.
- Create a traffic type profile. See *Creating Traffic Type Profiles*.
- Edit or delete a traffic type profile. See *Editing and Deleting Traffic Type Profiles*.
- Show or hide columns that contain information about traffic type profiles. See *Sorting Objects*.
- Search for 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 79 on page 230 shows the descriptions of the fields on the Application Traffic Type Profiles page.

Table 79: Fields on the Application Traffic Type Profiles Page

Field	Description
Name	Displays the traffic type profile name.
Priority	Displays the traffic type profile priority.
Status	Displays whether the traffic type profile is enabled or disabled.
DSCP Value	Shows the DSCP value assigned to the traffic type profile. Differentiated Services Code Point (DSCP) values define the forwarding properties of the packet within the Differentiated Services framework.
Bandwidth	Shows the minimum and maximum bandwidth allocation for the traffic type profile.
Buffer	Shows the buffer allocation for the traffic type profile.
Probe Parameters	Shows the following probe parameters configured for the traffic type profile: <ul style="list-style-type: none"> • Data Size (in bytes) • Probe Interval (in seconds) • Probe Count • Burst Size
Created by	Shows the user that created the SLA profile.

RELATED DOCUMENTATION

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 235](#).
- Edit or delete an SLA-based steering profile. See [“Editing and Deleting SLA-Based Steering Profiles” on page 242](#).
- Show or hide columns that contain information about SLA-based steering profiles. See *Sorting Objects*.
- 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 80 on page 232](#) shows the descriptions of the fields on the SLA-Based Steering Profiles page.

Table 80: 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 <i>SLA-Profile-Name</i> pane
Priority	Priority of the SLA-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for <i>SLA-Profile-Name</i> pane
Traffic Type Profile	Indicates the traffic type profile associated with the SLA-based steering profile. <ul style="list-style-type: none"> • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET 	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
Packet Loss (%)	Target packet loss for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
Jitter (ms)	Target jitter for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
RTT	Target round-trip time (RTT) for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab) Detail for <i>SLA-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>SLA-Profile-Name</i> pane
Created By	Name of the user who created the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)

Table 80: Fields on the SLA-Based Steering Profiles Page (continued)

Field	Description	Displayed On
Path Preference	The preferred path for the SLA profile. The available options are: <ul style="list-style-type: none"> • MPLS • Internet • Any (default) 	Detail for <i>SLA-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>SLA-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>SLA-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the SLA violations are counted.	Detail for <i>SLA-Profile-Name</i> 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 <i>SLA-Profile-Name</i> 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 <i>SLA-Profile-Name</i> pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the SLA-based steering profile.	Detail for <i>SLA-Profile-Name</i> pane
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for <i>SLA-Profile-Name</i> pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the SLA-based-steering profile.	Detail for <i>SLA-Profile-Name</i> pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for <i>SLA-Profile-Name</i> pane

RELATED DOCUMENTATION

| *Traffic-Based Steering Profiles and SD-WAN Policies Overview*

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 81 on page 236](#) lists the SLA-based steering profiles that are tuned for specific application categories and traffic types.

Table 81: 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 81: 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 81: 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

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 82 on page 239](#).

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 82: Fields on the Add SLA Profile page

Field	Guidelines
<i>General</i>	
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: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● Liberal—To use a relaxed SLA threshold. ● Baseline—To use the default SLA threshold. ● Conservative—To use a strict SLA threshold.
<i>SLA Parameters</i>	
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.

Table 82: Fields on the Add SLA Profile page (continued)

Field	Guidelines
<i>Path Selection Criteria</i>	
Path Preference	<p>Select the preferred WAN link type to associate with the SLA profile. The options are Any, MPLS, and Internet. Any is the default value.</p> <p>Select the preferred path (MPLS, Internet, or Any) to be used for site-to-site traffic.</p> <p>If a WAN link type that matches the preferred path is enabled for site-to-site traffic, then that WAN link type is used for site-to-site traffic.</p> <p>If you specify that any path can be used, then there is no preference and all site-to-site-traffic-enabled links are used in a load-balancing mode.</p>
Path Failover Criteria	<p>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. Failover is supported only for MPLS or Internet links.</p> <p>NOTE: Path failover is supported only for bandwidth-optimized SD-WAN networks.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> • 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.
<i>Advanced Configuration-</i>	
Rate Limiting	
Maximum Upstream Rate	<p>Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile.</p> <p>Range: 64 through 10,485,760 Kbps</p>
Maximum Upstream Burst Size	<p>Enter the maximum upstream burst size (in bytes).</p> <p>Range: 1 through 1,342,177,280 bytes</p>
Maximum Downstream Rate	<p>Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile.</p> <p>Range: 64 through 10,485,760 Kbps</p>

Table 82: Fields on the Add SLA Profile page (continued)

Field	Guidelines
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	
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.

RELATED DOCUMENTATION

Traffic-Based Steering Profiles and SD-WAN Policies Overview

[About the SLA-Based Steering Profiles Page | 231](#)

[Editing and Deleting SLA-Based Steering Profiles | 242](#)

Editing and Deleting SLA-Based Steering Profiles

IN THIS SECTION

- [Editing an SLA-Based Steering Profile | 242](#)
- [Deleting SLA-Based Steering Profiles | 243](#)

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 235](#).

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

Traffic-Based Steering Profiles and SD-WAN Policies Overview

[About the SLA-Based Steering Profiles Page | 231](#)

[Adding SLA-Based Steering Profiles | 235](#)

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 247](#).
- Edit or delete a path-based steering profiles. See [“Editing and Deleting Path-Based Steering Profiles” on page 249](#).
- Show or hide columns that contain information about path-based steering profiles. See *Sorting Objects*.
- 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 83 on page 244](#) shows the descriptions of the fields on the Path-Based Steering Profiles page.

Table 83: 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 <i>Path-Profile-Name</i> pane

Table 83: Fields on the Path-Based Steering Profiles Page (*continued*)

Field	Description	Displayed on
Traffic Type Profile	<p>Indicates the traffic type profile associated with the path-based-steering profile.</p> <ul style="list-style-type: none"> • VOICE-VIDEO • HIGH_PRIORITY_VIDEO • HOSTED_AV • PREMIUM_INTERNET • INTERNET 	<p>Path-Based Steering Profiles Page (Path Profiles List tab)</p> <p>Detail for <i>Path-Profile-Name</i> pane</p>
Path Preference	<p>The preferred path for the SLA profile. The available options are:</p> <ul style="list-style-type: none"> • MPLS • Internet 	<p>Path-Based Steering Profiles Page (Path Profiles List tab)</p> <p>Detail for <i>Path-Profile-Name</i> pane</p>
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 <i>Path-Profile-Name</i> pane
Packet Loss	Target packet loss for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
RTT	Target round-trip time (RTT) for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
Jitter	Target jitter for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>Path-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>Path-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>Path-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the path-based steering profile violations are counted.	Detail for <i>Path-Profile-Name</i> pane

Table 83: Fields on the Path-Based Steering Profiles Page (*continued*)

Field	Description	Displayed on
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 <i>Path-Profile-Name</i> 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 <i>Path-Profile-Name</i> pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the path-based steering profile.	Detail for <i>Path-Profile-Name</i> pane
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for <i>Path-Profile-Name</i> pane
Maximum Downstream Rate	The maximum downstream rate (in Kbps) for all applications associated with the path-based-steering profile.	Detail for <i>Path-Profile-Name</i> pane
Maximum Downstream Burst Size	The maximum downstream burst size (in bytes).	Detail for <i>Path-Profile-Name</i> pane

RELATED DOCUMENTATION

| *Traffic-Based Steering Profiles and SD-WAN Policies Overview*

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 84 on page 247](#).

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 84: 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.

Table 84: Fields on the Add Path Profile page (*continued*)

Field	Guidelines
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are MPLS, and Internet.
<i>Advanced Configuration</i>	
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
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

Traffic-Based Steering Profiles and SD-WAN Policies Overview

[About the Path-Based Steering Profiles Page | 244](#)

[Editing and Deleting Path-Based Steering Profiles | 249](#)

Editing and Deleting Path-Based Steering Profiles

IN THIS SECTION

- [Editing a Path-Based Steering Profile | 249](#)
- [Deleting a Path-Based Steering Profile | 250](#)

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 247](#).

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

Traffic-Based Steering Profiles and SD-WAN Policies Overview

[About the Path-Based Steering Profiles Page](#) | 244

[Adding Path-Based Steering Profiles](#) | 247

8

CHAPTER

Managing Licenses

[About the Device License Files Page | 252](#)

[Uploading a Device License File | 253](#)

[Editing and Deleting Device Licenses | 254](#)

[Pushing a License to Devices | 256](#)

[About the CSO Licenses Page | 257](#)

[Assign CSO Licenses, and Update or Unassign CSO License Assignments | 259](#)

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 253](#).
- Edit and delete device license entries. See [“Editing and Deleting Device Licenses” on page 254](#).
- Push licenses to devices. See [“Pushing a License to Devices” on page 256](#).
- 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**. See *Viewing Object Details*.
- Show or hide columns about the device license files.
- Sort the device license files. See *Sorting Objects*.
- Search an object about the device license files. See *Searching for Text in an Object Data Table*.

Field Descriptions

[Table 85 on page 252](#) describes the fields on the License Files page.

Table 85: Fields on the License Files Page

Field	Description
File Name	Displays the filename of the license. Example: license_image_v1.txt
Description	Displays the description of the license. Example: License file for application routing.

Table 85: Fields on the License Files Page (*continued*)

Field	Description
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 | 253](#)
[Editing and Deleting Device Licenses | 254](#)
[Pushing a License to Devices | 256](#)

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 | 252](#)

[Device Images Overview | 187](#)

Editing and Deleting Device Licenses

IN THIS SECTION

● [Editing a Device License Entry | 255](#)

● [Deleting a Device License | 255](#)

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 | 252](#)

[Editing and Deleting Device Licenses | 254](#)

About the CSO Licenses Page

To access this page, click **Administration > Licenses > CSO Licenses**.

Users with the OpCo Administrator role can use the CSO Licenses page to view information about the CSO licenses issued by the SP administrator, assign the licenses to one or more tenants, and update or unassign license assignments.

Tasks You Can Perform

You can perform the following tasks from this page:

- Assign CSO licenses to one or more tenants—See [“Assign CSO Licenses, and Update or Unassign CSO License Assignments” on page 259](#).
- View the tenants previously assigned to a CSO license—Click *assigned-number* corresponding to a license. The View Assigned page appears displaying the tenants and quantity assigned to each tenant.
- Update or unassign CSO license assignments—See [“Assign CSO Licenses, and Update or Unassign CSO License Assignments” on page 259](#).
- 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 86 on page 258](#) describes the fields on the CSO Licenses page.

Table 86: Fields on the CSO Licenses page

Field	Description
License SKU	Displays the license SKU name; for example, S-CSO-C-S1-A-3.
Sales Order	Sales order number; for example, 15563238.
Type	Type of site—on-premise or cloud.
Tier	Support tier associated with the license; for example, Standard.
Device Class	Class of the Juniper device associated with the license; for example, B-class.
SSRN	Software support reference number, 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.
Device Quantity	Total number of devices (that the tenant can add) that you can assign for a license.
Available	Available number of devices (that the tenant can add) that you can assign to tenants.
Assigned	<p>Number of devices (that the tenant can add) that are already assigned to one or more tenants:</p> <ul style="list-style-type: none"> Click <i>assigned-number</i> 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, click Assign to assign the license to one or more tenants. See “Assign CSO Licenses, and Update or Unassign CSO License Assignments” on page 259.

RELATED DOCUMENTATION

[Assign CSO Licenses, and Update or Unassign CSO License Assignments](#) | 259

Assign CSO Licenses, and Update or Unassign CSO License Assignments

IN THIS SECTION

- [Assign CSO Licenses to Tenants](#) | 259
- [Update or Unassign CSO License Assignments](#) | 261

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 87 on page 260](#).

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 87: Fields on the Assign CSO License page

Field	Description
License Information	<p>Displays the following information for the license:</p> <ul style="list-style-type: none"> • Sales Order • License SKU • Start Date
<i>License Assignment</i>	
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	<p>To assign the license to one or more tenants:</p> <ol style="list-style-type: none"> 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 87 on page 260](#) 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](#) | 257

9

CHAPTER

Managing Users and Roles

[Role-Based Access Control Overview | 264](#)

[About the Users Page in Administration Portal | 265](#)

[Adding OpCo Users | 266](#)

[Editing and Deleting OpCo Users | 268](#)

[Resetting the Password for OpCo and Tenant Users | 270](#)

[Roles Overview | 271](#)

[About the Roles Page | 274](#)

[Adding User-Defined Roles for OpCo, and Tenant Users | 275](#)

[Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users | 277](#)

[Access Privileges for Role Scopes \(Operating Company and Tenant\) | 279](#)

Role-Based Access Control Overview

Conrail Service Orchestration supports the authentication and authorization of users. Both 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 88 on page 264](#) shows predefined OpCo and tenant roles and their access privileges.

Table 88: Roles and Access Privileges

Role	Role Scope	Access Privileges
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.
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](#) | 37

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 Operating Company (OpCo) scope.

For information about OpCo user roles and access permissions, see [“Role-Based Access Control Overview” on page 264](#).

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 an OpCo user. See [“Adding OpCo Users” on page 266](#).
- Edit and delete an OpCo user. See [“Editing and Deleting OpCo Users” on page 268](#).

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 OpCo scope. See [Table 89 on page 266](#).
- 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 OpCo and Tenant Users” on page 270](#).
- 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 89 on page 266](#) displays the fields on the Users page in the OpCo scope.

Table 89: 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).
Role	Depending on the scope selected, indicates the roles assigned to 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

[Adding Tenant and OpCo Tenant Users](#)

[Editing and Deleting Tenant and OpCo Tenant Users](#)

Adding OpCo Users

Use the Add OpCo User page in the Administration portal to add Operating Company (OpCo) users. After you add a user, the user receives an e-mail with the initial login credentials.

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 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.

The Add OpCo User page appears.

3. Complete the configuration as described in [Table 90 on page 267](#).

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*.

Table 90: Fields on the 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 <i>user@domain</i> 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 90: Fields on the Add OpCo User Pages (continued)

Field	Description
Role	<p>You can only assign OpCo and OpCo tenant roles to a user.</p> <p>To assign roles:</p> <ol style="list-style-type: none"> 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. <p>To know more about the predefined roles for OpCo and tenant users, see "Role-Based Access Control Overview" on page 264.</p>

RELATED DOCUMENTATION

- About the Users Page in Customer Portal*
- Adding Tenant and OpCo Tenant Users*
- Editing and Deleting Tenant and OpCo Tenant Users*

Editing and Deleting OpCo Users

IN THIS SECTION

- [Editing OpCo Users | 269](#)
- [Deleting OpCo Users | 269](#)

You can edit the information about 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 OpCo Admin, that allows you to edit and delete users.

Editing OpCo Users

To modify the information about 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.

The Edit OpCo User page appears.

3. Modify the parameters by following the guidelines provided in [Table 90 on page 267](#).

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.

Deleting OpCo Users

To delete one or more 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

About the Users Page in Customer Portal

Adding Tenant and OpCo Tenant Users

Editing and Deleting Tenant and OpCo Tenant Users.

Resetting the Password for OpCo and Tenant Users

As an 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 both 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 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](#) | 265

Roles Overview

IN THIS SECTION

- [Types of Roles](#) | 271
- [Role Scopes](#) | 272
- [Access Privileges](#) | 272
- [Relationship Between Users, Roles, and Access Privileges](#) | 273
- [Benefits of Roles in CSO](#) | 273

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 264](#).
- **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 OpCo administrator or a tenant administrator.
- 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 (OpCo and tenant). 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:

- **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*.

Access Privileges

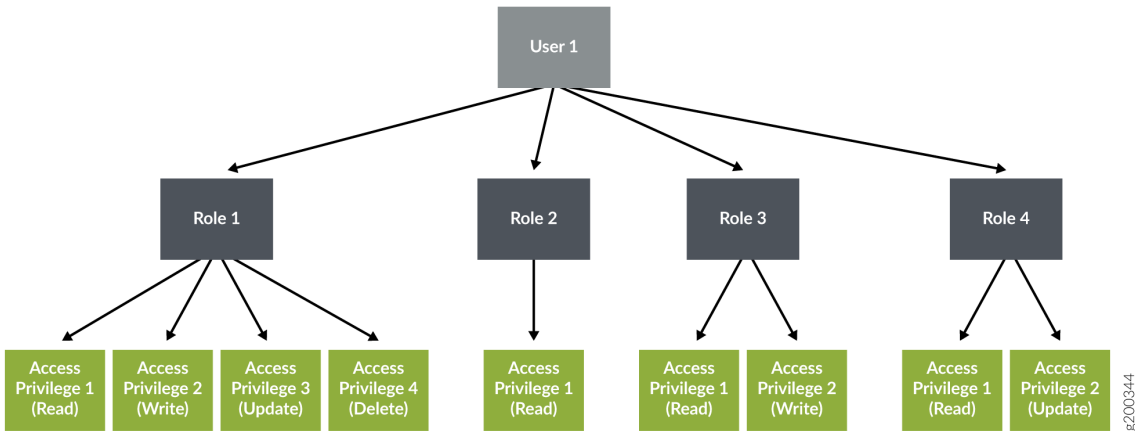
The following access privileges and actions can be assigned to a user role to access objects (Dashboard, Device Templates, Tenants, and so on) in CSO. For example, a user can be given only read, create, update privileges to device objects and only the delete privilege to security alerts objects.

- 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 10 on page 273 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 10: 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 | 264](#)

[About the Roles Page | 274](#)

[Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users | 277](#)

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 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 [“Adding User-Defined Roles for OpCo, and Tenant Users” on page 275](#).
- Edit, clone, or delete a role. See [“Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users” on page 277](#).

Field Descriptions

[Table 91 on page 274](#) describes the fields on the Roles page.

Table 91: 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

- [Adding User-Defined Roles for OpCo, and Tenant Users | 275](#)
- [Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users | 277](#)

Adding User-Defined Roles for 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 OpCo, and tenant user roles.

A user with the Create Role privilege can create custom roles for 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 92 on page 275](#).

4. Click **OK**.

A new role is created and listed on the Roles page.

NOTE: The tenant list in the top banner of the CSO is not displayed if the OpCo user that is logged in to CSO does not have tenant roles assigned.

Table 92: 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 92: Fields on the Add Role Page (*continued*)

Field	Description
Role scope (Visibility)	<p>Select the scope of the role. You can assign the role to the OpCo, or tenant user. There are three scopes for user roles:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>NOTE: You must assign at least one access privilege to a role.</p> <p>If you select the first-level objects, the submenu items that belong to the main object and the corresponding access privileges are also selected.</p> <p>The following access privileges can be assigned to a user role:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>

RELATED DOCUMENTATION

[Role-Based Access Control Overview | 264](#)

[About the Roles Page | 274](#)

[Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users | 277](#)

Editing, Cloning, and Deleting User-Defined Roles for OpCo, and Tenant Users

IN THIS SECTION

- [Editing Roles | 277](#)
- [Cloning Roles | 278](#)
- [Deleting Roles | 279](#)

You can edit and delete custom (user-defined) roles of OpCo, and tenant users from the Roles page. This topic has the following sections:

NOTE: You cannot modify or delete predefined roles.

Editing 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.

Cloning 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.

Deleting 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 | 274](#)

[Adding User-Defined Roles for OpCo, and Tenant Users | 275](#)

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 271](#).

[Table 93 on page 280](#) shows the access privileges for operating company scope.

[Table 94 on page 283](#) shows the access privileges for tenant scope.

Table 93: 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	-
	Device Events	Read	Manage Filter
	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	-
		Read, Create, Update, and Delete	-

Table 93: Access Privileges for Operating Company Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Path Based Steering Profiles		
	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 VPN	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	-

Table 93: Access Privileges for Operating Company Scope (*continued*)

Role Scope	Menu Name	Actions	Other Actions
	Release Notes	Read	-
	About	Read	-

Table 94: 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
	Device Events	Read	Manage Filter Create Alert
	Application Visibility	Read	-
	Threats Map (Live)	Read	-
	Application SLA Performance	Read	-
	Devices	Read	

Table 94: 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 94: 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 94: 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](#) | 264

[About the Roles Page](#) | 274

10

CHAPTER

Managing Jobs

About the Jobs Page | **289**

Viewing Job Details | **291**

Editing and Deleting Scheduled Jobs | **292**

Retrying a Failed Job on Devices | **294**

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 291](#).
- Retry a job. See [“Retrying a Failed Job on Devices” on page 294](#).
- Edit and delete schedule jobs. See [“Editing and Deleting Scheduled Jobs” on page 292](#).

Field Descriptions

[Table 95 on page 289](#) provides guidelines on using the fields on the Jobs page.

Table 95: 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 95: Fields on the Jobs Page (*continued*)

Field	Description
Number of Tasks	<p>View the number of tasks associated with the job.</p> <p>Example: 2</p> <p>For example, the tasks site.ucpe-32 and customer.sdwan are associated with this job.</p>
Job ID	<p>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:</p> <ul style="list-style-type: none"> • 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 96 on page 290](#) provides guidelines on using the fields on the Scheduled Jobs page.

Table 96: Fields on the Scheduled Jobs Page

Field	Description
Schedule ID	<p>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.</p> <p>Example: 48</p>
Name	<p>View the unique name of the scheduled job.</p> <p>Example: Tenant Delete_csp.tssm_remove_site_e340354716ae43859fad5ba15669eee2</p>

Table 96: 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 | 292](#)
[Retrying a Failed Job on Devices | 294](#)

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 | 289](#)

Editing and Deleting Scheduled Jobs

IN THIS SECTION

- [Editing Scheduled Jobs | 292](#)
- [Deleting Scheduled Jobs | 293](#)

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 | 289](#)

[Viewing Job Details | 291](#)

Retrying a Failed Job on Devices

You can retry **tssm.ztp** type jobs that did not complete successfully on your devices. Retrying a failed job saves time because instead of creating the job again and executing it, you can simply retry the failed job.

NOTE:

- The **Retry Job** button is enabled only for failed ZTP jobs.
- You cannot retry bootstrap jobs.

To retry a job that was not successful:

1. Select **Monitor > Jobs**.

The Jobs page appears.

2. Select the failed job (**tssm.ztp** type) that you want to retry.

3. At the top right corner of the Jobs page, click the **Retry Job** button.

The job is executed in the back end and the device status on the Sites page is changed to **PROVISIONED**.

RELATED DOCUMENTATION

[About the Jobs Page | 289](#)

[Editing and Deleting Scheduled Jobs | 292](#)

11

CHAPTER

Managing Audit Logs

[Audit Logs Overview](#) | **296**

[About the Audit Logs Page](#) | **296**

[Viewing the Details of an Audit Log](#) | **298**

[Exporting Audit Logs](#) | **300**

[Purging Audit Logs \(After Archiving or Without Archiving\)](#) | **302**

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 | 296](#)

[Exporting Audit Logs | 300](#)

[Purging Audit Logs \(After Archiving or Without Archiving\) | 302](#)

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 298](#).
- Export audit logs as a CSV file—See [“Exporting Audit Logs” on page 300](#).
- Purge audit logs—See [“Purging Audit Logs \(After Archiving or Without Archiving\)” on page 302](#).
- 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 97 on page 297](#) provides description of the fields on the Audit Logs page.

Table 97: 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 97: Fields on the Audit Logs Page (continued)

Field	Description
Status	<p>Displays the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Job ID	<p>For tasks that have associated jobs, displays the ID of the job associated with the task.</p> <p>You can click the job ID to go to the Jobs page, where you can view the status of the job.</p>

RELATED DOCUMENTATION

| [About the Jobs Page](#) | 289

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 98 on page 299](#) 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 98: Fields on the Audit Log Details Pane

Field	Description
Details	
User	
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.
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	<p>Displays the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • If the affected object is a site, the Sites page appears. See <i>About the Sites Page</i>. • If the affected object is a device, the Tenant Devices page appears. See <i>About the Devices Page</i>. • If the affected object is a tenant, clicking on the tenant name displays an error message as you do not have permission to view this page. <p>NOTE: If the object is deleted or if you do not have permissions to view it, an error message is displayed.</p>
Object UUID	Displays the Universally Unique Identifier (UUID) of the affected object.

Table 98: Fields on the Audit Log Details Pane (*continued*)

Field	Description
Log Info	
Audit Log ID	Displays the automatically-generated unique ID of the audit log associated with the task.
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 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.
Raw Audit Log	
Microservice	Displays the name of the microservice that initiated the execution of 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 | 296](#)

[Audit Logs Overview | 296](#)

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 99 on page 301](#).

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 99: 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	 296
About the Audit Logs Page	 296
Viewing the Details of an Audit Log	 298

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 100 on page 302](#).


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 100: Purge Audit Logs Settings

Field	Description
Purge Options	

Table 100: Purge Audit Logs Settings (*continued*)

Field	Description
Purge Logs	<p>Select one of the following options to purge audit logs:</p> <ul style="list-style-type: none"> • 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	<p>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)</p> <p>You specify the time in the local time zone of the client computer.</p>
Older than	<p>To purge generated audit logs older than a specified number of days, enter the number of days (from 1 through 90)</p>
Archive Logs Before Purging	<p>To archive audit logs <i>before</i> purging them, select this check box. By default, this check box is cleared, which means that audit logs are purged without archiving them.</p> <p>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.</p>
Archive Mode	<p>Specify whether you want to archive the log files locally (local) or on a remote server (remote).</p> <p>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.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • 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 100: 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	<p>Specify whether the audit logs should be purged immediately (Run now) or schedule the purge for later (Schedule at a later time).</p> <p>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.</p> <p>You specify the time in the local time zone of the client computer.</p>
Recurrence	<p>To specify whether the purge operation should occur on a recurring basis, select this check box.</p> <p>NOTE: This option is enabled only if you choose to archive and purge audit logs older than a specified number of days.</p>
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	<p>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.</p> <p>You specify the time in the local time zone of the client computer.</p>
Ends	<p>Specify whether the recurring purge ends or not:</p> <ul style="list-style-type: none"> • 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. <p>You specify the time in the local time zone of the client computer.</p>

RELATED DOCUMENTATION

12

CHAPTER

Monitoring

[About the Monitor Overview Page | 308](#)

[Alerts Overview | 309](#)

[About the Generated Alerts Page | 310](#)

[About the Alert Definitions Page | 312](#)

[Creating SD-WAN Alert Definitions | 314](#)

[Editing and Deleting SD-WAN Alert Definitions | 315](#)

[About the Alarms Page | 317](#)

[About the Device Events Page | 318](#)

[Multidepartment CPE Device Support | 323](#)

[About the SLA Performance of All Tenants Page | 324](#)

[About the SLA Performance of a Single Tenant Page | 327](#)

[Monitoring Application-Level SLA Performance for real time-optimized SD-WAN | 331](#)

[Viewing the SLA Performance of a Site | 333](#)

[Viewing the SLA Performance of an Application or Application Group | 337](#)

[Understanding SLA Performance Score for Applications, Links, Sites, and Tenants | 339](#)

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 101 on page 308](#) shows the descriptions of the fields on the Monitor Overview page.

Table 101: 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 101: Fields on the Monitor Overview Page (*continued*)

Field	Description
Only the node with alerts	<p>View the nodes with issues with the service.</p> <p>Click the drop-down list located next to the Only the nodes with alerts check box and select the type of alerts.</p> <ul style="list-style-type: none"> • 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. <p>NOTE: The nodes without any alerts are displayed in blue.</p>

RELATED DOCUMENTATION

[About the Alert Definitions Page | 312](#)

[Creating SD-WAN Alert Definitions | 314](#)

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 | 310](#)

[About the Alert Definitions Page | 312](#)

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 102 on page 311 provides information about the fields on the Generated Alerts page.

Table 102: 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 a 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 Page | 312](#)

[Creating SD-WAN Alert Definitions | 314](#)

[Editing and Deleting SD-WAN Alert Definitions | 315](#)

About the Alert Definitions Page

To access this page, select **Monitor > Alarms & Alerts > Alert Definitions** in the Administration Portal.

Use the Alert Definitions page to manage alert definitions for SD-WAN and view alert definitions for security. 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:

- View existing SD-WAN Alert Definitions in the SD-WAN tab. The SD-WAN alert definitions are loading by default when the Alert Definitions page is loaded. See [Table 103 on page 313](#) for descriptions of the fields on the SD-WAN alert definitions pane.
- Create SD-WAN alert definitions. See [“Creating SD-WAN Alert Definitions” on page 314](#).
- Edit or delete an existing SD-WAN alert definition. See [“Editing and Deleting SD-WAN Alert Definitions” on page 315](#).
- View existing security alert definitions by clicking **Security**. See [Table 104 on page 313](#) 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. See *Sorting Objects*.
- 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.

Field Descriptions

[Table 103 on page 313](#) describes the fields on the SD-WAN alert definitions pane.

Table 103: Fields on the SD-WAN Alert Definitions Pane

Field	Description
Rule Priority	View the priority of the alert definition. A value of one (1) indicates highest priority.
Alert Description	View the description of the alert.
Filter	View the matching alert criteria to trigger the alert.
Action	View the action to be performed to resolve issues.
Context	View the additional configuration parameters that you can pass on to the rule action function.

[Table 104 on page 313](#) provides guidelines on using the fields on the Security alert definitions pane.

Table 104: 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
Tenant	View the tenant who defined the alert.

RELATED DOCUMENTATION

[Creating SD-WAN Alert Definitions | 314.](#)

[Editing and Deleting SD-WAN Alert Definitions | 315.](#)

Creating SD-WAN Alert Definitions

You can use the Create SD-WAN Alert Definition page to create an alert definition for SD-WAN that consists of data criteria for triggering alerts about issues in the SD-WAN environment. In the alert definition, you can also define the necessary action that is required to resolve issues based on the severity of the alert.

To create an SD-WAN alert definition:

1. Click the add icon (+) on the **Monitor > Alarms & Alerts > Alert Definitions > SD-WAN** page in Administration Portal.

The Create SD-WAN Alert Definition page appears.

2. Enter the alert definition configuration according to the guidelines provided in [Table 105 on page 314](#).
3. Click **OK** to create the alert definition.

Alternatively, if you want to discard your changes, click **Cancel** instead.

[Table 105 on page 314](#) describes the fields on the Create SD-WAN Alert Definition page.

Table 105: Fields on the Create SD-WAN Alert Definition Page

Field	Guidelines
Alert Name	Enter the name of the alert definition. Enter a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed, and the maximum length is 256 characters.
Alert Description	Enter a description for the alert definition; maximum length is 512 characters.
Priority	Enter the priority for the alert definition. A value of 1 indicates highest priority.
Filter	<p>Select the matching severity criteria to trigger an alert. You can match severity, alert type, or object types. You can select one of the following options:</p> <ul style="list-style-type: none"> • To match severity options, select Match Severity Critical, Match Severity Not Critical, Match Severity Major, Match Severity Not Major, Match Severity Normal, Match Severity Not Normal, or Match Severity All. The Match Severity Critical option is selected by default. • To match alert types, such as alerts related to the device host or the application services on the host, select Match Alert Type Service or Match Alert Type Host. • To match object types, such as a single uCPE device or a uCPE VNF, select Match Object Type UCPE DEVICE or Match Object Type UCPE VNF respectively.

Table 105: Fields on the Create SD-WAN Alert Definition Page (*continued*)

Field	Guidelines
Action	<p>Select the action to be performed to resolve issues based on the severity of the alert. You can select one of the following actions:</p> <ul style="list-style-type: none"> • Alert Action Send to Rmq—Send the alert object to an external RabbitMQ broker. This option is selected by default. If this option is selected, you can also enter additional RabbitMQ broker configuration parameters in the Context field. • Alert Action Discard—Discard the alert object. • Alert Action Resolve Uuids—Resolve UUIDs to a machine-readable format.
Context	<p>Enter a set of additional configuration parameters for the external RabbitMQ broker. The configuration parameters include the RabbitMQ broker IP address, port number, the exchange name and type, and the username and password. The parameters must be entered in JSON format. The additional parameters are passed as arguments to the action function when the selected action is Alert Action Send to Rmq.</p> <p>Example:</p> <pre>{ "broker_ip": "192.0.2.0", "broker_port": "5672", "exchange_name": "external_alert_exchange", "exchange_type": "topic", "user": "user-name", "password": "password" }</pre>

RELATED DOCUMENTATION

[About the Alert Definitions Page | 312](#)
[Editing and Deleting SD-WAN Alert Definitions | 315](#)

Editing and Deleting SD-WAN Alert Definitions

You can edit and delete SD-WAN alert definitions from the SD-WAN Alert Definitions page.

Editing an SD-WAN Alert Definition

To modify an SD-WAN alert definition:

1. Select the check box for the alert definition that you want to modify, and click the edit icon on the **Monitor > Alarms & Alerts > Alert Definitions > SD-WAN** page in the Administration Portal.

The Edit SD-WAN Alert Definition page appears.

2. Update the configuration as needed and according to the guidelines in [“Creating SD-WAN Alert Definitions” on page 314](#).

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

The alert definition information that you updated appears on the SD-WAN Alert Definitions page.

Alternatively, if you want to discard your changes, click **Cancel** instead.

Deleting SD-WAN Alert Definitions

If the alert definition is no longer needed, then you can delete the alert definition. To delete an SD-WAN alert definition:

1. Select one or more alert definitions that you want to delete and click the delete icon (X) on the **Monitor > Alarms & Alerts > Alert Definitions > SD-WAN** page in the Administration Portal.

A page requesting confirmation for the deletion appears.

2. Click **Yes** to confirm that you want to delete the alert definition.

The alert definition is deleted.

Alternatively, if you want to cancel the delete operation, click **No** instead.

RELATED DOCUMENTATION

[About the Alert Definitions Page | 312](#)

[Creating SD-WAN Alert Definitions | 314](#)

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.

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 309](#).

For example, an alarm is raised when

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 106 on page 317](#) 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 106 on page 317](#) provides information about the fields on the Alarms page.

Table 106: Fields on the Alarms Page

Field	Description
Severity	View the severity of the alarm.

Table 106: Fields on the Alarms Page (*continued*)

Field	Description
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.
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 | 310](#)

[About the Alert Definitions Page | 312](#)

About the Device Events Page

To access this page, click **Monitor > Device Events**.

Use the Device Events page to view information about device events such as routine operations, failure and error conditions, and emergency or critical conditions.

You can view comprehensive details of device events in a tabular format that includes sortable columns and a line graph (also known as swim lanes). The data presented in the line graph is refreshed automatically

based on the selected time range. The line graph shows light blue areas that represent all device events and dark blue areas represent blocked device events

Tasks You Can Perform

You can perform the following tasks from this page:

- Click **Custom** button to select the date and time range to generate the device event.
- Show or hide time range in the carousel by clicking **show** or **hide** buttons at the top of the page.

Advanced Search

You can perform advanced search of all events using the text field present above the tabular column. It includes the logical operators as part of the filter string. Enter the search string in the text field and based on your input, a list of items from the filter context menu is displayed. You can select a value from the list and then select a valid logical operator to perform the advanced search operation. Press Enter to display the search result in the tabular column below.

To delete the search string in the text field, click the delete icon (X icon).

Examples of event log filters are shown in the following list:

- Specific events originating from or landing within United States
 Source Country = United States OR Destination Country = United States AND Event Name =
 IDP_ATTACK_LOG_EVENT, IDP_ATTACK_LOG_EVENT_LS, IDP_APPDDOS_APP_ATTACK_EVENT_LS,
 IDP_APPDDOS_APP_STATE_EVENT, IDP_APPDDOS_APP_STATE_EVENT_LS,
 AV_VIRUS_DETECTED_MT, AV_VIRUS_DETECTED, ANTISPAM_SPAM_DETECTED_MT,
 ANTISPAM_SPAM_DETECTED_MT_LS, FWAUTH_FTP_USER_AUTH_FAIL,
 FWAUTH_FTP_USER_AUTH_FAIL_LS, FWAUTH_HTTP_USER_AUTH_FAIL,
 FWAUTH_HTTP_USER_AUTH_FAIL_LS, FWAUTH_TELNET_USER_AUTH_FAIL,
 FWAUTH_TELNET_USER_AUTH_FAIL_LS, FWAUTH_WEBAUTH_FAIL, FWAUTH_WEBAUTH_FAIL_LS
- User wants to filter all RT flow sessions originating from IPs in specific countries and landing on IPs in specific countries
 Event Name = RT_FLOW_SESSION_CREATE, RT_FLOW_SESSION_CLOSE AND Source IP =
 177.1.1.1, 220.194.0.150, 14.1.1.2, 196.194.56.4 AND Destination IP = 255.255.255.255,
 10.207.99.75, 10.207.99.72, 223.165.27.13 AND Source Country = Brazil, United States, China, Russia,
 Algeria AND Destination Country = Germany, India, United States
- Traffic between zone pairs for policy – IDP2

Source Zone = trust AND Destination Zone = untrust, internal AND Policy Name = IDP2

- UTM logs coming from specific source country, destination country, source IPs with or without specific destination IPs

Event Category = antispam, antivirus, contentfilter, webfilter AND Source Country = Australia AND Destination Country = Turkey, United States, Australia AND Source IP = 1.0.0.0,1.1.1.3 OR Destination IP = 74.125.224.47,5.56.17.61

- Events with specific sources IPs or events hitting HTP, FTP, HTTP, and unknown applications coming from host DC-SRX1400-1 or VSRX-75.

Application = tftp, ftp, http, unknown OR Source IP = 192.168.34.10, 192.168.1.26 AND Hostname = dc-srx1400-1, vsrx-75

Field Descriptions

Table 107 on page 320 provides guidelines on using the fields on the Device Events page.

Table 107: Fields on the Device Events Detailed View Page

Field	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Tenant	View the name of the tenant.
Site	View the name of the tenant site.
Source Country	View the name of source country from where the event originated.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the name of destination country from where the event occurred.
Destination IP	View the destination IP address of the event.
Source Port	View the source port of the device event.
Destination Port	View the destination port of the device event.
Description	View the description of the log.

Table 107: Fields on the Device Events Detailed View Page (*continued*)

Field	Description
Attack Name	View the attack name of the log. For example, Trojan, worm, virus, and so on.
Threat Severity	View the severity level of the threat.
Policy Name	View the policy name in the log.
UTM Category or Virus Name	View the UTM category of the log.
URL	View the accessed URL name that triggered the event.
Event Category	View the event category of the log.
User Name	View the username of the log.
Argument	View the type of traffic. For example, ftp and http.
Action	View the action taken for the event. For example, warning, allow, or block.
Log Source	View the IP address of the log source.
Application	View the application name from which the events or logs are generated.
Hostname	View the host name in the log.
Service Name	View the name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role name associated with the log.
Reason	View the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.

Table 107: Fields on the Device Events Detailed View Page (*continued*)

Field	Description
NAT Source Port	View the translated source port.
NAT Destination Port	View the translated destination port.
NAT Source Rule Name	View the NAT source rule name.
NAT Destination Rule Name	View the NAT destination rule name.
NAT Source IP	View the translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
NAT Destination IP	View the translated (also called natted) destination IP address.
Traffic Session ID	View the traffic session ID of the log.
Path Name	View the path name of the log.
Logical System Name	View the name of the logical system.
Rule Name	View the name of the rule.
Profile Name	The name of the profile that triggered the event.
Event Count	View the number of events occurred.
Tenant	View the name of the tenant from which the event originated.

Multidepartment CPE Device Support

Multitenancy enables a single NFX Series device to be mapped to serve across multiple departments within a single tenant. Each department has its own Layer 3 VPN and all Layer 3 VPNs are carried over to the hub using a shared overlay. The traffic is segregated to each department. A single overlay of IPsec or generic routing encapsulation (GRE) tunnels is used to carry all department traffic from the 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 departments across a tenant. With multitenant device support, a dedicated share of the device is allocated to each department, and the data is kept private from the other tenants that access the same device.

NOTE: Only users with the Tenant Administrator role have access to the Customer Portal GUI.

The tenant administrator can perform the following tasks:

- Manage and monitor all policies and dashboards for all departments.
- Manage applications in the dashboard for each tenant.
- Create SD-WAN and security policies for each tenant and monitor the dashboard at the site level or at the department level.
- View or select SD-WAN or security services on the shared CPE device through the management portal.
- View the shared CPE device and its services and networks even though the WAN links might be shared by multiple departments.

The OpCo administrator can see all departments within the CPE device and activate the device.

RELATED DOCUMENTATION

About the SLA Performance of a Single Tenant Page

Viewing the SLA Performance of a Site

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 108 on page 325](#) describes the fields on the Tenants SLA Performance page.

Table 108: 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	<p>Specify the performance threshold, in percentage, based on which tenants can be classified as tenants with low, medium, or high SLA performance.</p> <p>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.</p> <p>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.</p>
Tenants with Low and Medium Performance	<p>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.</p> <p>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 327.</p>
Tenants with High Performance	<p>View the tenants that have high SLA performance in the selected time range.</p> <p>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 327.</p>

Table 109 on page 325 describes the fields in the card and grid views.

Table 109: 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 109: 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 339.
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 | 327](#)

[Viewing the SLA Performance of a Site | 333](#)

[Viewing the SLA Performance of an Application or Application Group | 337](#)

[Adding SLA-Based Steering Profiles | 235](#)

[Adding Path-Based Steering Profiles | 247](#)

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. .

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 110 on page 328](#) describes the fields on the SLA Performance of a Single Tenant page.

Table 110: 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	<p>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.</p> <p>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.</p> <p>Sites 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.</p>
Sites with Low and Medium Performance	<p>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.</p> <p>Click each site to view information about application-level SLA performance. See “Application and Link Level SLA Performance” on page 329.</p>
Sites with High Performance	<p>View the sites that have high SLA performance in the selected time range.</p> <p>Click each site to view information about the application-level SLA performance. See “Application and Link Level SLA Performance” on page 329.</p>

Table 111 on page 328 describes the fields in the card and grid views.

Table 111: 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.

Table 111: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views (continued)

Field Name	Card or Grid View	Description
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 339 .
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 112 on page 329](#) describes the fields on the SLA Performance of a Single Tenant page.

Table 112: 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.

Table 112: Fields on the SLA Performance of a Single Tenant Page (*continued*)

Field	Description
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	<p>Choose one of the following SLA parameters based on which you want to view the application SLA performance data:</p> <ul style="list-style-type: none"> • Throughput • Latency metric • Packet loss • Jitter metric <p>By default, Throughput is selected. The data for the selected parameter is displayed in the y-axis in the scatter plot view.</p>
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 .
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	

Table 112: Fields on the SLA Performance of a Single Tenant Page (*continued*)

Field	Description
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 | 324](#)
[Viewing the SLA Performance of a Site | 333](#)
[Viewing the SLA Performance of an Application or Application Group | 337](#)
[Adding SLA-Based Steering Profiles | 235](#)
[Adding Path-Based Steering Profiles | 247](#)

Monitoring Application-Level SLA Performance for real time-optimized SD-WAN

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.

In real time-optimized mode, 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 339](#).

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 | 332](#)
2. [Viewing SLA Performance of Sites | 332](#)

Viewing SLA Performance of Tenants

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 324 page appears.

2. Customize the view to your specific requirements.

For customization options, see [Table 108 on page 325](#)

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 109 on page 325](#)

Viewing SLA Performance of Sites

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 327.

2. Customize the view as required. For more information about the customization options, see [Table 110 on page 328](#)

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 111 on page 328](#).

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 112 on page 329](#).

Viewing the SLA Performance of a Site

IN THIS SECTION

- [SLA Not Met by SLA Profiles | 333](#)
- [Applications SLA Performance by Throughput | 334](#)
- [SLA Performance for ALL | 336](#)

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 337](#).

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 113 on page 335](#) describes the fields on the Applications SLA Performance by Throughput grid view.

Table 113: 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 337](#).

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 231](#) and [“About the Path-Based Steering Profiles Page” on page 244](#) page.

RELATED DOCUMENTATION

[About the SLA Performance of All Tenants Page | 324](#)

[About the SLA Performance of a Single Tenant Page | 327](#)

[Viewing the SLA Performance of an Application or Application Group | 337](#)

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 114 on page 337](#) describes the fields on the application or application group SLA Performance details page.

Table 114: 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 114: Fields on the Application or Application Group Details Page (*continued*)

Field	Description
Global SLA Profile Performance	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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 | 324](#)

[About the SLA Performance of a Single Tenant Page | 327](#)

[Viewing the SLA Performance of a Site | 333](#)

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

IN THIS SECTION

- [Application Score | 339](#)
- [Site Score | 340](#)
- [Tenant Score | 340](#)
- [Link Score | 340](#)

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 339](#).

The site score for bandwidth-optimized networks is calculated as an average of [“Link Score” on page 340](#).

Tenant Score

Tenant score is calculated as the average value of site scores. For information about site score calculation, see [“Site Score” on page 340](#).

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 (in bandwidth-optimized networks):

- Latency
- Jitter
- Packet Loss

For VoIP traffic, the link score calculation also considers the R-Value and MOS.