Administration Portal Online Help

Release
3.3

Modified: 2018-03-29

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. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

Administration Portal Online Help
3.3
Copyright © 2018 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://www.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 . . . xvii
Documentation and Release Notes . . . xvii
Documentation Conventions . . . xvii
Documentation Feedback . . . xix
Requesting Technical Support . . . xx
Self-Help Online Tools and Resources . . . xx
Opening a Case with JTAC . . . xx

Part 1 Overview

Chapter 1 **Introduction . . . 3**

Unified Administration and Customer Portal Overview . . . 3
Administration Portal Overview . . . 4
Logging in to Administration Portal . . . 5
Switching the Tenant Scope . . . 5
Changing the Administration Portal Password . . . 6
Changing the Password on First Login . . . 7
Resetting the Password . . . 8
Setting Password Duration . . . 9
Extending the User Login Session . . . 10
Setting Up the Cloud CPE Centralized Deployment Model with Administration Portal . . . 10
Setting Up the Cloud CPE Distributed Deployment Model with Administration Portal . . . 11

Chapter 2 **Managing Objects . . . 13**

Creating Objects . . . 13
Modifying an Object . . . 13
Deleting Objects . . . 14
Viewing Object Details . . . 14
Searching for Text in an Object Data Table . . . 15
Sorting Objects . . . 15

Part 2 Dashboard

Chapter 3 **Using the Dashboard . . . 19**

About the Administration Portal Dashboard . . . 19
Tasks You Can Perform . . . 19
Field Descriptions . . . 19

Part 3 Monitor

Chapter 4 **Monitoring Alerts, Alarms, and Device Events 23**

About the Monitor Overview Page 23
Tasks You Can Perform 23
Field Descriptions 23
About the Generated Alerts Page 24
Tasks You Can Perform 24
Field Descriptions 25
About the SD-WAN Alert Definitions Page 25
Tasks You Can Perform 25
Field Descriptions 26
Creating SD-WAN Alert Definitions 26
Editing and Deleting SD-WAN Alert Definitions 28
Editing an SD-WAN Alert Definition 28
Deleting SD-WAN Alert Definitions 29
About the Device Events Page 29
Tasks You Can Perform 29
Advanced Search 29
Field Descriptions 30

Chapter 5 **Monitoring Tenants SLA Performance 33**

Multidepartment CPE Device Support 33
About the SLA Performance of All Tenants Page 34
Tasks You Can Perform 34
Field Descriptions 34
About the SLA Performance of a Single Tenant Page 36
Tasks You Can Perform 36
Field Descriptions 37
Application and Link Level SLA Performance 39
Monitoring Application-Level SLA Performance for real time-optimized SD-WAN 40
Viewing SLA Performance of Tenants 40
Viewing SLA Performance of Sites 41
Viewing the SLA Performance of a Site 41
SLA Not Met by SLA Profiles 42
Applications SLA Performance by Throughput 42
SLA Performance for ALL 44
Viewing the SLA Performance of an Application or Application Group 45
Understanding SLA Performance Score for Applications, Links, Sites, and Tenants 46
Application Score 46
Site Score 47
Tenant Score 47
Link Score 47

Chapter 6 **Monitoring Jobs 49**

About the Jobs Page 49
Tasks You Can Perform 49
Field Descriptions 49

Field Descriptions . . . 50
Viewing Job Details . . . 51
Editing and Deleting Scheduled Jobs . . . 51
Editing Scheduled Jobs . . . 51
Deleting Scheduled Jobs . . . 52
Retrying a Failed Job on Devices . . . 52

Part 4 Resources

Chapter 7 **Managing POPs . . . 57**

About the POPs Page . . . 57
Tasks You Can Perform . . . 57
Field Descriptions . . . 58
Creating a Single POP . . . 59
Adding Information About the POP . . . 60
Adding a Device . . . 61
Adding a VIM . . . 64
Adding an EMS . . . 68
Reviewing and Saving the POP Configuration Settings . . . 69
Importing Data for Multiple POPs . . . 70
Customizing a POP Data File . . . 70
Uploading a POP Data File . . . 74
Viewing the History of POP Data Imports . . . 75
Viewing the History of POP Data Deletions . . . 77
Managing a Single POP . . . 78
About the VIMs Page . . . 79
Tasks You Can Perform . . . 79
Field Descriptions . . . 79
Creating a Cloud VIM . . . 81
About the EMS Page . . . 85
Tasks You Can Perform . . . 85
Field Descriptions . . . 85
Creating an EMS . . . 86
Changing the Junos Space Virtual Appliance Password . . . 87
About the Routers Page . . . 88
Tasks You Can Perform . . . 88
Field Descriptions . . . 88
Creating Devices . . . 89
Configuring Devices . . . 91
View the History of Device Data Deletions . . . 94

Chapter 8 **Managing Devices . . . 97**

About the Tenant Devices Page . . . 97
Tasks You Can Perform . . . 97
Field Descriptions . . . 98
About the Cloud Hub Devices Page . . . 100
Tasks You Can Perform . . . 101
Field Descriptions . . . 101
Managing a Tenant Device . . . 102
Managing a Cloud Hub Device . . . 103

Device Redundancy Support Overview 104
Prerequisites for SRX Series Devices 104
Supported Connection Plans 104
Create and Configure an SD-WAN Site 104
Dual CPE Devices Logical Topology for NFX Network Services Platform . . . 105
Dual CPE Devices Logical Topology for SRX Series Gateway Devices 105
Viewing the History of Tenant Device Activation Logs 106
Viewing the History of Cloud Hub Device Activation Logs 108
Adding a Cloud Hub Device 109
Rebooting a CPE Device 111

Chapter 9 **Managing Device Templates 115**

About the Device Template Page 115
Tasks You Can Perform 116
Field Descriptions 116
Cloning a Device Template 120
Importing a Device Template 121
Creating a Device Template File 121
Importing a Device Template File 121
Configuring a Device Template 122
Configuring Template Settings in a Device Template 122
Updating Stage-2 Configuration Template in a Device Template 125
Configuring Stage-2 Initial Configuration 128
Modifying a Device Template Description 129
Deleting a Device Template 130

Chapter 10 **Managing Software Images 131**

Device Images Overview 131
About the Device Images Page 132
Tasks You Can Perform 132
Field Descriptions 132
Deploying Device Images to Devices 133
Uploading a Device Image 135
Deleting Device Images 137

Part 5 Configuration

Chapter 11 **Configuring Network Services 141**

Network Services Overview 141
About the Network Services Page 142
Tasks You Can Perform 142
Field Descriptions 142
About the Service Overview Page 144
Tasks You Can Perform 144
Field Descriptions 144

About the Service Instances Page 145
Tasks You Can Perform 145
Field Descriptions 146
Configuring VNF Properties 147
Allocating a Service to Tenants 147
Removing a Service from Tenants 148
Viewing a Service Configuration 148
vSRX VNF Configuration Settings 149
LxCIPtable VNF Configuration Settings 156
Cisco CSR-1000v VNF Configuration Settings 159
Riverbed Steelhead VNF Configuration Settings 160
Managing a Single Service 161

Chapter 12 **Configuring Application SLA Profiles 163**

Application Quality of Experience (AppQoE) Overview 163
Limitations 164
Workflow 164
About the Application Traffic Type Profiles Page 165
Default Traffic Type Profiles 165
Tasks You Can Perform 167
Field Descriptions 167
Creating Traffic Type Profiles 168
Editing and Deleting Traffic Type Profiles 171
Editing Traffic Type Profiles 171
Deleting Traffic Type Profiles 171
SLA Profiles and SD-WAN Policies Overview 172
SLA Profiles 172
SD-WAN Policies 173
Local Breakout Overview 175
About the Application SLA Profiles Page 176
Tasks You Can Perform 176
Field Descriptions 176
Creating SLA Profiles 177
Editing and Deleting SLA Profiles 179
Editing an SLA Profile 179
Deleting SLA Profiles 180

Chapter 13 **Configuring Application Signatures 181**

Application Signatures Overview 181
About the Application Signatures Page 182
Tasks You Can Perform 182
Field Descriptions 182
Creating Application Signature Groups 183
Editing, Cloning, and Deleting Application Signature Groups 184
Editing Application Signature Groups 184
Cloning Application Signature Groups 184
Deleting Application Signature Groups 185

Part 6 Tenants

Chapter 14 Managing Tenants 189

Tenant Overview 189
Full Mesh Topology Overview 189
Connection Modes in Full Mesh Topology 190
Local Breakout in Full Mesh Topology 191
About the Tenants Page 192
Before You Begin 192
Tasks You Can Perform 192
Field Descriptions 192
Adding a Single Tenant 194
Editing Tenant Information 198
Importing Data for Multiple Tenants 199
Creating a Tenant Data File 199
Importing Tenant Data 202
Allocating Network Services to a Tenant 203
Viewing the History of Imported Tenant Data 204
Viewing the History of Deleted Tenant Data 205

Part 7 Administration

Chapter 15 Configuring MSP Users 211

Role-Based Access Control Overview 211
About the Service Provider Users Page 212
Tasks You Can Perform 212
Field Descriptions 212
Adding Service Provider Users 213
Editing and Deleting Service Provider Users 214
Editing Service Provider Users 214
Deleting Service Provider Users 215

Chapter 16 Configuring Authentication 217

Authentication Methods Overview 217
About the Authentication Page 218
Tasks You Can Perform 218
Field Descriptions 218
Editing the Authentication Method 219
Configuring a Single Sign-On Server 221
Editing and Deleting SSO Servers 223
Editing SSO Server Configuration 223
Delete SSO Server Configurations 224
Configuring SMTP Settings 224

Chapter 17 Configuring Licenses 227
About the License Files Page 227
Tasks You Can Perform 227
Field Descriptions 227
Uploading a License File 228
Editing and Deleting Licenses 229
Editing a License Entry 229
Deleting a License 229
Pushing a License to Devices 230
Chapter 18 Customizing the Unified Portal 233
Personalizing the Unified Administration and Customer Portal 233
Chapter 19 Managing Signature Database 237
Signature Database Overview 237
About the Active Database Page 238
Tasks You Can Perform 238
Field Descriptions 238
Downloading a Signature Database 239
Download Locations for Signature Database 240
Installing Signatures 241

List of Figures

Part 4 Resources

Chapter 8 **Managing Devices 97**

Figure 1: Dual CPE Device Topology - NFX Network Services Platform 105
Figure 2: Dual CPE Device Topology - SRX Series Devices 105

Part 6 Tenants

Chapter 14 **Managing Tenants 189**

Figure 3: Dense Mode 191
Figure 4: Sparse Mode 191

List of Tables

About the Documentation xvii

Table 1: Notice Icons xviii
Table 2: Text and Syntax Conventions xviii

Part 1 Overview

Chapter 1 **Introduction 3**

Table 3: Fields on the Change Password Page 7
Table 4: Fields on the Reset Password Page 8

Part 2 Dashboard

Chapter 3 **Using the Dashboard 19**

Table 5: Widgets on the Dashboard 20

Part 3 Monitor

Chapter 4 **Monitoring Alerts, Alarms, and Device Events 23**

Table 6: Fields on the Monitor Overview Page 24
Table 7: Fields on the Generated Alerts Page 25
Table 8: Fields on the SD-WAN Alert Definitions Page 26
Table 9: Fields on the Create SD-WAN Alert Definition Page 27
Table 10: Fields on the Device Events Detailed View Page 30

Chapter 5 **Monitoring Tenants SLA Performance 33**

Table 11: Fields on the Tenants SLA Performance Page 35
Table 12: Fields on the Tenants SLA Performance Page 35
Table 13: Fields on the SLA Performance of a Single Tenant Page 37
Table 14: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views 38
Table 15: Fields on the SLA Performance of a Single Tenant Page 39
Table 16: Fields on the Applications SLA Performance by Throughput Grid View 43
Table 17: Fields on the Application or Application Group Details Page 45

Chapter 6 **Monitoring Jobs 49**

Table 18: Fields on the Jobs Page 49
Table 19: Fields on the Scheduled Jobs Page 50

Part 4 Resources

Chapter 7 **Managing POPs 57**

Table 20: Widgets on the POPs Page . . . 58
Table 21: Fields on the POPs Page . . . 58
Table 22: Fields on the Add POP page . . . 60
Table 23: Fields on the Add Device Page . . . 62
Table 24: Fields on the Add Cloud VIM Page . . . 65
Table 25: Fields on the Add EMS Page . . . 69
Table 26: Fields on the POPs Page . . . 71
Table 27: Fields on the Import History Page . . . 76
Table 28: Fields on the Import POPs Tasks Page . . . 76
Table 29: Fields on the Job Status Page . . . 76
Table 30: Fields on the Delete History Page . . . 77
Table 31: Fields on the Delete POPs Tasks Page . . . 77
Table 32: Fields on the Job Status Page . . . 78
Table 33: Widgets on the VIMs Page . . . 79
Table 34: Fields on the VIMs Page . . . 79
Table 35: Fields on the Add Cloud VIM Page . . . 82
Table 36: Fields on the EMS Page . . . 85
Table 37: Fields on the Add EMS Page . . . 86
Table 38: Change Password Fields . . . 87
Table 39: Fields on the Routers Page . . . 88
Table 40: Fields on the Add Device Page . . . 90
Table 41: Fields on the PNE Configure Page . . . 92
Table 42: Fields on the Delete History Page . . . 95
Table 43: Fields on the Delete Device Tasks Page . . . 95
Table 44: Fields on the Job Status Page . . . 95

Chapter 8 **Managing Devices . . . 97**

Table 45: Widgets on the Tenant Devices Page . . . 98
Table 46: Fields on the Tenant Devices Page . . . 98
Table 47: Fields on the Cloud Hub Devices Page . . . 101
Table 48: Fields on the ZTP History Page . . . 106
Table 49: Fields on the ZTP Logs Page . . . 107
Table 50: Fields on the Job Status Page . . . 107
Table 51: Fields on the ZTP History Page . . . 108
Table 52: Fields on the ZTP Logs Page . . . 109
Table 53: Fields on the Job Status Page . . . 109
Table 54: Fields on the Add Hub Device Page . . . 110

Chapter 9 **Managing Device Templates . . . 115**

Table 55: Fields on the Device Templates Page . . . 117
Table 56: Device Templates Supported on NFX250 Device . . . 118
Table 57: Device Templates Supported on SRX Series Services Gateways . . . 119
Table 58: Device Templates Supported on MX Series Router . . . 119
Table 59: Fields on the Template Settings Page . . . 123
Table 60: Fields on the Stage-2 Configuration Templates Page . . . 125
Table 61: Fields on the Add New Template Page . . . 126
Table 62: Fields for the VLAN Settings on the Stage-2 Initial Configuration Page . . . 128
Table 63: Fields for the LAN Settings on the Stage-2 Initial Configuration Page . . . 129

Table 64: Fields for the SRX Basic SD-WAN Settings on the Stage-2 Initial Configuration Page . . . 129

Chapter 10 Managing Software Images . . . 131

Table 65: Fields on the Images Page . . . 132
Table 66: Fields on the Upgrade History Page . . . 133
Table 67: Fields on the Deploy Image: Select Devices Page . . . 134
Table 68: Fields on the Upload Device Image Page . . . 136

Part 5 Configuration

Chapter 11 Configuring Network Services . . . 141

Table 69: Widgets on the Services Page . . . 142
Table 70: Fields on the Services Page . . . 143
Table 71: Fields on the Service Detail Page . . . 143
Table 72: Fields on the Service Overview Page . . . 144
Table 73: Fields on the Service Instances Page . . . 146
Table 74: Fields on the Service Instance Details Page . . . 146
Table 75: Fields for the vSRX Base Settings . . . 150
Table 76: Fields for the vSRX Firewall Settings . . . 151
Table 77: Fields for the vSRX NAT Settings . . . 153
Table 78: Fields for the vSRX UTM Settings . . . 154
Table 79: Fields for the LxCIP Base Settings . . . 156
Table 80: Fields for the LxCIP Firewall Policy Settings . . . 157
Table 81: Fields for the LxCIP NAT Policy Settings . . . 158
Table 82: Fields for the CSR-1000v Base Settings . . . 159
Table 83: Fields for the CSR-1000v Firewall Settings . . . 159

Chapter 12 Configuring Application SLA Profiles . . . 163

Table 84: Default Traffic Type Profiles and Parameters . . . 166
Table 85: Fields on the Application Traffic Type Profiles Page . . . 167
Table 86: Fields on the Create Traffic Type Profiles page . . . 169
Table 87: SLA Profile Categories . . . 172
Table 88: Fields on the Application SLA Profiles Page . . . 176
Table 89: Fields on the Create SLA Profile page . . . 177

Chapter 13 Configuring Application Signatures . . . 181

Table 90: Fields on the Application Signatures Page . . . 182
Table 91: Fields on the Create Application Signature Group Page . . . 183

Part 6 Tenants

Chapter 14 Managing Tenants . . . 189

Table 92: Widget on the Tenants Page . . . 192
Table 93: Fields on the Tenants Page . . . 193
Table 94: Fields on the Add Tenant Page . . . 194
Table 95: Tenant Configuration Fields . . . 200
Table 96: Fields on the Import History Page . . . 204
Table 97: Fields on the Import Tenants Task Page . . . 205
Table 98: Fields on the Job Status Page for Imported Tenant Data . . . 205
Table 99: Fields on the Delete History Page . . . 206

Table 100: Fields on the Delete Tenants Tasks Page 206
Table 101: Fields on the Job Status Page for Deleted Tenant Data 206

Part 7 Administration

Chapter 15 **Configuring MSP Users 211**

Table 102: Roles and Access Privileges 211
Table 103: Fields on the Users Page 212
Table 104: Fields on the Add User Page 213

Chapter 16 **Configuring Authentication 217**

Table 105: Fields on the Authentication Page 218
Table 106: Fields on the Authentication Type Page 219
Table 107: Fields on the Single Sign-On Server Page 222
Table 108: Attribute Values and Roles 223
Table 109: SMTP Settings 225

Chapter 17 **Configuring Licenses 227**

Table 110: Fields on the License Files Page 228

Chapter 18 **Customizing the Unified Portal 233**

Table 111: Fields on the Preferences Page 233

Chapter 19 **Managing Signature Database 237**

Table 112: Fields on the Active Database Page 238
Table 113: Fields on the Signature Download Settings Page 239

About the Documentation

- Documentation and Release Notes on page xvii
- Documentation Conventions on page xvii
- Documentation Feedback on page xix
- Requesting Technical Support on page xx

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 xviii 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 xviii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*

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

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

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

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

Documentation Feedback

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

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at https://www.juniper.net/documentation/index.html, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at https://www.juniper.net/documentation/feedback/.

- E-mail—Send your comments to **techpubs-comments@juniper.net**. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit 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/
- Open a case online in the CSC Case Management tool: https://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at https://www.juniper.net/cm/.
- 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://www.juniper.net/support/requesting-support.html.

PART 1

Overview

- Introduction on page 3
- Managing Objects on page 13

CHAPTER 1

Introduction

- Unified Administration and Customer Portal Overview on page 3
- Administration Portal Overview on page 4
- Logging in to Administration Portal on page 5
- Switching the Tenant Scope on page 5
- Changing the Administration Portal Password on page 6
- Changing the Password on First Login on page 7
- Resetting the Password on page 8
- Setting Password Duration on page 9
- Extending the User Login Session on page 10
- Setting Up the Cloud CPE Centralized Deployment Model with Administration Portal on page 10
- Setting Up the Cloud CPE Distributed Deployment Model with Administration Portal on page 11

Unified Administration and Customer Portal Overview

Contrail Service Orchestration supports a unified portal for both service provider users and tenant users and for the services managed and consumed by the administrators and tenants.

The unified portal contains the features of vCPE, uCPE, and SD-WAN for both Administration and Customer portals; enforces role-based access control (RBAC), which prevents tenants from accessing administrator data; and supports different backend authentication methods for service provider users and tenant users.

The unified portal enable service providers to deploy Juniper Networks security features as a virtualized network function (VNF) function either in distributed or centralized mode or in the branch SRX Series device. This VNF provides advanced firewall and Network Address Translation (NAT) management capabilities to end users from a single pane of glass (SPOG) user interface, in a multitenant environment. . Service provider administrators are able to manage all phases of the security policy life cycle more quickly and intuitively, from policy creation through deployment.

Firewall and NAT management features include policy configuration such as rule reordering, event viewer for firewall and NAT events, alerts and alarms, logs and dashboard widgets. All features have RBAC enforced, which enables either the MSP administrator or the tenant administrator to configure policies for the tenant.

The unified portal also provides SD-WAN capabilities with integrated firewall, NAT management, and device management.

Related Documentation

- SLA Profiles and SD-WAN Policies Overview on page 172
- Device Images Overview on page 131

Administration Portal Overview

Administration Portal offers service providers 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

- Setting Up the Cloud CPE Centralized Deployment Model with Administration Portal on page 10

- Setting Up the Cloud CPE Distributed Deployment Model with Administration Portal on page 11
- Logging in to Administration Portal on page 5

Logging in to Administration Portal

To start Administration Portal:

1. Review the Keystone username and password that you defined for Contrail OpenStack.

   You can view these settings on the Contrail Configure and Control node in the files **/etc/contrail/keystonerc** and **/etc/contrail/openstackrc**.

2. Using a Web browser, access the URL for Administration Portal. The URL for Administration Portal is https:*//Central-IP-Address*, where the *Central-IP-Address* denotes the IP address of the virtual machine (VM) that hosts the microservices for the central POP.

   For example, if the IP address of the VM is 192.0.2.1, then the URL is https://192.0.2.1.

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

3. Log in with the username **cspadmin** and password that you specified for Contrail OpenStack.

   The Dashboard page appears.

   NOTE: **You are prompted to change the password when you login to the portal for the first time.**

Related Documentation

- Administration Portal Overview on page 4
- Personalizing the Unified Administration and Customer Portal on page 233

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 on page 3
- Role-Based Access Control Overview on page 211

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 on page 4
- Logging in to Administration Portal on page 5

Changing the Password on First Login

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

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

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

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

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

2. Change your password following the guidelines provided in Table 3 on page 7.

3. Click **Ok**.

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

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

Table 3: Fields on the Change Password Page

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

Related Documentation

- Logging in to Administration Portal on page 5
- Changing the Administration Portal Password on page 6
- Resetting the Password on page 8
- Setting Password Duration on page 9

Resetting the Password

If you have forgotten your password, you can reset the password from the login screen.

NOTE: **Your account is locked after five consecutive unsuccessful login attempts.**

To reset the password:

1. On the login page, click the **Forgot Password** link.

   The Forgot Password page appears, with a message that an e-mail notification with a verification code is sent to your e-mail address.

   NOTE: **The Forgot Password link appears only after you specify the username.**

2. In **Verification Code**, specify the verification code that you have received through an e-mail.

   NOTE: **The verification code expires after a time duration of 15 minutes.**

3. Click **OK**.

   The Reset Password page appears.

4. Change your password following the guidelines provided in Table 4 on page 8.

5. Click **OK**.

Your password is reset.

Table 4: Fields on the Reset Password Page

Field	Description
Username	Enter your username.

Table 4: Fields on the Reset Password Page *(continued)*

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

Related Documentation

- Logging in to Administration Portal on page 5
- Changing the Administration Portal Password on page 6
- Changing the Password on First Login on page 7
- Setting Password Duration on page 9

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, for **User Password Expires** select one of the following option:

   - **Never**—If you select this option, the password never expires.
   - **After specified number of days**—If you select this option, the **Password Expiration Days** field appears.

     In **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 194.

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

- Logging in to Administration Portal on page 5
- Changing the Administration Portal Password on page 6
- Changing the Password on First Login on page 7
- Resetting the Password on page 8

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 on page 6

Setting Up the Cloud CPE Centralized Deployment Model with Administration Portal

In the Cloud CPE Centralized Deployment Model, end users at a specific customer site access most network services in a regional point of presence (POP), while accessing a few specialist network services in the central POP.

You use the following workflow to set up the Cloud CPE Centralized Deployment Model with Administration Portal:

1. Create the POPs and associated resources. See "Creating a Single POP" on page 59 and "Importing Data for Multiple POPs" on page 70.
   - You must create a VIM for each POP.
   - You can add an MX Series router as a physical network element (PNE) to provide a Layer 3 routing service to customer sites through use of virtual routing and forwarding (VRF) instances.
   - You add the Junos Space element management system (EMS) if you use a VNF that requires this EMS.
2. Create customers. See "Adding a Single Tenant" on page 194 and "Importing Data for Multiple Tenants" on page 199.
3. If you add customers one at a time, rather than importing data for multiple tenants, create and configure sites for each customer:
   - You must create each site individually.You can create the following sites:
     - On-Premise sites—required for all customer sites. See *Creating On-Premise Spoke Sites for SD-WAN Deployment*.
     - Cloud sites—required for all service providers. See *Creating Cloud Hub Sites for SD-WAN Deployment*.
     - Data Center—Only required for a network in which users access the Internet through the corporate VPN.
   - If you configured a PNE in Step 1, then associate the PNE with the site and configure a VRF for each customer site. See *Configuring VRFs and PNE Details for a Site in a Centralized Deployment*
4. Allocate network services to customers. See "Allocating a Service to Tenants" on page 147

Related Documentation

- Logging in to Administration Portal on page 5
- Administration Portal Overview on page 4

Setting Up the Cloud CPE Distributed Deployment Model with Administration Portal

In the Cloud CPE Distributed Deployment Model, end users at a specific customer site access network services in both a regional point of presence (POP) and a central POP.

You use the following workflow to set up the Cloud CPE Distributed Deployment Model with Administration Portal:

1. Add data for the POPs and provider edge (PE) router. See "Creating a Single POP" on page 59 and "Importing Data for Multiple POPs" on page 70.
2. Upload images for devices used in the deployment, such as the vSRX gateway and the NFX 250 platform to the central activation server. See "Uploading a Device Image" on page 135.

3. Upload VNF images. See "Uploading a Device Image" on page 135.
4. Create customers. See "Adding a Single Tenant" on page 194 and "Importing Data for Multiple Tenants" on page 199.
5. If you add customers one at a time, rather than importing data for multiple tenants, create and configure sites for each customer. .
6. Allocate network services to customers. See "Allocating a Service to Tenants" on page 147.

Related Documentation

- Logging in to Administration Portal on page 5
- Administration Portal Overview on page 4

CHAPTER 2

Managing Objects

- Creating Objects on page 13
- Modifying an Object on page 13
- Deleting Objects on page 14
- Viewing Object Details on page 14
- Searching for Text in an Object Data Table on page 15
- Sorting Objects on page 15

Creating Objects

You can use the create icon (**+**) in the top right corner of a page to create an object on that page.

To create an object:

1. Click the **+** icon.

   The object configuration page appears.

2. Update the configuration as needed.

   See the relevant *About the Objects Page* topic for a description of the fields.

3. Click **Upload**.

   The object information that you updated appears in the main page.

Related Documentation

- Deleting Objects on page 14

Modifying an Object

You can use the pencil icon in the top right of a page to modify or edit an object on that page.

To modify an object:

1. Select the check box of the object that you want to modify, and click the pencil icon.

   The object configuration page appears.

2. Update the configuration as needed.

3. Click **Save**.

   The object information that you updated appears in the main page.

Related Documentation

- Deleting Objects on page 14

Deleting Objects

You can use the delete icon (**X**) in the top right corner of a page to delete an object on that page.

To delete an object:

1. Select the object that you want to delete and click the **X** icon.

   The Confirm Delete page appears.

2. Click **Yes** to delete the object or **No** to cancel the deletion.

   The object information is deleted from the main page.

Related Documentation

- Creating Objects on page 13

Viewing Object Details

You can use the Detailed View page to view all the configured parameters of an object. Only some of the configured parameters appear in the list of features on the main page.

To view details for an object:

- Right-click the object that you want to see the detailed view for and click **Quick View**, or select the object and click **More > Details**.

- Alternatively, hover over the object name and click the Detailed View icon that appears before it.

The Detailed View page appears showing the configuration information. See the relevant *About the Objects Page* topic for a description of the fields on these pages.

Related Documentation

- Deleting Objects on page 14

Searching for Text in an Object Data Table

You can use the search icon in the top right corner of a page to search for text containing letters and special characters on that page.

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.

   The search results are displayed.

2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

Related Documentation

- Creating Objects on page 13

Sorting Objects

You can use the **Show Hide Columns** icon in the top right corner of a page to show or hide objects on a page. You can also sort the objects in a page by clicking the object column. The following options are available for sorting the objects:

- Sort text in alphabetical order.
- Sort numbers in ascending or descending order.
- Sort by date or time.
- Rearrange columns in a table.
- Increase or decrease column width.

To show or hide an object:

1. Click the **Show Hide Columns** icon.

   The objects that are relevant to the page are displayed. By default all objects are selected and displayed on the page.

2. Select the objects that need to be displayed on the page and clear the objects that are not required to be displayed.

   The objects are displayed or hidden as per the selection.

Related Documentation

- Creating Objects on page 13

PART 2

Dashboard

- Using the Dashboard on page 19

CHAPTER 3

Using the Dashboard

- About the Administration Portal Dashboard on page 19

About the Administration Portal Dashboard

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

Each time you log in to the Administration Portal, the first thing you see is a user-configurable dashboard that 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 on a per user basis.
- Update the dashboard or an individual widget by clicking the refresh icon.
- Show or hide widget thumbnails in the carousel by clicking **Select Widgets** at the top of the page.
- Add a widget to the dashboard by dragging the widget from the palette or thumbnail container into the workspace.
- Delete a widget from the dashboard page by clicking the X icon in the title bar.

Field Descriptions

You can quickly view important data using the widgets at the top of your dashboard.

Table 5 on page 20 describes the dashboard widgets.

Table 5: Widgets on the Dashboard

Widget	Description
Alerts Donut Chart	View the total number of alerts grouped by severity level. Click each alert name to view the total number of tenant sites receiving alerts that are critical, major, or minor.
Top 5 POPs with Alerts	View the top five POPs receiving alerts. • **POP**—Name of the POP. • **Tenant**—Number of tenants in the POP. • **Location**—Location of the POP. • **Status**—Type of alerts received that are critical, major or minor.
Top 5 Sites with Alerts	View the top five tenant sites receiving alerts. • **Name**—Name of the tenant site. • **Location**—Location of the tenant site. • **Status**—Type of alerts received that are critical, major, or minor.
Top 5 Tenants with Alerts	View the top five tenants receiving alerts. • **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 on page 4

PART 3

Monitor

- Monitoring Alerts, Alarms, and Device Events on page 23
- Monitoring Tenants SLA Performance on page 33
- Monitoring Jobs on page 49

CHAPTER 4

Monitoring Alerts, Alarms, and Device Events

- About the Monitor Overview Page on page 23
- About the Generated Alerts Page on page 24
- About the SD-WAN Alert Definitions Page on page 25
- Creating SD-WAN Alert Definitions on page 26
- Editing and Deleting SD-WAN Alert Definitions on page 28
- About the Device Events Page on page 29

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 6 on page 24 shows the descriptions of the fields on the Monitor Overview page.

Table 6: 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**.
Only the node with alerts	View the nodes with issues with the service. Click the drop-down list located next to the **Only the nodes with alerts** check box and select the type of alerts. • Critical—Issues that prevent the node from working and require action from the operator. The nodes with critical alerts are displayed in red. • Major—Issues that prevent the node from working at this time, but they do not require action from the operator. The nodes with major alerts are displayed in orange. • Minor—Issues that allow a node to continue working, but not optimally. The network operator may need to take action to resolve the issue. The nodes with minor alerts are displayed in yellow. NOTE: The nodes without any alerts are displayed in blue.

Related Documentation

- *About the Monitor Tenants Page*
- *About the Monitor POPs Page*
- *About the Monitor Sites Page*

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**.
- Select the generated alert and then right-click or click **More > Clear All Selections**.

Field Descriptions

Table 7 on page 25 provides guidelines on using the fields on the Generated Alerts page.

Table 7: Fields on the Generated Alerts Page

Field	Description
Time	View the date and time when the alert was generated.
Alert Name	View the name of the alert.
Alert Description	View the description of the alert.
Alert Source	View the source.
Alert Type	View the type of alert.
Severity	View the severity of the alert.
Tenant	View the name of the tenant.
Site	View the tenant site
Object Type	View the object type
Alert ID	View the alert ID.

Related Documentation

- About the SD-WAN Alert Definitions Page on page 25
- Creating SD-WAN Alert Definitions on page 26
- Editing and Deleting SD-WAN Alert Definitions on page 28

About the SD-WAN Alert Definitions Page

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

You can use the SD-WAN Alert Definitions page to view and manage alert definitions for SD-WAN. 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.
- Create SD-WAN alert definitions. See "Creating SD-WAN Alert Definitions" on page 26.
- Edit or delete an existing SD-WAN alert definition. See "Editing and Deleting SD-WAN Alert Definitions" on page 28.
- Show or hide columns that contain information about SD-WAN 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 8 on page 26 describes the fields on the SD-WAN Alert Definitions page.

Table 8: Fields on the SD-WAN Alert Definitions Page

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.

Related Documentation

- Creating SD-WAN Alert Definitions on page 26.
- Editing and Deleting SD-WAN Alert Definitions on page 28.

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 > SD-WAN Alert Definitions** 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 9 on page 27.

3. Click **OK** to create the alert definition.

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

Table 9 on page 27 describes the fields on the Create SD-WAN Alert Definition page.

Table 9: 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	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: • 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.
Action	Select the action to be performed to resolve issues based on the severity of the alert. You can select one of the following actions: • **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.

Table 9: Fields on the Create SD-WAN Alert Definition Page *(continued)*

Field	Guidelines

Context	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**.
	
	Example:
	
	`{`
	`“broker_ip”: “192.0.2.0”,`
	`“broker_port”: “5672”,`
	`“exchange_name”: “external_alert_exchange”,`
	`“exchange_type”: “topic”,`
	`“user”: “user-name”,`
	`“password”: “password”`
	`}`

Related Documentation

- About the SD-WAN Alert Definitions Page on page 25
- Editing and Deleting SD-WAN Alert Definitions on page 28

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 > SD-WAN Alert Definitions** 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 26.

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 > SD-WAN Alert Definitions** 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 SD-WAN Alert Definitions Page on page 25
- Creating SD-WAN Alert Definitions on page 26

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 operationPress 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, unknonw OR Source IP = 192.168.34.10,192.168.1.26 AND Hostname = dc-srx1400-1,vsrx-75

Field Descriptions

Table 10 on page 30 provides guidelines on using the fields on the Device Events page.

Table 10: 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.

Table 10: Fields on the Device Events Detailed View Page *(continued)*

Field	Description
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.
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.

Table 10: Fields on the Device Events Detailed View Page *(continued)*

Field	Description
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.
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.

CHAPTER 5

Monitoring Tenants SLA Performance

- Multidepartment CPE Device Support on page 33
- About the SLA Performance of All Tenants Page on page 34
- About the SLA Performance of a Single Tenant Page on page 36
- Monitoring Application-Level SLA Performance for real time-optimized SD-WAN on page 40
- Viewing the SLA Performance of a Site on page 41
- Viewing the SLA Performance of an Application or Application Group on page 45
- Understanding SLA Performance Score for Applications, Links, Sites, and Tenants on page 46

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 service provider 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 11 on page 35 describes the fields on the Tenants SLA Performance page.

Table 11: Fields on the Tenants SLA Performance Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance. You can choose between card and grid views. By default, card view is selected.
Performance Threshold	Specify the performance threshold, in percentage, based on which tenants can be classified as tenants with low, medium, or high SLA performance. To set the performance threshold, click **More** > **Performance Threshold**. From the **Performance Threshold** dialog box, move the slider button to set the low and high thresholds. Tenants that have a performance score below the low threshold are marked as having low SLA performance and tenants that exceed the high threshold are marked as having high SLA performance. Tenants that have a performance score between the low and high are considered as having medium SLA performance.
Tenants with Low and Medium Performance	View tenants that have low and medium SLA performance in the selected time period. The low and medium performance classification is done based on the performance threshold you specify. Click each tenant to view information about the SLA performance of the sites in the tenant. See "About the SLA Performance of a Single Tenant Page" on page 36..
Tenants with High Performance	View the tenants that have high SLA performance in the selected time range. Click each tenant to view information about the SLA performance of the sites in the tenant. See "About the SLA Performance of a Single Tenant Page" on page 36.

Table 12 on page 35 describes the fields in the card and grid views.

Table 12: Fields on the Tenants SLA Performance Page

Field	View	Description
Tenant name	Card and Grid	Name of the tenant.
Sites	Card and Grid	Number of sites associated with the tenant.
AppQoE Function	Card and Grid	Shows whether AppQoE is enabled or not. AppQoE is enabled only when the SD-WAN mode is set to Real time-Optimized.
SLA Performance	Card and Grid	Displays the SLA performance score on a scale of 100. Scores that exceed the high performance threshold are displayed in green. Scores that are below the low performance threshold are displayed in red, and the medium scores that are between the low and high performance threshold are displayed in orange. For information about SLA performance score, see "Understanding SLA Performance Score for Applications, Links, Sites, and Tenants" on page 46.

Table 12: Fields on the Tenants SLA Performance Page *(continued)*

Field	View	Description
SLA not met events	Card and Grid	Number of events that failed to meet the SLA.
SLA not met duration	Card and Grid	Total duration of time the sessions on the site failed to meet the SLA. For example, if there were 15 sessions that failed to meet SLA for 10 minutes each on the past one hour, the SLA met duration value would be 150 minutes.
Total sessions	Card and Grid	Total number of sessions during the specified period.
Session switch count	Card and 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 on page 36
- Viewing the SLA Performance of a Site on page 41
- Viewing the SLA Performance of an Application or Application Group on page 45
- Creating SLA Profiles on page 177

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 13 on page 37 describes the fields on the SLA Performance of a Single Tenant page.

Table 13: Fields on the SLA Performance of a Single Tenant Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance for all sites in the tenant. You can choose between card and grid views. By default, card view is selected.
Performance Threshold	Specify the performance threshold based on which sites can be classified as sites with low, medium, or high SLA performance. The performance threshold is specified in percentage terms. To set the performance threshold, click **More** > **Performance Threshold**. From the **Performance Threshold** dialog box, move the slider button to set the low and high thresholds. Site that have a performance score below the low threshold are marked as having low SLA performance and sites that exceed the high threshold are marked as having high SLA performance. Sites that have a performance score between the low and high are considered as having medium SLA performance.

Table 13: Fields on the SLA Performance of a Single Tenant Page *(continued)*

Field	Description
Sites with Low and Medium Performance	View sites that have low and medium SLA performance in the selected time period. The low and medium performance classification is done based on the performance threshold you specify. Click each site to view information about application-level SLA performance. See "Application and Link Level SLA Performance" on page 39.
Sites with High Performance	View the sites that have high SLA performance in the selected time range. Click each site to view information about the application-level SLA performance. See "Application and Link Level SLA Performance" on page 39.

Table 14 on page 38 describes the fields in the card and grid views.

Table 14: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views

Site name	Card and Grid	Name of the tenant.
AppQoE Function	Card and Grid	Shows whether AppQoE is enabled or not. AppQoE is enabled only when the SD-WAN mode is set to Real time-Optimized.
SLA Performance	Card and Grid	Displays the SLA performance score on a scale of 100. Scores that exceed the high performance threshold are displayed in green. Scores that are below the low performance threshold are displayed in red, and the medium scores that are between the low and high performance threshold are displayed in orange. For information about SLA performance score, see "Understanding SLA Performance Score for Applications, Links, Sites, and Tenants" on page 46.
SLA not met events	Card and Grid	Number of events that failed to meet the SLA.
SLA not met duration	Card and Grid	Total duration of time the sessions on the site that failed to meet the SLA. For example, if there were 15 sessions that failed to meet SLA for 10 minutes each on the past one hour, the SLA met duration value would be 150 minutes.
Total sessions	Card and Grid	Total number of sessions during the specified period.
Session switch count	Card and Grid	Number of instances when a session switch occurred because of non-compliance with SLA.
Total tenant traffic	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 15 on page 39 describes the fields on the SLA Performance of a Single Tenant page.

Table 15: Fields on the SLA Performance of a Single Tenant Page

Field	Description
Time range	Select the time range for which you want to view the SLA performance. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.
View	Select the view in which you want to display the SLA performance. You can choose between graph and grid views. By default, graph view is selected.
View App Names	Select this check box to view the names of the applications in the graph view.
Top 10 applications	Select this check box to see the top 10 applications.
Application SLA Performance	
Departments	Select All Departments to view application SLA data for all departments, or select one department to view application SLA data specific to that department. By default, All Departments is selected.
SLA Parameters	Choose one of the following SLA parameters based on which you want to view the application SLA performance data: • Throughput • Latency metric • Packet loss • Jitter metric By default, Throughput is selected. The data for the selected parameter is displayed in the y-axis in the scatter plot view.
Group by	Select whether you want to group the applications based on the SLA Profile or the Traffic Type. By default, the SLA Profile option is selected.
SLA Profile	If you selected **SLA Profile** for **Group by**, select the SLA Profile for which you want to view the SLA performance information. This option is available only if you selected **SLA Profile** for **Group by**.
Traffic Type	If you selected **Traffic Type** for **Group by**, select the **Traffic Type** for which you want to view the SLA performance information. This option is available only if you selected **Traffic Type** for **Group by**.

Table 15: Fields on the SLA Performance of a Single Tenant Page *(continued)*

Field	Description
Graph	Select whether you want to view the SLA performance information for applications in the **Scatter Plot** view or in **Tree Graph** view. By default, **Scatter Plot** is selected.
Link SLA Performance	
Traffic Type	Select the traffic type for which you want to view the link SLA performance. You can choose either **All Traffic Type** or one of the available traffic types.
Links	Select the links for which you want to view the SLA performance. You can choose either **All Links** or one of the available links.

Related Documentation

- About the SLA Performance of All Tenants Page on page 34
- Viewing the SLA Performance of a Site on page 41
- Viewing the SLA Performance of an Application or Application Group on page 45
- Creating SLA Profiles on page 177

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.

I

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 46.

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 on page 40
2. Viewing SLA Performance of Sites on page 41

Viewing SLA Performance of Tenants

Service provider 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 34 page appears.

2. Customize the view to your specific requirements.

   For customization options, see Table 11 on page 35

   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 12 on page 35

Viewing SLA Performance of Sites

Service provider 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 36.

2. Customize the view as required. For more information about the customization options, see Table 13 on page 37

   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 14 on page 38.

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 15 on page 39.

Viewing the SLA Performance of a Site

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 on page 42
- Applications SLA Performance by Throughput on page 42
- SLA Performance for ALL on page 44

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 45.

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 16 on page 43 describes the fields on the Applications SLA Performance by Throughput grid view.

Table 16: 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.

Table 16: Fields on the Applications SLA Performance by Throughput Grid View *(continued)*

Field	Description
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 45.

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 "Application SLA Profiles" on page 176 page.

Related Documentation

- About the SLA Performance of All Tenants Page on page 34
- About the SLA Performance of a Single Tenant Page on page 36
- Viewing the SLA Performance of an Application or Application Group on page 45

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 17 on page 45 describes the fields on the application or application group SLA Performance details page.

Table 17: 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.

Table 17: Fields on the Application or Application Group Details Page *(continued)*

Field	Description
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.
Global SLA Profile Performance	View the performance for all the SLA parameters of the SLA profile associated with the application or application group. The SLA performance is represented by a color-coded donut chart. The section in blue in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were met. The section in red in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were not met. Click the red colored section of the donut chart to view more information about when SLA requirements for the SLA profile were not met. The **SLA Profile Performance** page appears. The SLA Profile Performance page displays the following fields: • SLA Profile—SLA profile associated with the application or application group • Target—Target throughput configured in the SLA profile • SLAs Not Met—Percentage of time SLA requirements were not met for the SLA profile • Sessions—Number of sessions consumed by the application or application group • Start Time—Time at which the WAN links associated with the application or application groups started to fail meeting the SLA requirements • End Time—Time at which SLA profile requirements started to be met again • Avg Val—Average throughput (in Mbps) when the SLA requirements started to fail • Duration—Total duration (in seconds) during which SLA requirements were not met • From—Source WAN link • To—Destination WAN link

Related Documentation

- About the SLA Performance of All Tenants Page on page 34
- About the SLA Performance of a Single Tenant Page on page 36
- Viewing the SLA Performance of a Site on page 41

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

This topic explains the following SLA performance scores:

- Application Score on page 46
- Site Score on page 47
- Tenant Score on page 47
- Link Score on page 47

Application Score

From Release 3.3 onward, 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 46.

The site score for bandwidth-optimized networks is calculated as an average of "Link Score" on page 47.

Tenant Score

Tenant score is calculated as the average value of site scores. For information about site score calculation, see "Site Score" on page 47.

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.

CHAPTER 6

Monitoring Jobs

- About the Jobs Page on page 49
- Viewing Job Details on page 51
- Editing and Deleting Scheduled Jobs on page 51
- Retrying a Failed Job on Devices on page 52

About the Jobs Page

To access this page, click **Monitor > Jobs**.

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 51.
- Retry a job. See "Retrying a Failed Job on Devices" on page 52.
- Edit and delete schedule jobs. See "Editing and Deleting Scheduled Jobs" on page 51.

Field Descriptions

Table 18 on page 49 provides guidelines on using the fields on the Jobs page.

Table 18: Fields on the Jobs Page

Field	Description
Job Name	View the name of the job. Example: MSEC_DOWNLOAD_IPS/APPLICATION_SIGNATURES_08_Jul_17_124229_024
Resource Name	View the resource name of the job. Example: Download IPS/Application Signatures

Table 18: Fields on the Jobs Page *(continued)*

Field	Description
Status	View the status of the job to know whether the job succeeded or failed. Example: Success
Owner	View the name of the owner who created the job. Example: cspadmin
Number of Tasks	View the number of tasks associated with the job. Example: 2 For example, the tasks **site.ucpe-32** and **customer.sdwan** are associated with this job.
Job Type	View the job type. Example: tssm import pop
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 19 on page 50 provides guidelines on using the fields on the Scheduled Jobs page.

Table 19: Fields on the Scheduled Jobs Page

Field	Description
Schedule ID	View the unique ID of the scheduled job. The value is generated by the database when a new schedule record is inserted into the database. Example: 48
Name	View the unique name of the scheduled job. Example: Tenant Delete_csp.tssm_remove_site_e340354716ae43859fad5ba15669eee2
Status	View the status of the last triggered job. The following state are available: scheduled, In progress, complete, or failed. The default status is scheduled.
Job Type	View the job type. Example: tssm onboard tenant
Owner	View the name of the owner who scheduled the job. Example: cspadmin

Table 19: Fields on the Scheduled Jobs Page *(continued)*

Field	Description
Next Run Time	View the time when the job is scheduled to run next.

Related Documentation

- Editing and Deleting Scheduled Jobs on page 51
- Retrying a Failed Job on Devices on page 52

Viewing Job Details

You can use the Detailed View page to view all the parameters of a job.

To view details of a job:

- Right-click the job name that you want to see the detailed view for and select **Detail View**, or 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 Detailed View page appears, showing the details of the job and the number of tasks associated with the job. See the relevant topic *About the Jobs Page* for a description of the fields on these pages.

Related Documentation

- About the Jobs Page on page 49

Editing and Deleting Scheduled Jobs

You can edit and delete scheduled jobs. This topic contains the following sections:

- Editing Scheduled Jobs on page 51
- Deleting Scheduled Jobs on page 52

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 Scheduled Jobs page appears.

2. Select the job that you want to reschedule the deployment, and click the edit icon.

   The Edit Schedule page appears.

3. To execute the job immediately, delete the existing scheduled entry, create a new entry, and then select the **Run now** option. To reschedule the job for a later date and time, or select the **Schedule at a later time** option.

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

   The modified job and its details are displayed on a page

Deleting Scheduled Jobs

You can delete one or more scheduled jobs.

To delete a scheduled job:

1. Select **Monitor > Jobs> Scheduled Jobs**.

   The Scheduled Jobs page appears with a list of jobs.

2. Select the check box of the job that you want to delete and then click the delete icon (X).

   The Confirm Delete page appears.

3. Click **Yes** to confirm.

   The scheduled job is deleted.

Related Documentation

- About the Jobs Page on page 49
- Viewing Job Details on page 51

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 and it is available only for All Tenants scope.**

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 on page 49
- Editing and Deleting Scheduled Jobs on page 51

PART 4

Resources

- Managing POPs on page 57
- Managing Devices on page 97
- Managing Device Templates on page 115
- Managing Software Images on page 131

CHAPTER 7

Managing POPs

- About the POPs Page on page 57
- Creating a Single POP on page 59
- Importing Data for Multiple POPs on page 70
- Viewing the History of POP Data Imports on page 75
- Viewing the History of POP Data Deletions on page 77
- Managing a Single POP on page 78
- About the VIMs Page on page 79
- Creating a Cloud VIM on page 81
- About the EMS Page on page 85
- Creating an EMS on page 86
- Changing the Junos Space Virtual Appliance Password on page 87
- About the Routers Page on page 88
- Creating Devices on page 89
- Configuring Devices on page 91
- View the History of Device Data Deletions on page 94

About the POPs Page

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

You can use the POPs page to view the list of available POPs in the service provider 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:

- Quickly view important data about POPs in the widgets that appear at the top of the page. See Table 20 on page 58.
- Create a POP. See "Creating a Single POP" on page 59.
- Import data for multiple POPs. See "Importing Data for Multiple POPs" on page 70.

- View the history of POP data imports. See "Viewing the History of POP Data Imports" on page 75.
- View the history of POP data deletions. See "Viewing the History of POP Data Deletions" on page 77.
- View details about a POP. Hover over the name of a POP or click **More** > **Quick View**. See "Viewing Object Details" on page 14.
- Show or hide columns about the POPs. See "Sorting Objects" on page 15.
- Search an object about the POPs. See "Searching for Text in an Object Data Table" on page 15.
- Delete a POP. See "Deleting Objects" on page 14.

Field Descriptions

Table 20 on page 58 describes the widgets on the POPs page.

Table 20: Widgets on the POPs Page

Widget	Description
Top POPs by CPU Allocation	View the top three POPs using the largest percentage of CPU from the assigned cores. Click a POP name to view detailed information about the resources the POP uses.
Top POPs by Storage Allocation	View the top three POPs using the most storage from the allocated storage space in gigabytes (GB). Click a POP name to view detailed information about the resources the POP uses.
Top POPs by Memory Allocation	View the top three POPs using the most memory from the allocated memory size in megabytes (MB). Click a POP name to view detailed information about the resources the POP uses.

Table 21 on page 58 shows the fields on the POPs page.

Table 21: Fields on the POPs Page

Field	Description
Name	View the name of the POP. Example: regional
Location	View the location of the POP. Example: Sunnyvale, CA
CPU Allocated	View the amount of CPU allocated for the POP.

Table 21: Fields on the POPs Page *(continued)*

Field	Description
Memory Allocated	View the amount of memory allocated for the POP.
Storage Allocated	View the amount of storage allocated for the POP.
VIMs	View the number of VIMs provisioned in the POP. • 0—Either a distributed deployment or a centralized deployment for which you have not yet configured a VIM. 1—Centralized deployment Example: 1
EMS	View the number of EMS applications provisioned in the POP. Example: 2
Routers	View the number of routers provisioned in the POP. Example: 1
Tenants	View the list of tenants in the POP. Example: Softbank, ATT, and Juniper
Sites	View the number of tenant sites in the POP. Example: 4

Related Documentation

- Creating a Single POP on page 59
- About the VIMs Page on page 79
- About the EMS Page on page 85
- About the Routers Page on page 88

Creating a Single POP

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

Creating a single POP involves adding several types of objects, depending on whether the POP is for a centralized or distributed deployment. The sections in this topic describe how to add each type of object to a POP in Administration Portal. You must finish the

steps in each section to create the objects that you need for a single POP and to save the POP successfully. This topic includes the following sections:

- Adding Information About the POP on page 60
- Adding a Device on page 61
- Adding a VIM on page 64
- Adding an EMS on page 68
- Reviewing and Saving the POP Configuration Settings on page 69

Adding Information About the POP

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

1. Click **Resources > POPs**.

   The POPs page appears.

2. Click the plus icon(+) .

   The Add POP page appears.

3. Complete the configuration settings according to the guidelines provided in Table 22 on page 60.

4. Click **Next** and proceed to "Adding a Device".

   The Add Device table appears.

Table 22: Fields on the Add POP page

Field	Description
Region	Regions are used to group services for various business reasons such as location, proximity, service distribution and load. • For a centralized deployment, select the region that you want to use to manage services in the POP; the default is regional. NOTE: The regions are configured during CSO installation. For a distributed deployment, the default region is selected and cannot be modified. Example: regional NOTE: The administrator must not delete the region name.
POP Name	Enter the name of the POP. You can use an unlimited number of alphanumeric characters, including special characters. Example: north-east.

Table 22: Fields on the Add POP page *(continued)*

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

Adding a Device

You can add the following devices to a POP:

- A router that acts as an SDN gateway and provides a Layer 3 routing service to customer sites for a centralized deployment.
- A router that acts as a provider edge (PE) router and an IPsec concentrator for a distributed deployment.

To add a device:

1. Click **Resources > POPs > +** .

   The Add POP page appears.

2. Complete the configuration settings according to the guidelines provided in Table 22 on page 60.

3. Click **Next**.

   The Device section appears.

4. Click the plus icon (+) in the Add Device section.

   The Add Device page appears.

5. Complete the configuration according to the guidelines in Table 23 on page 62.

6. Click **Save**.

7. Proceed as follows:
   - For a centralized deployment, click **Next** and proceed to "Adding a VIM".
   - For a distributed deployment, click **5 (Summary)** and proceed to "Reviewing and Saving the POP Configuration Settings" on page 69.

Table 23: Fields on the Add Device Page

Field	Description
Name	Enter the name of the device, such as a data center gateway, a PE router, or an IPsec concentrator. Some device examples are listed below. • An MX Series router used as an SDN gateway in a centralized deployment. • An MX Series router used as a provider edge (PE) router in a distributed deployment. • An SRX Services Gateway router or a vSRX instance used as a CPE device in a distributed deployment. You can use letters, numbers, spaces, periods, dashes, underscores, commas, @, #, $, %, &, and *. Maximum length is 255 characters. Example: MX-router-10
Family	Select the product family for the device. Example: MX

Table 23: Fields on the Add Device Page *(continued)*

Field	Description
Device Template	Select the name of the device template for the device: • Juniper-MX-MIS—Customized device template for an MX Series router that prevents the creation of black holes when an administrative user activates a service at a site. Select this option only if you have been advised to do so by Juniper Networks. • SDN-GW-MX—Default template for MX Series router. Select this option for MX routers in centralized and distributed deployments unless Juniper Networks advises use of the *Juniper-MX-MIS* device template. • SRX_Basic_SDWAN_HUB—Device template for an SRX Services Gateway used as a CPE device that offers basic SD-WAN functionality in a distributed deployment. Select this option only if you have been advised to do so by Juniper Networks. • SRX_deployment_option_1—Device template for an SRX Services Gateway or a vSRX used as a CPE device in a distributed deployment. • NFX_deployment_option_1—Device template for an NFX device in distributed deployment. This template supports port-forwarding with Contrail Service Orchestration initiated connection. • SRX_Managed_Internet_CPE—Device template to manage an SRX Services Gateway devices for a managed internet service. • NFX_Managed_Internet_CPE—Device template to manage an NFX device for a managed internet service. • NFX_deployment_option_4—Device template for an NFX device in distributed deployment. This template supports outbound SSH, which is the device initiated connection, with port-forwarding capability. • vSRX-VNF-NFX—Device template for a vSRX VNF application on an NFX platform for a distributed deployment.
Type of Device	Select the type of device: • PNE—Device is managed by the EMS. Use this option for devices, such as data center gateway, in a centralized deployment, for an SRX Services Gateway or a vSRX used as a CPE device in a distributed deployment, and for PE routers in a distributed deployment that you want the EMS to manage. • PE/IPsec—Device is not managed by the EMS. Use this option for devices, such as provider edge (PE) router or IPsec concentrator, in a distributed deployment that you do not want the EMS to manage.
PNE package	If you specified that the device is a PNE for a centralized deployment, select the name of the package that contains metadata and configuration instructions for the PNE: • SRX—Use with SRX Series device template. • Juniper-MX—Use with the SDN-GW-MX device template. • Juniper-MX-MIS—Customized device template with MX Series configuration that prevents the creation of black holes when an administrative user activates a service at a site. Use with the Juniper-MX-MIS device template. You must specify the PNE package only for data center gateway device. Do not use the SRX Series package for the MX router.

Table 23: Fields on the Add Device Page *(continued)*

Field	Description
Management Type	Specify the management type for the PE device. The following options are available: • Managed—Select Managed if you use Contrail Service Orchestration to manage the device. • Unmanaged—Select Unmanaged if you use another application to manage the device. Example: Unmanaged
Device IP	Enter the IPv4 address of the management interface for the device. Example: 192.0.2.15
Internet Gateway (optional)	If you specified that the device is a PE router or an IPsec concentrator for a distributed deployment, then specify the IPv4 address of the Internet gateway. You can also specify a list of public IP addresses of the Internet Key Exchange (IKE) gateways on this device. Example: 192.0.2.20
User Name	You must enter the username that you configured when you set up the device. You use this username to log into the device. Providing login credentials gives Contrail Service Orchestration access to the device.
Password	Enter the password that you configured when you set up the device. You use this password to log into for the device. Providing login credentials gives Contrail Service Orchestration access to the device.

Adding a VIM

For a centralized deployment, you must specify information about Contrail Cloud Platform, which provides the VIM.

You must add a VIM for a centralized deployment. Do not add a VIM for a distributed deployment.

To add a VIM:

1. Click **Resources** > **POPs** > **+** .

   The Add POP page appears.

2. Complete the configuration settings according to the guidelines provided in Table 22 on page 60.

3. Click **Next**.

   The Device section appears.

4. Click **Next**.

   The VIM page appears.

5. In the Connection Information section, specify details for the Contrail Cloud Platform that provides the VIM for this POP.

6. Complete the configuration according to the guidelines in Table 24 on page 65.

7. In the Network Information section, click the plus icon (+) to add each resource pool.

8. In the Network Information section, specify details for the management network in Contrail.

   You can either specify details for a management network that you already created in Contrail or specify details for a new management network that Administration Portal notifies Contrail to automatically create.

9. If this POP has a direct connection to the Internet, in the Internet Network section, click the plus icon (+) icon to add information about the Internet network in Contrail.

10. Click **Save**.

11. Proceed as follows:

    - If you use virtualized network functions (VNFs) that require an EMS other than the EMS microservice, click **Next** and proceed to "Adding an EMS".
    - If you do not need an additional EMS, click **5 (Summary)** and proceed to "Reviewing and Saving the POP Configuration Settings" on page 69.

Table 24: Fields on the Add Cloud VIM Page

Field	Guidelines
Name	Enter the name of the virtualized infrastructure manager (VIM) for a centralized deployment. You can add multiple VIMs to a point of presence (POP). You can use letters, numbers, spaces, periods, dashes, underscores, commas, @, #, $, %, &, and *. Maximum length is 255 characters. Example: vcpe-vim
Type	View the VIM type. The default VIM type is cloud. Example: Cloud
Connection Information	
IP address	Enter the IPv4 address of the Contrail Controller node in the Contrail Cloud Platform that provides the virtualized infrastructure manager (VIM). If you use a high availability (HA) configuration for the Contrail Cloud Platform, specify the virtual IP address of the Contrail Controller node. Example: 10.102.28.36

Table 24: Fields on the Add Cloud VIM Page *(continued)*

Field	Guidelines
Auth URL	Enter the authentication URL for the OpenStack Keystone. Example: http://ip:5000/v3
User Name	Enter the OpenStack Keystone username that you configured. Example: admin
Password	Enter the OpenStack Keystone password that you configured. Example: contrail123
Domain	Enter the name of the OpenStack domain that you configured. Example: default
Tenant	Enter the name of the OpenStack tenant that you configured. Example: admin
Network Information *Resource Pools*	
Resource Pool Name	Enter a resource pool for each VIM. You can use an unlimited number of alphanumeric characters, including special characters. Example: north-east.
Compute Zone	Enter the availability zone in Contrail OpenStack in which the virtual machines for network services reside. The default availability zone is nova. You can run the **nova availability-zone-list** command on the Contrail OpenStack to find the list of available zones. Example: nova
Does Management Network Exists?	Select whether to use an existing virtual network in Contrail OpenStack or to create a new one. • yes—Import the named virtual network from Contrail OpenStack. • no—Create a virtual network in Contrail OpenStack with the specified name.
Management Network Name	Enter the name of the existing management network in Contrail or the new management network that you want to create in Contrail. Example: mgmt-net
Management Network Information	

Table 24: Fields on the Add Cloud VIM Page *(continued)*

Field	Guidelines
Route Target	Specify one or more route targets for the existing management network in Contrail or the new management network that you want to create in Contrail. Example: 64512:10000.
Subnet	Specify one or more prefixes that define the subnets for the Contrail Compute nodes. You can use an IPv4 address. Specify one or more IPv4 prefixes for the existing network in Contrail or the new network that you want to create in Contrail. Example: 192.0.2.0/24.
Internet Network Information	
Network Name	Enter the name of the Internet network . Example: int-net
Does Exist	Specify whether to use an existing virtual network in Contrail OpenStack or to create a new one. • True—Import the named virtual network from Contrail OpenStack. • False—Create a virtual network in Contrail OpenStack with the specified name.
Route Target	Select the route target for the internet network in Contrail. Example: 64512:10000.
Subnet	Select the prefix that defines the subnet for the Contrail Compute nodes. You can use an IPv4 address. Example: 192.0.2.0/24.
Service Profile Information	
Profile Name	Enter the name of the service profile in a VIM instance. Create one or more service profiles if you use a dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment. A service profile specifies the Contrail OpenStack tenant, domain, and login credentials. After Contrail Service Orchestration authenticates a tenant (customer), it uses the information in the service profile to provide access to Contrail OpenStack. Example: vim-service-profile
Tenant Name	Enter the name of the infra tenant for whom you want to assign the service profile. Example:test-tenant
Domain Name	Enter the Infra domain name. Example:Default

Table 24: Fields on the Add Cloud VIM Page *(continued)*

Field	Guidelines
User Name	Enter the username of the tenant. Example: admin
Password	Enter the password for the tenant user. Example: password123
Default Service Profile	Select the name of the default service profile if you use a dedicated OpenStack Keystone for Contrail Service Orchestration. If you do not specify a service profile when you configure the tenant, Contrail Service Orchestration uses the default profile to authenticate the tenant. Example: default-service-profile

Adding an EMS

Configure an element management system (EMS) if you use virtualized network functions (VNFs) that require an EMS other than the EMS microservice.

To add an EMS:

1. Click **Resources** > **POPs** > **+** .

   The Add POP page appears.

2. Complete the configuration settings according to the guidelines provided in Table 22 on page 60.

3. Click **Next**.

   The Device section appears.

4. Click **Next**.

   The VIM page appears.

5. Click **Next**.

   The EMS page appears.

6. Click the plus icon (+) to add the EMS.

7. Complete the configuration according to the guidelines in Table 25 on page 69.

8. Click **Save**.

9. Click **Next** to review the configuration settings for the POP.

Table 25: Fields on the Add EMS Page

Field	Guidelines
Name	Name of the EMS. This field is auto-populated with the name that you specified when you deployed the Junos Space Virtual Appliance. Example: Junos Space
IP	Enter the IPv4 address of the Junos Space Web user interface (UI). For a redundant Contrail Service Orchestration, configure the IP address of the Web UI for the primary Junos Space Virtual Appliance. Example: 192.0.2.3.
Vendor	Enter the vendor name for the EMS. Example: Juniper Networks
Version	Enter the version number of the EMS. The default version is 15.1. Example: 15.1
Authentication URL	Enter the authentication URL for the EMS application.
User Name	Enter the username of the device administrator that you configured. This user should be assigned the admin role in all the tenants. The default username is super. Example: super
Password	Enter the administrator password that you configured. The default password is juniper123. Example: juniper123

Reviewing and Saving the POP Configuration Settings

After you have configured a POP and its associated resources, you can review and save a copy of the configuration settings. Finally, you must save the POP that you configured.

1. Click **Resources** > **POPs** > **+** .

   The Add POP page appears.

2. Complete the configuration settings according to the guidelines provided in Table 22 on page 60.

3. Click **Next**.

   The Device section appears.

4. Click **Next**.

   The VIM page appears.

5. Click **Next**.

   The EMS page appears.

6. Click **Next**.

   The Summary page appears.

7. Click **Summary** > **Edit** to edit the configuration settings of the objects that you configured.

8. Click **Download POP Payload** to save a JSON file of the configuration settings of the objects that you configured.

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

Related Documentation

- About the POPs Page on page 57
- About the EMS Page on page 85
- About the VIMs Page on page 79
- About the Routers Page on page 88

Importing Data for Multiple POPs

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

- Customizing a POP Data File on page 70
- Uploading a POP Data File on page 74

Customizing a POP Data File

To customize a POP data file:

1. Select **Resources** > **POPs**.

2. Click **Import POPs** > **Import**.

   The Import POPs page appears.

3. Click the **Download Sample JSON** link to open and save the sample JSON data file.

   The sample file opens at the bottom of the page.

4. Save the file to your computer with an appropriate name.

   Example: sample-pop-data.json

   NOTE: **You need to retain the file format as .json to successfully upload the POP details to the Administration Portal.**

5. Customize the sample JSON file using the guidelines in Table 26 on page 71.

6. Save the customized file.

Table 26: Fields on the POPs Page

Field	Description
POP Information	
dc_name	Specify the name of the region for this POP. Example: regional NOTE: Administrator should not delete the region name.
name	Specify the name of the POP. You can use an unlimited number of alphanumeric characters, including special characters. Example: pne-pop10
street	Specify the street address. Example: 1133 Innovation Way
city	Specify the name of the city. Example: Sunnyvale.
state	Specify the name of the state. Example: CA
zip_code	Specify the zip code or postal code for the state. Example: 94089.
country	Specify the name of the country. Example: USA
VIM Information NOTE: You must add a VIM for a centralized deployment. Do not add a VIM for a distributed deployment.	

Table 26: Fields on the POPs Page *(continued)*

Field	Description
name	Specify the name of the VIM instance. You can use an unlimited number of alphanumeric characters, including special characters. Example: vim10
vim_type	Specify the VIM instance type. The default VIM type is cloud. Example: cloud
address	Specify the IP address of the primary Contrail Configure and Control node for the Contrail Cloud Reference Architecture (CCRA) for this POP. Example: 10.102.28.148
auth_url	Specify the authentication URL for the OpenStack Keystone. Example: http://10.102.28.148:5000/v3
default_domain	Specify the name of the OpenStack domain that you configured. Example: Default.
password	Specify the OpenStack Keystone password that you configured. Example: contrail123
default_tenant	Specify the name of the OpenStack tenant that you configured. Example: admin
username	Specify the OpenStack Keystone username that you configured. Example: admin
Resource Pool	
name	Specify a resource pool for each VIM. You can use an unlimited number of alphanumeric characters, including special characters. Example: ResoucePool123
compute_zone	Specify the availability zone in Contrail OpenStack in which the VMs for network services reside. The default availability zone is nova. You can run the **nova availability-zone-list** command on the Contrail OpenStack to find the list of available zones. Example: nova
Management Network	

Table 26: Fields on the POPs Page *(continued)*

Field	Description
vld_name	Specify the name of the virtual link descriptor for the management network. The default name is mgmt. Example: mgmt
vl_name	Specify the name of the management network in Contrail. Example: mgmt-net
onboard	Specify the onboard value for the management network. • true—Import named virtual network object from VIM. • false—Create a virtual network in VIM with the specified name.
route_target	Select the route target for the management network in Contrail. Example: 8887:887
subnet	Specify one or more prefixes that define the subnets for the Contrail Compute nodes. You can use an IPv4 address. Example: 10.102.82.0/23
EMS Information	
name	Specify the name of the EMS application. Example: Junos Space
ip	Specify the IP address of the Junos Space Web user interface (UI). For a redundant Contrail Service Orchestration, configure the IP address of the Web UI for the primary Junos Space Virtual Appliance. Example: 10.102.86.12
username	Specify the username of the device administrator that you configured. This user should be assigned the admin role in all the tenants. The default username is super. Example: super
password	Specify the administrator password that you configured. The default password is juniper123. You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters. Example: juniper123
vendor	Specify the vendor for the EMS. Example: Juniper Networks

Table 26: Fields on the POPs Page *(continued)*

Field	Description
version	Specify the version number of the EMS. Example: 15.1
Device Information	
name	Specify the name of the device, such as a physical network element (PNE) for a centralized deployment. You can use any number of alphanumeric characters, including special characters. Example: PNE-MX10
device_ip	Specify the management IP address of the device. Example: 192.0.2.15.
pne_package	Specify the name of the package providing metadata and configuration templates needed to program a PNE device for service chain attachments in the case of a vCSO solution. If you configure a PNE for the POP in a centralized deployment, select a software image from the menu: • SDN-GW-MX—Default for MX Series router. Select this option for most installations. • Juniper-MX-MIS—Customized device profile with MX configuration that prevents the creation of black holes when an administrative user activates a service at a site. You must specify the PNE package only for a data center gateway device. Do not use the SRX Series package for the PE router or the SDN gateway.
assigned_device_profile	Select the name of the configuration image for the SDN gateway or the PE router. • SDN-GW-MX—Default for MX Series router. Select this option for most centralized deployments and for all distributed deployments. • Juniper-MX-MIS—Customized device profile with MX Series configuration that prevents the creation of black holes when an administrative user activates a service at a site. • SRX_Basic_SDWAN_HUB—Device profile for an SRX Services Gateway used as a CPE device that offers basic SD-WAN functionality in a distributed deployment. Select this option only if you have been advised to do so by Juniper Networks.
username	Specify the username of the device administrator for logging into the device. Example: root
password	Specify the password for logging into the device. Example: pwd123

Uploading a POP Data File

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

To upload a POP data file:

1. Select **Resources > POPs**.

2. Click **Import POPs > Import**.

   The Import POPs page appears.

3. Click **Browse** and navigate to the directory containing the POP data file.

4. Select the file and click **Open**.

5. Click **Import**. If you want to discard the import process, click **Cancel** instead.

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

See Also

- Creating a Single POP on page 59
- Viewing the History of POP Data Imports on page 75
- Viewing the History of POP Data Deletions on page 77

Viewing the History of POP Data Imports

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

To import your POP data, see "Importing Data for Multiple POPs" on page 70.

To view the history of imported POP data:

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

   The Import History page is displayed. Table 27 on page 76 describes the fields on the Import History page.

2. Click a task name.

   The Import POPs Tasks page appears. Table 28 on page 76 describes the fields on the Import Task page.

3. Click the Task ID.

   The Job Status page appears. Table 29 on page 76 describes the fields on the Job Status page.

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

Table 27: Fields on the Import History Page

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

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

Table 29: Fields on the Job Status Page

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

Related Documentation

- Importing Data for Multiple POPs on page 70
- Viewing the History of POP Data Deletions on page 77

Viewing the History of POP Data Deletions

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

To view the history of deleted POP data:

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

   The Delete History page is displayed. Table 30 on page 77 describes the fields on the Delete History page.

2. Click a task name.

   The Delete POPs Tasks page appears. Table 31 on page 77 describes the fields on the Delete Task page.

3. Click the Task ID.

   The Job Status page appears. Table 32 on page 78 describes the fields on the Job Status page.

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

Table 30: Fields on the Delete History Page

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

Table 31: Fields on the Delete POPs Tasks Page

Field	Description
Success	View the number of times the delete operations has been successful for a POP.

Table 31: Fields on the Delete POPs Tasks Page *(continued)*

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

Table 32: Fields on the Job Status Page

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

Related Documentation

- Importing Data for Multiple POPs on page 70
- Viewing the History of POP Data Imports on page 75

Managing a Single POP

Use the tabs on this page to view and manage resources for this POP.

- About the VIMs Page on page 79
- About the EMS Page on page 85
- About the Routers Page on page 88

Related Documentation

- About the POPs Page on page 57
- Creating a Single POP on page 59

About the VIMs Page

To access this page, click **Resources** > **POPs** > ***POP Name*** > **VIMs**.

You can use the VIMs page to create a virtualized infrastructure manager (VIM) and to view information about VIMs provisioned in the POP. The VIM in a Network Functions Virtualization (NFV) implementation manages the hardware and software resources that the service provider uses to create service chains and deliver network services to customers.

Tasks You Can Perform

You can perform the following tasks from this page:

- Quickly view important data about VIMs created for POPs in the widgets that appear at the top of the page. See Table 33 on page 79.
- Create a Cloud VIM. See "Creating a Cloud VIM" on page 81.
- Select a different POP from the drop-down list above the top left of the table to view the VIM details in grid view.
- View details about a VIM. Click the details icon that appears when you hover over the name of a VIM instance. See "Viewing Object Details" on page 14.
- Show or hide columns about the VIMs. See "Sorting Objects" on page 15.
- Search an object about the VIMs. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

- Table 33 on page 79 describes the widgets on the VIMs page.
- Table 34 on page 79 shows the fields on the VIMs page.

Table 33: Widgets on the VIMs Page

Widget	Description
Top VIMs by CPU Allocation	View the top VIMs using the largest percentage of CPU from the assigned cores.
Top VIMs by Storage Allocation	View the top VIMs using the most storage from the allocated storage space in gigabytes(GB).
Top VIMs by Memory Allocation	View the top VIMs using the most memory from the allocated memory size in megabytes IMB).

Table 34: Fields on the VIMs Page

Field	Description
Name	View the name of the VIM in the POP.

Table 34: Fields on the VIMs Page *(continued)*

Field	Description
IP Address	View the IP address of the primary Contrail Configure and Control node for the Contrail Cloud Reference Architecture (CCRA) for this POP.
CPU Allocated	View the amount of CPU cores allocated to the POP by the VIM.
Memory Allocated	View the amount of memory allocated to the POP by the VIM.
Storage Allocated	View the amount of storage allocated to the POP by the VIM.
Domains	View the name of the OpenStack domain that you configured.
Vendor	View the vendor name of the VIM instance.
URL	View the uniform resource locator (URL) for the OpenStack Keystone.
Tenants	View the number of OpenStack tenants in the POP.

Related Documentation

- About the POPs Page on page 57
- About the VIMs Page on page 79
- About the Routers Page on page 88
- Creating a Single POP on page 59

Creating a Cloud VIM

You can use the VIMs page to create virtualized infrastructure managers (VIMs) for each POP in the network. You create one VIM object for each POP in your network. Although the Contrail Cloud Reference Architecture (CCRA) provides a VIM, when you create a VIM you can specify several Contrail OpenStack settings. See Table 35 on page 82.

You can only create a VIM for a centralized deployment. A distributed deployment has a default VIM that is created when the deployment is installed.

There are two authentication methods, namely, CSO Keystone (Central Keystone) authentication and independent VIM Instances's keystone (also known as *regional keystone*) authentication. Customers can authenticate and authorize their own system through OpenStack. Customers have to configure service profiles as a part of VIM and associate it with a tenant.

For example, consider **ABC** as a service provider and **customer-a** as the tenant for ABC. The workflow for associating the service profile with the tenant is listed below:

1. The **cspadmin** configures the POP (vim-instance and domain creations) along with vim-service-profiles when configuring the vim-instance. The vim-service-profiles contains the respective VIM's infra tenant details.

2. Configure ABC data center as a VIM.

3. ABC admin configures customer-a along with service-profile-name. This enables VIM microservice to map customer-a to equivalent infra tenant as specified in service-profile-name.

4. ABC admin, ABC tenant details, customer-a tenant, and customer-a account details are present in CSO Keystone (Central Keystone), while infra tenant details that are available as part of vim-service-profile is present only in regional keystone.

5. When creating a service, customer-a instantiates a network service. The customer-a's request is received at NSO with customer-a's authentication token from the regional VIM keystone.

6. Based on tenant-name customer-a, the VIM region maps to "admin" infra tenant, because when configuring "customer-a " tenant, the service-profile-name with admin was provided.

7. VIM regional microservice can now use the infra tenant for its service instantiation activities.

To create a VIM in the cloud:

1. Click **Resources** > **POPs** > ***POP Name*** > **VIMs**.

2. Click the plus icon(+).

   The Add Cloud VIM page appears.

3. Configure the fields using the information provided in Table 35 on page 82.

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

Table 35: Fields on the Add Cloud VIM Page

Field	Guidelines
Name	Specify the name of the virtualized infrastructure manager (VIM) for a centralized deployment. You can add multiple VIMs to a point of presence (POP). You can use letters, numbers, spaces, periods, dashes, underscores, commas, @, #, $, %, &, and *. Maximum length is 255 characters. . Example: vcpe-vim
Type	View the VIM type. The default VIM type is cloud. Example: Cloud
Connection Information	
IP address	Specify the IP address of the Contrail Controller node in the Contrail Cloud Platform that provides the virtualized infrastructure manager (VIM). Example: 10.102.28.36
Auth URL	Specify the authentication URL for the Contrail OpenStack Keystone. Example: http://ip:5000/v3
User Name	Specify the username for logging into Contrail Service Orchestration. The default is cspadmin. Example: cspadmin
Password	Specify the password for logging into Contrail Service Orchestration. The default is passw0rd. Example: passw0rd
Domain	Specify the name of the Contrail OpenStack domain that you configured for the Contrail Cloud Platform. Example: default
Tenant	Specify the name of the Contrail OpenStack tenant that you configured for the Contrail Cloud Platform. Example: admin
Network Information *Resource Pools*	

Table 35: Fields on the Add Cloud VIM Page *(continued)*

Field	Guidelines
Resource Pool	Specify a resource pool name and the corresponding compute zone, which is a group of compute nodes. You configure compute zones as availability zones in Contrail OpenStack. The default availability zone is Nova, and you can run the nova availability-zone-list command on the Contrail contoller node to view a list of available zones.
Resource Pool Name	Specify a resource pool, which identifies the location in which the virtual network functions (VNFs) are implemented. You can use an unlimited number of alphanumeric characters, including special characters. Example: north-east.
Compute Zone	Specify the availability zone in Contrail OpenStack in which the virtual machines for network services reside. The default availability zone is nova. You can run the **nova availability-zone-list** command on the Contrail OpenStack to find the list of available zones. Example: nova
Does Management Network Exists?	Specify whether to use an existing virtual network in Contrail OpenStack or to create a new one. • yes—Import the named virtual network from Contrail OpenStack. • no—Create a virtual network in Contrail OpenStack with the specified name.
Management Network Name	Specify the name of the existing network in Contrail or of the new network that you want to create in Contrail. Example: mgmt-net
Management Network Information	
Route Target	Specify one or more route targets for the management network to be created in Contrail Example: 64512:10000.
Subnet	Specify one or more prefixes that define the subnets for the Contrail Compute nodes. You can use an IPv4 address. Example: 192.0.2.0/24.
Internet Network Information	
Network Name	Specify the name of the Internet network. Example: int-net
Does Exist?	Select to add a new Internet connection for the VIM in Contrail OpenStack.

Table 35: Fields on the Add Cloud VIM Page *(continued)*

Field	Guidelines
Route Target	Select the route target for the internet network in Contrail. Example: 64512:10000.
Subnet	Select the prefix that defines the subnet for the Contrail Compute nodes. You can use an IPv4 address. Example: 192.0.2.0/24.
Service Profile Information	
Profile Name	Specify the name of the service profile in a VIM instance. Example: vim-service-profile
Tenant Name	Specify the infra tenant for whom you want to assign the service profile. Example:test-tenant
Domain Name	Specify the Infra domain name. Example:Default
User Name	Specify the username of the tenant. Example: admin
Password	Specify the password for the tenant user. Example: password123
Default Service Profile	If you use a dedicated OpenStack Keystone for Contrail Service Orchestration, specify the name of the default service profile. If you do not specify a service profile when you configure the tenant, Contrail Service Orchestration uses the default profile to authenticate the tenant. Example: default-service-profile

NOTE: **Infra Tenants such as admin is available only in Regional Keystone and not in CSO Keystone (Central Keystone).**

Related Documentation

- About the Routers Page on page 88
- Configuring Devices on page 91
- Creating an EMS on page 86

About the EMS Page

To access this page, click **Resources** > **POPs** > ***POP Name*** > **EMS**.

You can use the EMS page to create an element management system and to view information about an EMS configured in your POP. You need to configure your Junos Space Virtual Appliance with the Administration Portal so that the virtual appliance can communicate with other components in your deployment.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an EMS. See "Creating an EMS" on page 86.
- Change the Junos Space Password. See "Changing the Junos Space Virtual Appliance Password" on page 87.
- Select a different POP from the drop-down list above the top left of the table to view details about an EMS in grid view.
- View details about an EMS. Click the details icon that appears when you hover over the name of an EMS application. See "Viewing Object Details" on page 14.
- Show or hide columns about an EMS. See "Sorting Objects" on page 15.
- Search an object about an EMS. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

Table 36 on page 85 shows the fields on the EMS page.

Table 36: Fields on the EMS Page

Field	Description
Name	View the name of the EMS application. Example: Junos Space
IP Address	View the IP address of the Junos Space Web user interface(UI). For a redundant Contrail Service Orchestration, configure the IP address of the Web UI for the primary Junos Space Virtual Appliance. Example: 192.0.2.3
Vendor	View the vendor name for the EMS. Example: Juniper Networks

Related Documentation

- About the POPs Page on page 57
- Creating a Single POP on page 59

- About the VIMs Page on page 79
- About the Routers Page on page 88

Creating an EMS

You can use the EMS Management page to configure the primary instance of each element management system (EMS) that you use for the Cloud CPE Centralized Deployment Model. Administration Portal automatically adds an object for the EMS, using the name that you specify when you deploy the Junos Space Virtual Appliance.

Verify that the VIM Management page displays the virtualized infrastructure managers (VIMs).

To create an EMS:

1. Click **Resources** > **POPs** > ***POP Name*** > **EMS**.
2. Click the plus (+) icon.

   The Add EMS page appears.
3. Complete the configuration according to the guidelines provided in Table 37 on page 86.
4. Click **Save**. If you want to discard your changes, click **Cancel** instead.

Table 37: Fields on the Add EMS Page

Field	Guidelines
Name	Name of the EMS. This field is auto-populated with the name that you specified when you deployed the Junos Space Virtual Appliance. Example: Junos Space
IP	Specify the IP address of the Junos Space Web user interface (UI). For a redundant Contrail Service Orchestration, configure the IP address of the Web UI for the primary Junos Space Virtual Appliance. Example: 192.0.2.3.
Vendor	Specify the vendor for the EMS. Example: Juniper Networks
Version	Specify the version number of the EMS. The default version is 15.1. Example: 15.1
Authentication URL	Specify the authentication URL for the EMS application.

Table 37: Fields on the Add EMS Page *(continued)*

Field	Guidelines
User Name	Specify the username of the device administrator that you configured. This user should be assigned the admin role in all the tenants. The default username is super. Example: super
Password	Specify the administrator password that you configured. The default password is juniper123. Example: juniper123

Related Documentation

- About the Routers Page on page 88
- Creating a Cloud VIM on page 81

Changing the Junos Space Virtual Appliance Password

Administration Portal enables you to change the password for your Junos Space Virtual Appliance from the EMS Page.

To change the password:

1. Click **Resources** > **POPs** > ***POP Name*** > **EMS**.
2. Select the POP name from the drop-down list.
3. Select the Junos Space Virtual Appliance whose password you want to change.
4. Click **More** > **Change Password**.

   The Change Password page appears.
5. Complete the configuration according to the guidelines provided in Table 38 on page 87.
6. Click **Save**. If you want to discard your changes, click **Cancel** instead.

Table 38: Change Password Fields

Field	Description
Username	Specify the administrator username that you configured. Example: super

Table 38: Change Password Fields *(continued)*

Field	Description
Password	Specify the new password that you want to configure. You can choose a password that is at least eight characters long and contains characters from at least three of the following four character classes: uppercase letters, lowercase letters, numbers (0 through 9), and special characters.

Related Documentation

- About the EMS Page on page 85
- Creating an EMS on page 86

About the Routers Page

To access this page, click **Resources** > **POPs** > ***POP Name*** > **Routers**.

You can use the Routers page to view information about the gateway router configured in the POP and to create and configure physical network elements (PNEs) associated with a specific customer site. A PNE is a device in the network that you can provision and configure through Contrail Service Orchestration.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a device. See "Creating Devices" on page 89.
- Configure a device. See "Configuring Devices" on page 91.
- Select a different POP from the drop-down list above the top left of the table to view router details in grid view.
- View details about a router. Click the details icon that appears when you hover over the name of a router application. See "Viewing Object Details" on page 14.
- Show or hide columns about the routers. See "Sorting Objects" on page 15.
- Search an object about the router. See "Searching for Text in an Object Data Table" on page 15.
- Delete a device. See "Deleting Objects" on page 14.

Field Descriptions

Table 39 on page 88 describes the fields on the Routers page.

Table 39: Fields on the Routers Page

Field	Description
Name	View the name of the device configured in the POP. Example: blue_device

Table 39: Fields on the Routers Page *(continued)*

Field	Description
IP Address	View the IP address of the device. Example: 10.155.67.6
Serial Number	View the serial number of the device. Example: JN116548FAFC
Management Status	View the management status of the device. Example: ACTIVE

Related Documentation

- About the POPs Page on page 57
- About the VIMs Page on page 79
- About the EMS Page on page 85
- Creating a Single POP on page 59

Creating Devices

You can use the Routers page to create physical network elements (PNEs) to a specific point of presence (POP).

To create a device:

1. Click **Resources** > **POPs** > ***POP Name*** > **Routers**.

2. Click **Add** > **Discover Device**.

   The Add Device page appears.

3. Complete the configuration according to the guidelines provided in Table 40 on page 90.

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

Table 40: Fields on the Add Device Page

Field	Description
Name	Specify the name of the device, which can be: • An MX Series router used as an SDN gateway in a centralized deployment. • An MX Series router used as a provider edge (PE) router in a distributed deployment. • An SRX Series Services Gateway used as an IPsec concentrator in a distributed deployment. You can use any number of alphanumeric characters, including special characters. Example: MX-router-10
Family	Select the product series for the device. Example: MX
Device Template	Select the name of the device template for the device: • Juniper-MX-MIS—Customized device template for an MX Series router that prevents the creation of black holes when an administrative user activates a service at a site. Select this option only if you have been advised to do so by Juniper Networks. • SDN-GW-MX—Default template for MX Series router. Select this option for MX Series routers in centralized and distributed deployments. • SRX_Basic_SDWAN_HUB—Device template for an SRX Services Gateway used as a hub that offers basic SD-WAN functionality in a distributed deployment. Select this option only if you have been advised to do so by Juniper Networks. • SRX_Managed_Internet_CPE—Device template to manage an SRX Services Gateway devices for a managed internet service. • SRX_SDWAN_SUPPORT—Device template for an SRX Series Services Gateway with SDWAN deployment.
Type of Device	Select the type of device: • PNE—Use this option in a centralized deployment to add an MX Series router as an SDN gateway. • PE/IPsec—Use this option in a distributed deployment to add an MX Series router as a PE router, an IPsec concentrator or both, or to add an SRX Series gateway as an IPsec concentrator.
PNE package	If you specified that the device is an MX Series router for a centralized deployment, select the name of the package that contains metadata and configuration instructions for the PNE: • Juniper-MX—Use with the SDN-GW-MX device profile. • Juniper-MX-MIS—Customized device profile with MX Series configuration that prevents the creation of black holes when an administrative user activates a service at a site. Use with the Juniper-MX-MIS device profile.
Management Type	If you specified that the device is a PE router, IPsec concentrator, or both, specify whether Contrail Service Orchestration manages the device: • Managed—Select this option if you use Contrail Service Orchestration to manage the device. • Unmanaged—Select this option if you use an application other than Contrail Service Orchestration to manage the device. In this case, Contrail Service Orchestration uses the device object that you configure for presentation purposes only.

Table 40: Fields on the Add Device Page *(continued)*

Field	Description
Device IP	Specify the IPv4 address of the management interface for the device. Example: 192.0.2.15
Internet Gateway (optional)	Specify one or more Internet gateway IPv4 addresses if the device connects to CPE devices that have access to the Internet. An Internet gateway IPv4 address may be the same as the IPv4 address of the endpoint of the IPsec tunnel on the IPsec concentrator for a CPE device. Example: 192.0.2.20
User Name	Specify the username that you configured when you set up the device. You use this username to log into the device. Providing login credentials gives Contrail Service Orchestration access to the device. Example: root
Password	Specify the password that you configured when you set up the device. You use this password to log into for the device. Providing login credentials gives Contrail Service Orchestration access to the device. Example: pwd123

Related Documentation

- About the Routers Page on page 88
- Configuring Devices on page 91

Configuring Devices

You can use the Routers page to configure physical network elements (PNEs) associated with a specific customer site.

To configure a device:

1. Click **Resources** > **POPs** > ***POP Name*** > **Routers**.
2. Select the router that you want to configure.
3. Click **More** > **PNE Configure**.

   The PNE Configure page appears.
4. Click the + icon to add interface configuration details.
5. Complete the configuration according to the guidelines provided in Table 41 on page 92.
6. Click **Ok**. If you want to discard your changes, click **Cancel** instead.

Table 41: Fields on the PNE Configure Page

Field	Description
Interface Configuration	
Name	Specify the identifier of the physical interface of the device that acts as the management interface. This interface connects to the management network in Contrail. You either configure this network in Contrail or in Administration Portal when you create the virtualized infrastructure manager (VIM). Example: xe-1/1/1
Vlan	(Optional) If you use VLANs to segment the VPN, specify the identifier of the VLAN interface that connects to the management network in Contrail. The identifier is an integer in the range 1–4096. Example: 100
Addr	Specify an IPv4 prefix for the management interface. Example: 192.0.2.15
BGP Configuration	
AS Number	Specify the autonomous system (AS) number for BGP routing with the Contrail Controller node. Example: 64512
Local Address	Specify an IPv4 address, such as the loopback address, that the router uses for BGP sessions. Example: 192.0.2.15
Remote Address (Contrail Controller)	Select the IPv4 address of the data interface for the Contrail Controller node. Example: 192.0.2.25.
Contrail Compute Prefix	Select one or more IPv4 prefixes that define the subnets between the SDN gateway and the Contrail Compute nodes. Example: 192.0.2.0/24.
Management VRF Configuration	
Interface Name	Reenter the management interface identifier that you specified in the Interface Configuration Name field. In the Management VRF Configuration section, you associate this interface with a virtual routing and forwarding instance (VRF). Example: xe-1/1/1.

Table 41: Fields on the PNE Configure Page *(continued)*

Field	Description
Interface VLAN	(Optional) If you use VLANs to segment the VPN, reenter the identifier that you specified in the Interface Configuration VLAN field. In the Management VRF Configuration section, you associate this interface with a virtual routing and forwarding instance (VRF). Example:100
Default Gateway	(Optional) Specify the IPv4 address on the router that provides the default route for management traffic. Example: 192.0.2.40.
Route Target	Specify the route target for the management network used in Contrail. Example: 64512:10000.
Route Distinguisher	Specify the route distinguisher for the management network used in Contrail. Example: 64512:10000.
Internet VRF Configuration	
Interface Name	Specify one or more physical interfaces on the router that connect to the Internet. Example: xe-2/2/2
Interface VLAN	(Optional) If you use VLANs to segment the VPN, specify the identifiers of the VLAN interfaces that connect to the Internet. A VLAN identifier is an integer in the range 1–4096. Example:500
Default Gateway	(Optional) Specify the IPv4 address on the router that provides the default route for Internet traffic. Example: 192.0.2.50
Route Target	Specify the route target for Internet traffic on this interface. This value matches the Route Target value that you configure for the VPN associated with the site. Example: 64512:12000.
Route Distinguisher	Specify a unique route distinguisher for traffic on this interface. This value matches the Route Distinguisher value that you configure for the VPN associated with the site. You can specify any unique route distinguisher, such as the route target for Internet traffic. Example: 64512:12000

You can also configure the devices from the POPs landing page.

To configure a device:

1. Select **Resources** > **POPs** > ***Pop-Name***.

   The Pop-Name page appears.

2. Click the **Routers** tab.

3. Select the device that you want to configure and click the **Configure Device** button.

   The Stage 2 Config page appears. This page is dynamically rendered based on stage-2 configuration specified in the device profile.

4. Enter the configuration data on the page.

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

   A confirmation message is displayed and the deployment status changes to pending deployment.

6. Click **Deploy** to save and deploy the configuration.

   A confirmation message is displayed indicating that the job is created and subsequently that the job was successful. You can click Deploy History to view the job logs.

7. Click **Cancel** to go back to the Pop-Name page.

Related Documentation

- About the Routers Page on page 88
- Creating Devices on page 89

View the History of Device Data Deletions

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

To view the history of deleted device data:

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

   The Delete History page is displayed. Table 42 on page 95 describes the fields on the Delete History page.

2. Click a task name.

   The Delete Device Tasks page appears. Table 43 on page 95 describes the fields on the Delete Task page.

3. Click the Task ID.

   The Job Status page appears. Table 44 on page 95 describes the fields on the Job Status page.

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

Table 42: Fields on the Delete History Page

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

Table 43: Fields on the Delete Device Tasks Page

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

Table 44: Fields on the Job Status Page

Field	Description
Name	View the name of the task.
Actual Start Time	View the start date and time of the task.
User	View the name of the user who deleted the task.

Table 44: Fields on the Job Status Page *(continued)*

Field	Description
End Time	View the end date and time of the task.
State	View the status of the task to know whether the task succeeded or failed.

Related Documentation

- Creating Devices on page 89
- Configuring Devices on page 91

CHAPTER 8

Managing Devices

- About the Tenant Devices Page on page 97
- About the Cloud Hub Devices Page on page 100
- Managing a Tenant Device on page 102
- Managing a Cloud Hub Device on page 103
- Device Redundancy Support Overview on page 104
- Viewing the History of Tenant Device Activation Logs on page 106
- Viewing the History of Cloud Hub Device Activation Logs on page 108
- Adding a Cloud Hub Device on page 109
- Rebooting a CPE Device on page 111

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 service provider 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 45 on page 98.
- View the history of activation data. See *Viewing the History of Activation Data Uploads*.
- View the history of deactivation requests. See *Viewing the History of Deactivation Requests*.
- Reboot a CPE device. See "Rebooting a CPE Device" on page 111.
- 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" on page 14.
- Deleting a CPE. See "Deleting Objects" on page 14.
- Show or hide columns about the CPE. See "Sorting Objects" on page 15.
- Search an object about the CPE device. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

- Table 45 on page 98 describes widgets on the Tenant Devices page.
- Table 46 on page 98 describes the fields on the Tenant Devices page.

Table 45: Widgets on the Tenant Devices Page

Widget	Description
Cloud CPEs by Status	View the management status of the CPE devices deployed in the cloud. • 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 46: Fields on the Tenant Devices Page

Field	Description
Device Name	View the name of the device. Example: sunny-NFX-250
Tenant	View the name of the tenant. Example: tenant-blue
Site Name	View the name of the tenant site. Example: site-blue-white
Location	View the name of the location. Example: San Jose, CA

Table 46: Fields on the Tenant Devices Page *(continued)*

Field	Description
Status Message	View the latest status message. Example: IPsec provision success
WAN Links	View the number of WAN links. Example: 2
POP Name	View the name of the POP. Example: pop_blue
Management Status	View the management status of the CPE devices deployed in the cloud. • Expected—Regional server has activation details for the CPE device, but CPE device has not yet established a connection with the server. • Active—CPE device has downloaded images, but is not yet configured. • Provisioned—IPsec tunnel on NFX250 device is operational. • Provision Failed—CPE device failed when the vSRX was not instantiated properly.
Model	View the name of the device model. Example: NFX
Active Services	View the number of services that are activated for the device. Example: 3
Image Name	View the name of the device image file. Example: install_nfx_fmpm_agent_1_0.sh
OS Version	View the Junos OS Release version. Example: 15.1X49-D40
Serial Number	View the serial number of the device. Example: DD0416AA0117

Related Documentation

- *Viewing the History of Activation Data Uploads*
- *Viewing the History of Deactivation Requests*

About the Cloud Hub Devices Page

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

You can use the Cloud Hub Devices page to view the list of cloud hub devices that are owned by the administrator in the service provider network. You can also create new cloud hub devices, delete existing cloud hub devices, and view detailed information about each cloud hub device in the network. You can add either an MX Series router or an SRX Series services gateway as a cloud hub (SD-WAN) device in a hub-and-spoke topology. Contrail Service Orchestration (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.

The hub models that are supported are:

- Cloud hub—This hub can be shared by multiple tenants. You can add a cloud hub by logging in to Administration Portal and following the procedure for creating a cloud hub device.
- Tenant hub—This hub is specific to a tenant. You can add a tenant hub by logging in to Customer Portal and following the site creation procedure.

NOTE:

- An MX Series router can be added as an SD-WAN cloud-hub device in brown-field deployment only.
- An MX Series router can be used as an SD-WAN hub in single-hub and multihoming deployment.
- An MX Series router is supported as an SD-WAN hub only in a hub-and-spoke topology.
- An MX Series router is not supported as an on-premise SD-WAN hub.
- When you use an MX Series router as SD-WAN hub, you must configure the NAT pools through the stage-2 configuration template.

The workflow for configuring a device as SD-WAN hub is as follows:

1. Create a point of presence (POP). See "Creating a Single POP" on page 59.
2. Add a cloud hub device for the POP. See "Adding a Cloud Hub Device" on page 109.
3. Add a cloud site for the cloud hub device. See *Creating Cloud Hub Sites for SD-WAN Deployment*.

Tasks You Can Perform

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

- Add a cloud hub device. See "Adding a Cloud Hub Device" on page 109.
- Reboot a cloud hub device. Select **Resources** > **Cloud Hub Devices** > ***Device Name*** > **More** > **Reboot** to reboot the hub device.
- Activate a cloud hub device that is in **Expected** state. Click **Activate** to initiate the activation process. The status of the operation is displayed on the Device Activation page. After the activation process is completed successfully, the device is provisioned.
- View details about a cloud hub device. See "Viewing Object Details" on page 14.
- Deleting a cloud hub device. See "Deleting Objects" on page 14.
- Show or hide columns that contain details about the cloud hub device. See "Sorting Objects" on page 15.
- Search an object about the cloud hub device. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

- Table 47 on page 101 describes the fields on the Cloud Hub Devices page.

Table 47: Fields on the Cloud Hub Devices Page

Field	Description
Device Name	Displays the name of a cloud hub device. Example: mx-cloud-hub
Tenant	Displays the name of the tenant. Example: tenant-blue
Site Name	Displays the name of the tenant site. Example: site-blue-white
Location	Displays the name of the location. Example: San Jose, CA
Status Message	Displays the latest status message. Example: IPsec provision success
WAN Links	Displays the number of WAN links for a device. Example: 2

Table 47: Fields on the Cloud Hub Devices Page *(continued)*

Field	Description
POP Name	Displays the name of the POP. Example: pop_blue
Management Status	Displays the management status of the cloud hub devices deployed in the cloud. • **Expected**—The regional server has activation details for the CPE device, but the CPE 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.
Model	Displays the name of the device model. Example: MX
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

- About the Tenant Devices Page on page 97

Managing a Tenant Device

You can use the Tenant Devices page to view and manage a single customer premises equipment (CPE) device at the tenant site. To access this page, click **Resources > Tenant Devices > *Device-Name***.

View the following information on the Overview tab:

- Geographical location of the device at the tenant site.
- Aggregate throughput of the device.
- Recent alerts for the device.
- Details of the device, such as serial number, management IP address, OS version, device template, tenant name, site name, and site location.

Related Documentation

- About the Tenant Devices Page on page 97

Managing a Cloud Hub Device

You can use the Cloud Hub Devices page to view details of and manage a single cloud hub device at the tenant site. To access this page, click **Resources > Cloud Hub 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, and site location.

You can perform the following operations on the **Configuration** tab:

- Save the stage-2 configuration template for the device.
- Deploy the stage-2 configuration template for the device.
- Roll back the stage-2 configuration template for the device.
- View the deployment history of the stage-2 configuration template for the device.

Related Documentation

- About the Cloud Hub Devices Page on page 100

Device Redundancy Support Overview

Contrail Service Orchestration (CSO) provides support for spoke device redundancy for large enterprise SD-WAN on-premise spoke sites. You can configure an SD-WAN site with two CPE devices to act as primary and secondary devices and protect the site against device and link failures. 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:

- AppQOE (latency-optimized SLA)
- CPE in Full-mesh Topology
- LTE WAN backup link
- Service chain support
- Hub in Hub-Spoke Topology

NOTE: **Device redundancy is supported only on SD-WAN deployments.**

Prerequisites for SRX Series Devices

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:

- NFX_SDWAN_Dual_CPE—Supports dual CPE NFX Series devices on an SD-WAN site.
- SRX_SDWAN_Dual_CPE—Supports dual CPE SRX Series devices on an SD-WAN site.

Create and Configure an SD-WAN Site

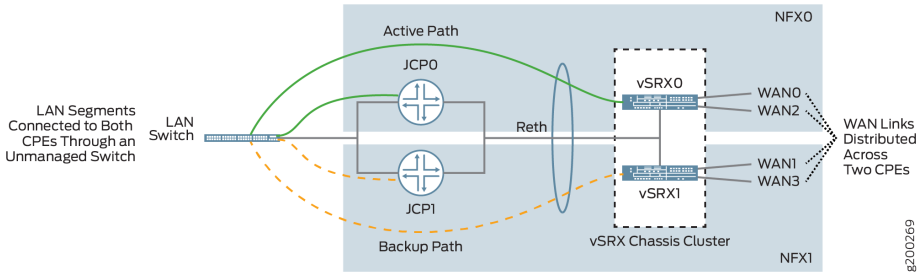
You can create and configure an SD-WAN site with dual CPE devices and the two devices back up each other, with one node acting as the primary device and the other as the

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 *Creating On-Premise Spoke Sites for SD-WAN Deployment* and *Configuring a Single Site*.

Dual CPE Devices Logical Topology for NFX Network Services Platform

Figure 1 on page 105 shows the logical topology of the NFX Series dual CPE devices.

Figure 1: Dual CPE Device Topology - NFX Network Services Platform



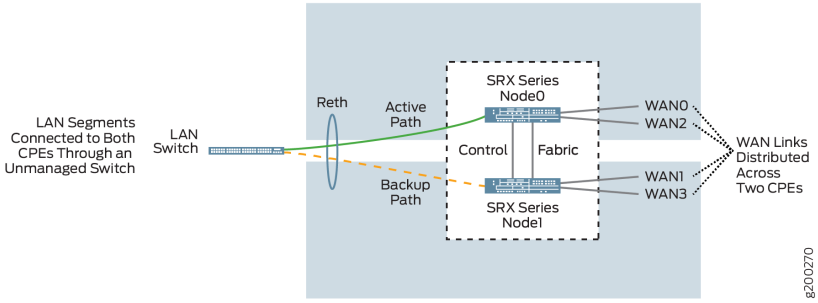
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

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 2 on page 105 shows the logical topology of the SRX Series dual CPE devices.

Figure 2: 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 NFX Series device.

Related Documentation

- *Creating On-Premise Spoke Sites for SD-WAN Deployment*
- *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 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 48 on page 106 describes the fields on the Activation Logs page.

3. Click a task name.

   The ZTP Logs page appears. Table 49 on page 107 describes the fields on the ZTP Logs page.

4. Click the Task Name.

   The Job Status page appears. Table 50 on page 107 describes the fields on the Job Status page.

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

Table 48: 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

Table 48: Fields on the ZTP History Page *(continued)*

Field	Description
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 49: 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 50: 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 on page 97

Viewing the History of Cloud Hub Device Activation Logs

You can use the ZTP History 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 device activation logs:

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

   The Cloud Hub Devices page appears, which list all devices.

2. Select a device and click **More > Activation Logs**.

   The ZTP History page is displayed. Table 51 on page 108 describes the fields on the ZTP History page.

3. Click a task name.

   The ZTP Logs page appears. Table 52 on page 109 describes the fields on the ZTP Logs page.

4. Click the Task Name.

   The Job Status page appears. Table 53 on page 109 describes the fields on the Job Status page.

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

Table 51: 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.
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 52: 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 53: 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 Cloud Hub Devices Page on page 100

Adding a Cloud Hub Device

You can add either an MX Series router or an SRX Series services gateway as a cloud hub device. The device templates that are currently supported for cloud hub devices are:

- MX_Advanced_SDWAN_HUB_option_1
- SRX_Advanced_SDWAN_HUB_option_1

Before You Begin

Create all the resources required for the network point of presence (POP). See "Creating a Single POP" on page 59.

To add a cloud hub device:

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

   The Cloud Hub Devices page appears.

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

   The Add Hub Device page appears.

3. Complete the configuration according to the guidelines provided in Table 54 on page 110.

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

   If you click **Ok**, then the information about the new hub device appears on the Cloud Hub Devices page.

Table 54: Fields on the Add Hub Device Page

Field	Description
Name	Enter the name of the hub device. You can use any number of alphanumeric characters, including special characters. The maximum length is 256 characters. Example: MX-cloud-hub
Management Region	Displays the regional server with which the CPE device communicates. The management region name is populated based on the information from the device template. Example: regional
POP	Select the POP where the hub device needs to be added. Example: pop_blue
Device Template	Select the device template that supports SD-WAN deployment with hub-and-spoke topology. Example: MX_Advanced_SDWAN_HUB_option_1
Connectivity Based on the site requirement, the following fields are populated:	
GRE Interfaces	Enter one or more interface names for the generic routing encapsulation (GRE) tunnel. Example: gr-0/0/1
VT Interfaces	Enter one or more interface names for the virtual tunnel (VT). Example: vt-0/0/1
MS Interfaces	Enter one or more interface names for the multiservices (MS) tunnel. Example: ms-0/0/1
OAM Traffic Information	(Optional) Select this option if the management connectivity is initiated by Contrail Service Orchestration (CSO).
VLAN ID	Enter the Operation, Administration, and Maintenance (OAM) VLAN ID for the in-band management of the site. Example: 53

Table 54: Fields on the Add Hub Device Page *(continued)*

Field	Description
IP Prefix	Enter one or more prefixes for the site's management network. You can specify IPv4 or IPv6 addresses. Example: 172.16.1.1
Gateway IP	Enter the IP address of the default route for the management network. You can specify an IPv4 or IPv6 address. Example: 172.16.0.0

WAN_0
 	
WAN_1
 	
WAN_2
 	
WAN_3
	Select a WAN link to enable it. After selecting the link, specify the following information:
	
	• WAN Interface—Displays the interface name configured in the device template. You cannot modify this field.
	• Link Type—Select the link type (MPLS or Internet) configured in the device template.
	• Address Assignment—Select the method for IP address assignment. The options available are:
	  ◦ DHCP—Select DHCP to assign IP address by using a DHCP server.
	  ◦ STATIC—Select STATIC to assign a static IP address.
	• Traffic Type—Select the traffic type. The options available are:
	  ◦ DATA_ONLY—Select this option if you want to use the WAN link to transmit only data traffic.
	  ◦ OAM_AND_DATA—Select this option if you want to use the WAN link to transmit both data traffic and management traffic.
	
	  NOTE: You must select at least one WAN link with the **OAM_AND_DATA** traffic type.
	
	• 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.

Devices	
Serial Number	Enter the serial number of the hub device. Example: XXXXXXXXXXXX
User Name	Enter the username that you configured when you set up the device. You use this username to log in to the device. Providing login credentials gives CSO access to the device.
Password	Enter the password that you configured when you set up the device. You use this password to log in to the device. Providing login credentials gives CSO access to the device.

After you add the cloud hub device, you activate it. During activation, the device is discovered and the required details are stored in CSO.

Related Documentation

- About the Cloud Hub Devices Page on page 100

Rebooting a CPE Device

You need to reboot a CPE device if the device is down, or if all troubleshooting options fail. A CPE device might be a tenant device or a cloud hub device.

To reboot a tenant device:

1. Select **Resources** > **Tenant Devices**.

2. Select the tenant device that you want to reboot and select **More** > **Reboot**.

   A Device Reboot job link is created and the Status Message column displays the status as **Reboot in-progress**.

   NOTE: **If you reboot a tenant device, deployments that are in progress are stopped.**

3. (Optional) Click the **Device Reboot** link to view the device reboot logs.

4. (Optional) You can view the job status on the **Monitor** > **Jobs** page.

To reboot a cloud hub device:

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

2. Select the cloud hub device that you want to reboot and select **More** > **Reboot**.

   A Device Reboot job link is created and the Status Message column displays the status as **Reboot in-progress**.

   NOTE: **If you reboot a cloud hub device, deployments that are in progress are stopped.**

3. (Optional) Click the **Device Reboot** link to view the device reboot logs.

4. (Optional) You can view the job status on the **Monitor** > **Jobs** page.

You can view the status of reboot in the Status Message column.

On successful reboot of the CPE device, the Status Message column displays the status as **Reboot Succeeded**.

If a CPE device is not reachable or if the reboot time exceeds the timeout value, the reboot fails and the Status Message column displays the status as **Reboot Failed**.

NOTE: **The timeout value for rebooting a CPE device is 14 minutes.**

Related Documentation

- About the Cloud Hub Devices Page on page 100
- About the Tenant Devices Page on page 97

CHAPTER 9

Managing Device Templates

- About the Device Template Page on page 115
- Cloning a Device Template on page 120
- Importing a Device Template on page 121
- Configuring a Device Template on page 122
- Modifying a Device Template Description on page 129
- Deleting a Device Template on page 130

About the Device Template Page

To access this page, click **Resources > Device Templates**.

A device template contains configuration and provisioning instructions for a physical device that you manage through Contrail Service Orchestration (CSO), such as a CPE device or a router. The CSO installation includes several device templates for CPE devices and other physical devices. The device templates for non-CPE devices are fixed and you cannot customize them. You assign a device template to this type of device in CSO when you add it to a point of presence (POP). The CPE device templates are specific to the type of device and topology of the solution. You must assign a device template to each CPE device at each site in a distributed deployment. The CPE device templates contain three types of information:

- Template settings information prepares the device for remote activation, connects the device to the peer MX Series router, and establishes an IPsec tunnel with the router.
- Stage-2 configuration template information specifies the additional settings that you or your customer can configure for the device. For example, you can enable configuration of a 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 provides the actual values for the stage-2 configuration templates. In general, your customers perform this configuration through Customer Portal.

In some cases, however, you might want all CPE devices to use the same values, and you have the option to provide those values through the device template. You can use the default CSO CPE device templates if they are suitable for the topology of your solution.

You can also customize the default device templates or create your own device templates and upload them to CSO.

The device templates support the following deployment models:

- MPLS WAN with Internet backup—Device templates NFX_deployment_option_1 and SRX_deployment_option_1 support this deployment model.
- Secure WAN over Internet—Device template NFX_deployment_option_4 supports this deployment model.
- CPE for a Managed Internet Service—Device templates NFX_Managed_Internet_CPE and SRX_Managed_Internet_CPE support this deployment model.

Tasks You Can Perform

You can perform the following tasks from this page:

- Clone a device template. See "Cloning a Device Template" on page 120.
- Import a device template from a file. See "Importing a Device Template" on page 121.
- Configure a device template. See "Configuring a Device Template" on page 122.
- Modify a device template description. See "Modifying a Device Template Description" on page 129.
- Delete a device template. See "Deleting a Device Template" on page 130.
- View details about a device template. See "Viewing Object Details" on page 14.
- Show or hide columns about the templates. See "Sorting Objects" on page 15.
- Search an object about the templates. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

Table 55 on page 117 describes the fields on the Device Templates page.

Table 55: Fields on the Device Templates Page

Field	Description
Template Name	View the name of the device template. • Juniper-MX-MIS—Customized device template for an MX Series router that prevents the creation of black holes when an administrative user activates a service at a site. Select this option only if you have been advised to do so by Juniper Networks. • SDN-GW-MX—Default template for MX Series router. Select this option for MX Series routers in centralized and distributed deployments. • SRX_Basic_SDWAN_HUB—Device template for an SRX Series Services Gateway used as a hub that offers basic SD-WAN functionality in a distributed deployment. Select this option only if you have been advised to do so by Juniper Networks. • SRX_deployment_option_1—Device template for an SRX Series Services Gateway or a vSRX used as a CPE device in a distributed deployment. • SRX_Managed_Internet_CPE—Device template to manage SRX Series Services Gateway devices for a managed internet service. • NFX_deployment_option_1—Device template for an NFX250 device in a distributed deployment. This template supports port-forwarding with a CSO-initiated connection. • NFX_deployment_option_4—Device template for an NFX250 device in a distributed deployment. This template supports outbound SSH, which is the device-initiated connection, with port-forwarding capability. • NFX_Managed_Internet_CPE—Device template to manage an NFX250 device for a managed Internet service. • SRX_Advanced_SDWAN_CPE_option_1—Device template for an SRX Series Services Gateway spoke in an SD-WAN deployment with hub-spoke topology. • SRX_Advanced_SDWAN_HUB_option_1—Device template for an SRX Series Services gateway hub in an SD-WAN deployment with hub-spoke topology. • VRR_Advanced_SDWAN_option_1—Device template for an SD-WAN deployment with hub-spoke topology. • NFX_Advanced_SDWAN_CPE_option_1—Device template for an NFX250 device that you use for an SD-WAN deployment with SP-managed hub-spoke topology. • NFX_SDWAN_SUPPORT—Device template for an NFX250 device that you use for an SD-WAN deployment. • SRX_SDWAN_SUPPORT—Device template for an SRX Series Services Gateway with an SD-WAN deployment. • MX_Advanced_SDWAN_HUB_option_1—Device template for MX Series router in an SD-WAN deployment with hub-spoke topology. • NFX_SDWAN_Dual_CPE—Device template for an NFX250 device in an SD-WAN deployment with a redundant NFX CPE device. • SRX_SDWAN_Dual_CPE—Device template for an SRX Series Services Gateway in an SD-WAN deployment with a redundant SRX CPE device. • NFX_AWS_Cloud_Connect—Device template for an NFX250 device that is deployed on-premise for an AWS VPC. • vSRX_AWS_SDWAN_Endpoint_option_1—Device template for a vSRX spoke in SD-WAN deployment for AWS in hub.
Description	View the description of the device template. Example: NFX250 device deployed as a CPE device with SD-WAN capability.

Table 55: Fields on the Device Templates Page *(continued)*

Field	Description
Assigned to	View the number of tenant sites using the device template. Example: 2 Tenants (2 Sites)
Workflows	View the number of workflows used in the device template. Example: 7
Target Family	View the name of the device family for which the device template is created. Example: juniper-srx
Last Updated	View the date and time when the device template was last updated. Example: 05/23/2017 06:22

The list of device templates and their default configurations are listed in Table 56 on page 118, Table 57 on page 119, and Table 58 on page 119.

Table 56: Device Templates Supported on NFX250 Device

Device Template Name	NFX_deployment_option_1	NFX_Managed_Internet_CPE	NFX_deployment_option_4	NFX_Advanced_SDWAN_CPE_option_1
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled	Disabled	Disabled
ZTP_ENABLED	—	—	—	—
PRE-STAGED-CPE	—	—	—	—
ACTIVATION_CODE_ENABLED	Enabled	Enabled	Enabled	Enabled
OOB_OAM_Port	—	—	—	—
S2_MODEL_HUGEPAGE_COUNT	21	21	21	13
S1_MODEL_HUGEPAGE_COUNT	9	9	9	5
USE_SINGLE_SSH_TO_NFX	Enabled	Enabled	Enabled	Disabled
ENC_ROOT_PASSWORD	Specified	Specified	Specified	Specified
WAN Port Names	WAN_0 ge-0/0/10 WAN_1 ge-0/0/11	WAN_0 ge-0/0/10	WAN_0 ge-0/0/10	WAN_0 ge-0/0/10 WAN_1 ge-0/0/11 WAN_2 xe-0/0/12 WAN_3 xe-0/0/13

Table 57: Device Templates Supported on SRX Series Services Gateways

Device Template Name	SRX_Managed_Internet_CPE	SRX_deployment_option_1	SRX_Advanced_SDWAN_CPE_option_1	SRX_Advanced_SDWAN_HUB_option_1
AUTO_DEPLOY_STAGE2_CONFIG	Disabled	Disabled	Disabled	Disabled
ZTP_ENABLED	Enabled	Enabled	Disabled	Disabled
PRE-STAGED-CPE	Enabled	—	—	—
ACTIVATION_CODE_ENABLED	Disabled	Disabled	Disabled	Disabled
OOB_OAM_Port	fxp0	fxp0	fxp0	fxp0
USE_SINGLE_SSH_TO_NFX	—	—	—	—
S2_MODEL_HUGEPAGE_COUNT	—	—	—	—
S1_MODEL_HUGEPAGE_COUNT	—	—	—	—
ENC_ROOT_PASSWORD	—	—	—	—
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

Table 58: Device Templates Supported on MX Series Router

Device Template Name	MX_Advanced_SDWAN_HUB_option_1
ACTIVATION_CODE_ENABLED	Disabled
AUTO_DEPLOY_STAGE2_CONFIG	Disabled
OOB_OAM_Port	fxp0
ZTP_ENABLED	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

Related Documentation

- Creating a Single POP on page 59

- Creating Devices on page 89

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_Advanced_SDWAN_CPE_option_1_Custom.

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_Advanced_SDWAN_CPE_option_1_Custom.

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 on page 121

Importing a Device Template

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 on page 121
- Importing a Device Template File on page 121

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.

Related Documentation

- Creating a Single POP on page 59

Configuring a Device Template

Device templates contain global parameters and workflows. Global parameters are a set of variables that can be customized easily.

- Configuring Template Settings in a Device Template on page 122
- Updating Stage-2 Configuration Template in a Device Template on page 125
- Configuring Stage-2 Initial Configuration on page 128

Configuring Template Settings in a Device Template

To configure the device template settings:

1. Select **Resources > Device Template**.

   The Device Templates page appears.

2. Select a 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 provided in Table 59 on page 123.

4. Click **Save**.

Table 59: Fields on the Template Settings Page

Name	Description
Customer Parameters	
AUTO_DEPLOY_STAGE2_CONFIG	Specify whether to automatically deploy stage-2 configuration at the end of the Zero Touch Provisioning (ZTP) workflow. Example: Enabled
ZTP_ENABLED	Specify whether to enable ZTP for the device. NOTE: This option is supported on SRX Series Services Gateways only. Example: Enabled
PRE_STAGED_CPE	Specify whether the CPE device is prestaged with WAN configuration. NOTE: This option is supported on SRX Series Services Gateways only. Example: Enabled
ACTIVATION_CODE_ENABLED	Specify whether the customer must use an activation code to activate the CPE device. Example: Enabled
OOB_OAM_Port	Specify the name of the port used for out-of-band Operation, Administration, and Maintenance (OAM) traffic. This port is used in deployments where OAM and data traffic are on separate physical ports. NOTE: This option is supported on SRX Series Services Gateways only. Example: fxp0
S2_MODEL_HUGEPAGE_COUNT	Specify the number of 1-GB huge pages to be used by the VNFs on an NFX250-S2 device with a total memory of 32 GB. Example: 21
USE_SINGLE_SSH_TO_NFX	Specify whether to enable device-initiated connections (outbound SSH) with port-forwarding capability. Port forwarding enables Contrail Service Orchestration to manage an NFX250 device through a single IP address. Example: Enabled

Table 59: 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-encrypted 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.

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 60 on page 125 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 61 on page 126.

4. Click **Save**.

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

Table 60: Fields on the Stage-2 Configuration Templates Page

Name	Description
Name	View the name of the stage-2 configuration template. Example: LAN side config
Family	View the name of the device family. Example: juniper-srx

Table 60: Fields on the Stage-2 Configuration Templates Page *(continued)*

Name	Description
Component Name	View the name of the component through which the settings are configured. The components that are currently supported are: • JUNOS—Supported on SRX Series Services Gateway. • Juniper Device Manager (JDM)—Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. Example: JUNOS
Hide	Displays whether the template is hidden on Customer Portal. • true—Template is not visible on Customer Portal. • false—Template is visible on Customer Portal. Example: false

Table 61: Fields on the Add New Template Page

Name	Description
Template	Select the configuration template from the drop-down list. The configuration templates are designed in the Configuration Designer tool. Example:srx-basic-sdwan-cpe-config
Display Name	Specify the name of the template that you want to display on the configuration interface. Example: SDWAN Config
Component Name	Specify the component name through which the settings are configured. The components that are currently supported are: • JUNOS—Supported on SRX Series Services Gateway. • Juniper Device Manager (JDM)— Supported on NFX250 device. JDM is a Linux container that manages software components. • Juniper Control Plane (JCP)—Supported on NFX250 device. JCP is the Junos VM running on the hypervisor. Administrators can use JCP to configure the network ports of the NFX250 device. JCP is used to configure the switching and routing function on the NFX250 device. • Gateway Router (GWR)—Supported on NFX250 device. vSRX as a gateway provides the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, or policy control. This virtual security and routing appliance ensures reliability and high availability for each application. Example: JUNOS

Table 61: Fields on the Add New Template Page *(continued)*

Name	Description
Hide	Specify whether you want to hide the configuration template on Customer Portal. You might want to choose to hide the template if you are reusing the template for multiple components. • hide—White dot on right with blue background. • show—White dot on left with gray background. Example: hide
Copy From Template	If you have chosen to hide the configuration template on the user interface, then specify the template from which you want to copy the settings. Example: srx-mis-lan-to-wan-config

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 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 config 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

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 62 on page 128, Table 63 on page 129, and Table 64 on page 129.

4. Click **Ok**.

Table 62: 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 63: 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 64: Fields for the SRX Basic SD-WAN Settings on the Stage-2 Initial Configuration Page

Field	Description
Manage App Group	Click to manage the application groups. The application group is predefined in the system for all SRX Series and vSRX configuration settings. The settings are preloaded and displayed on the portal. You can also create new application groups.
Manage App SLA Profile	Click to manage the application service-level agreements (SLA) profiles.
Rule Name	Specify the rule name. Example: critical-apps
Application/Groups	Specify the applications or application groups for the rule. Example: Oracle, SAP
Application SLA Profile	Specify the application SLA profile for the rule. Example: critical-apps

See Also

- About the Device Template Page on page 115

Related Documentation

- Modifying a Device Template Description on page 129

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:

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 on page 115

Deleting a Device Template

Before deleting a device template, ensure that the template is not associated with any tenant site or a CPE device.

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 on page 115

CHAPTER 10

Managing Software Images

- Device Images Overview on page 131
- About the Device Images Page on page 132
- Deploying Device Images to Devices on page 133
- Uploading a Device Image on page 135
- Deleting Device Images on page 137

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 or on a server in a service provider's cloud to deploy the VNF in that location.

Administration Portal enables you to upload both CPE device and VNF images from your local file system and deploy them 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 download software images from Junos Platforms - Download Software.

After you upload a CPE device or VNF image, 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. In addition, you can modify the platforms supported by the device image and the description of the device image.

You can store all the images in a central repository and use a file service to retrieve images from the file server when the image needs to be deployed to the devices.

Related Documentation

- About the Device Images Page on page 132

About the Device Images Page

To access this page, click **Resources > Images**.

You can use the Device Images page to view uploaded device images for physical and virtual devices and upload device images from your local file system. You can deploy device images on a single device or simultaneously on multiple devices of the same family. See "Device Images Overview" on page 131.

Tasks You Can Perform

You can perform the following tasks from this page:

- Upload device images. See "Uploading a Device Image" on page 135.
- Deploy device images. See "Deploying Device Images to Devices" on page 133.
- 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" on page 14.
- Show or hide columns that contain information about the device image. See "Sorting Objects" on page 15.
- Search an object for a device image. See "Searching for Text in an Object Data Table" on page 15.
- View the history of image upgrade. Click **Image Upgrade History > Upgrade History** at the top right corner of a page. See Table 66 on page 133.

Field Descriptions

Table 65 on page 132 shows the fields on the Device Images page.

Table 65: Fields on the Images Page

Field	Description
Image Name	View the name of the device image. Example: juniper_srx_v1.tgz
Type	View the type of the device image. Example: VNF Image
Version	View the version number of the device image. Example: 1.1
Vendor	View the vendor name of the device. Example: Juniper

Table 65: Fields on the Images Page *(continued)*

Field	Description
Size	View the size of the device image. Example: 14 KB

Table 66 on page 133 shows fields on the Upgrade History page.

Table 66: Fields on the Upgrade History Page

Field	Description
In progress	View the number of image upgrade tasks that are in progress.
Success	View the number of image upgrade tasks that are successful.
Failure	View the number of image upgrade 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 upgrade images.

Related Documentation

- Uploading a Device Image on page 135
- Deploying Device Images to Devices on page 133

Deploying Device Images to Devices

Use the Device Images page to view a list of physical and virtual devices that are relevant to the selected image. You can deploy an image on a single device or multiple devices on a per-site basis or across all sites of a tenant. A device can be a CPE device or a virtual network function (VNF). You can also schedule the deployment of images.

To deploy a device image to the device:

1. Select **Resource > Images**.

   The Images page appears.

2. Select the device image to be deployed on the device and then 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 67 on page 134 for the details of the device.

NOTE: **The Deploy button is enabled only for the device images.**

4. Select one or more devices on which the device image needs to be deployed and schedule a date and time for image deployment.

Table 67: Fields on the Deploy Image: Select Devices Page

Field	Description
Device Name	View the name of the device configured in the point of presence (POP) or site. Example: sunny-NFX-250
Tenant	View the name of the tenant. Example: tenant-blue
Site Name	View the name of the tenant site. Example: site-blue-white
Location	View the name of the location. Example: San Jose, CA
WAN Links	View the number of WAN links. Example: 3
POP Name	View the name of the POP. Example: pop_blue
Management Status	View the management status of the devices deployed in the cloud. • EXPECTED—Regional server has activation details for the device, but the device has not yet established a connection with the server. • ACTIVE—Device has downloaded images, but is not yet configured. • PROVISIONED—IPsec tunnel on the NFX250, SRX, or vSRX device is operational. • PROVISION_FAILED—Device failed if the vSRX was not instantiated properly.
Model	View the name of the device model. Example: NFX250
Active Services	View the number of services that are activated for the device. Example: 3

Table 67: Fields on the Deploy Image: Select Devices Page *(continued)*

Field	Description
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.

Related Documentation

- About the Device Images Page on page 132

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 68 on page 136.

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 68: Fields on the Upload Device Image Page

Field	Description
Name	Specify the filename for the device image that you are uploading. Example: juniper_nfx_250_v1_img.tgz You must use the following filename format for device images of VNFs as listed below: • Riverbed—**riverbed-img** • vSRX—**vsrx-vmdisk-15.1.qcow2** • NFX—**juniper_nfx_1.5_img.tgz**
Image Type	Specify the type of device image. • **Device Image**—Software image for the physical device (CPE). • **VNF Image**—Software image for the virtual device (VNF). • **VNF Script**—Provision script for the VNF image. • **EMS Plugin Package**—EMS plugin package to support a new device family. • **Device Extension Package**—Extension software package that can be installed on the device. • **Boot Config Image**—Boot configuration ISO image that can be used to boot up the VNF or virtual device. • **Telemetry Agent Package**—Installable package containing telemetry agent to run on a device. For example, NFX. Yes • **VNFM Plugin Package**—Installable package containing VNF Manager (VNFM) plugin specific to a certain set of VNFs.
Description	Enter a description of the device image.
File Location	Click **Browse** to navigate to the file location in your local system and select an image file to upload.
Vendor	Specify the vendor name of the device. Example: Juniper Networks.
Family	Specify the name of the device family. Example: NFX
Supported Platform	Specify the platform supported by the device image. Example: NFX250
Major Version Number	Specify the major version of the device image. Example: 12
Minor Version Number	Specify the minor version of the device image. Example: 1

Table 68: Fields on the Upload Device Image Page *(continued)*

Field	Description
Build Number	Specify the build name of the device image. Example: X53-D102.2

Related Documentation

- Device Images Overview on page 131
- About the Device Images Page on page 132

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 on page 132

PART 5

Configuration

- Configuring Network Services on page 141
- Configuring Application SLA Profiles on page 163
- Configuring Application Signatures on page 181

CHAPTER 11

Configuring Network Services

- Network Services Overview on page 141
- About the Network Services Page on page 142
- About the Service Overview Page on page 144
- About the Service Instances Page on page 145
- Configuring VNF Properties on page 147
- Allocating a Service to Tenants on page 147
- Removing a Service from Tenants on page 148
- Viewing a Service Configuration on page 148
- vSRX VNF Configuration Settings on page 149
- LxCIPtable VNF Configuration Settings on page 156
- Cisco CSR-1000v VNF Configuration Settings on page 159
- Riverbed Steelhead VNF Configuration Settings on page 160
- Managing a Single Service on page 161

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 on page 142

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 141.

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 69 on page 142.
- Assign a service to one or more tenants. See "Allocating a Service to Tenants" on page 147.
- Remove a service from one or more tenants. See "Removing a Service from Tenants" on page 148.
- 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 145.

Field Descriptions

Table 69 on page 142 shows the descriptions of the widgets that appear at the top of the Services page.

Table 69: Widgets on the Services Page

Widget	Description
Top Network Services Used	View the numbers of instances of the three services that are most used by tenants in the network. This view might help you to identify trends for network services, especially when you introduce a new service.
Services with Critical Alerts	View the top three network services that are receiving maximum number of critical alerts in the network.
Top Services by POP CPU Usage	View the top three network services that are using the largest percentage of CPU from the assigned cores in the network.

Table 70 on page 143 shows the descriptions of the fields on the Network Services page.

Table 70: Fields on the Services Page

Field	Description
Name	View the name of the networkservice. Click the name to view full information about a service.
Tenants	View the number of tenants and the names of the tenants that have access to this netowkr service. • View the name of the first tenant that used the network service (left of the table cell). • View the additional number of tenants using this network service (right of the table cell). • Hover over the additional number of tenants to view a complete list of all the tenants using this network service.
Sites	View the total number of sites at which the network service is deployed for the tenant.
Instances	View the total number of occurrences of the network service that administrative users have activated for the tenant.
Last Update	View the date on which the network service designer last modified the service.

Table 71 on page 143 shows the descriptions of the fields on the Detail for *Service-Name* page.

Table 71: Fields on the Service Detail Page

Field	Description
General Information	
Type	View the category of service.
Configuration	View the settings that the network service designer or you have configured for this service.
Version	View the version number of the network service.
State	View the status of the network service. Example: Published
Performance Goals	View performance of the network service which include bandwidth, number of sessions, and latency.

Related Documentation

- Network Services Overview on page 141
- About the Service Overview Page on page 144
- About the Service Instances Page on page 145
- Allocating a Service to Tenants on page 147
- Removing a Service from Tenants on page 148

- Viewing Object Details on page 14

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 72 on page 144.
- View resources required for the service and its performance specification. See *Service Requirements* and *Service Performance* in Table 72 on page 144.
- View the service chain, with its constituent VNFs. See *Service Configuration* in Table 72 on page 144.

Field Descriptions

Table 72 on page 144 provides guidelines on using the fields on the Service Overview page.

Table 72: Fields on the Service Overview Page

Field	Description
General Information	
Description	View a summary about the service's capabilities. The network service designer provides this summary.
State	View the state of the network service: • Discontinued—Service is no longer available for customers. • Published—Service designer has published service to network catalog, and it is available for customers.
Tenants	View the number of tenants using this service.
Service Requirements	
CPU	View the number of CPUs that the service needs (cores).
Memory	View the amount of RAM that the service needs in gigabytes (GB).
Service Performance	

Table 72: Fields on the Service Overview Page *(continued)*

Field	Description
Sessions	View the number of sessions concurrently supported by one instance of the service.
Bandwidth	View the data rate for the service in megabytes per second (Mbps) or gigabytes per second (Gbps).
Latency	View the time a packet takes to traverse the service in milliseconds (ms) or nanoseconds (ns).
License cost	Specify the license cost for the network service in USD.
Service Configuration (graphic of the service chain)	
I	View the ingress point—the point at which packets enter the service.
E	View the egress point—the point at which packets exit the service.
One or more VNFs	Click to view settings for the VNF. See "vSRX VNF Configuration Settings" on page 149. The service designer can configure the VNF settings in Network Service Designer and the administrative user can configure the VNF settings in Customer Portal. BEST PRACTICE: The network service designer configures settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and the administrative user configures settings for the service, such as policies. The service designer can also configure a few example settings for the service. These example settings should be generic and not network-specific.

Related Documentation

- About the Network Services Page on page 142
- vSRX VNF Configuration Settings on page 149
- LxCIPtable VNF Configuration Settings on page 156
- Cisco CSR-1000v VNF Configuration Settings on page 159
- *Silver Peak VX VNF Configuration Settings*

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 74 on page 146.

- 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. See "Configuring VNF Properties" on page 147.

Field Descriptions

Table 73 on page 146 shows the descriptions of the fields on the Service Instances page.

Table 73: Fields on the Service Instances Page

Field	Description
Name	View the name of the occurrence of a service at a specific tenant site.
Tenant	View the name of the tenant.
Status	View the state of the service at the customer site: • Created—Administrative user for the tenant has enabled this service instance, which is active. • Blank—Administrative user for the tenant has disabled this service instance.
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 74 on page 146 shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

Table 74: Fields on the Service Instance Details Page

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

Related Documentation

- Network Services Overview on page 141
- About the Network Services Page on page 142

Configuring VNF Properties

You can specify whether to enable automatic recovery of a network service or virtualized network function (VNF) for a network service instance in a centralized deployment. Enabling automatic recovery of a network service or VNF improves reliability of the implementation.

Conversely, disabling automatic recovery of a network service or VNF allows you to quickly investigate a problem with a network service or VNF itself.

To enable or disable automatic recovery of a network service or VNF:

1. Select **Configuration > Network Services** > *Services Name* > **Instances**.

   The Services Instances page appears.

2. Select a service instance for which you want to enable or disable automatic recovery.

3. Click **Enable Auto Healing**.

   The Service Properties page appears.

4. Select whether you want to enable or disable automatic recovery.

   NOTE: **By default, automatic recovery of a network service or VNF is enabled.**

5. Click **Save**.

Related Documentation

- About the Service Instances Page on page 145

Allocating a Service to Tenants

For a tenant to have access to a service, you must assign the service to the tenant. You can assign a service to multiple tenants simultaneously; however, you can assign only one service at a time.

To assign a service to tenants:

1. Select **Configuration > Network Services**.

   The Network Services page appears.

2. Select the service that you want to assign to the tenants.

3. Click **Allocate Services**.

   The Tenants: Select Tenant(s) to allocate the Service page appears.

4. Select the tenants to which you want to assign the service.

5. Click **OK** to save the changes.

Related Documentation

- About the Network Services Page on page 142
- Removing a Service from Tenants on page 148

Removing a Service from Tenants

You can remove a service from one or more tenants simultaneously. You can only remove one service at a time, however.

To remove a service from tenants:

1. Click **Configuration > Network Services**.

   The Network Services page appears.

2. Select the service that you want to remove from the tenants.

3. Click **Detach Services**.

   The Detach Service from Tenants page appears.

4. Select the tenants from which you want to remove the service.

5. Click **Ok**.

Related Documentation

- About the Network Services Page on page 142
- Allocating a Service to Tenants on page 147

Viewing a Service Configuration

The following personnel can configure network services.

- The network service designer can configure a service in Network Service Designer.
- The administrative user for the tenant can configure a service in Customer Portal.

Settings that the administrative user configures override any settings that the network service designer or administrator configure.

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.

To configure a service:

1. Select **Configuration** > **Network Services** > ***Service Name*** > **Overview**.

   The Services Overview page for the service that you selected appears.

2. In the service chain graphic, click the first VNF.

   The Service page appears.

3. Click each tab to review the settings.

   The Base Configure tab shows the settings for the virtual machine (VM) that contains the VNF, and the other tabs show the settings for specific functions in the VNF.

   Refer to the related topics for the specific VNF settings for details on the configuration settings.

4. (Optional) Click the next VNF in the service chain graphic to view settings for that VNF.

5. Click **Ok**.

Related Documentation

- vSRX VNF Configuration Settings on page 149
- LxCIPtable VNF Configuration Settings on page 156
- Cisco CSR-1000v VNF Configuration Settings on page 159

vSRX VNF Configuration Settings

You can configure the vSRX VNF from **Configuration** > **Network Services** > ***Service Name*** > **Overview** > **Service Configuration**. Your service provider usually configures base settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and you configure settings for the service, such as policies.

NOTE: A vSRX firewall virtualized network function (VNF) is always part of a service chain for a network service on a CPE device.

NOTE: vSRX is the GWR for an on-premise CPE device.

Use the information in the following tables to provide values for the available settings:

- Table 75 on page 150 shows the settings you can configure for the virtual machine (VM) that contains the VNF.

  NOTE: **Your service provider usually configures the base settings and you should not need to change them.**

- Table 76 on page 151 shows the firewall settings you can configure.
- Table 77 on page 153 shows the network address translation (NAT) settings you can configure.
- Table 78 on page 154 shows the unified threat management (UTM) settings you can configure.

Table 75: Fields for the vSRX Base Settings

Field	Description
Host Name	For a cloud site, specify the hostname of the VM that contains the vSRX VNF. The field has no limit on the number of characters and accepts letters, numbers, and symbols. Example: vm-vsrx For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.
Loopback Address	Specify an IPv4 loopback address for the management interface of the VM. Example: 192.0.2.25
DNS Servers	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers. Example: 192.0.2.35
NTP Servers	Specify the FQDNs or IP addresses of one or more NTP servers. Example: 192.0.2.45
Syslog Servers	Specify the FQDNs or IP addresses of one or more system log servers. Example: 192.0.2.55
Enable Re-filter	Select **True** to enable a stateless firewall filter that protects the Routing Engine from denial-of-service (DoS) attacks or **False** to allow DoS attacks. Example: True
Enable Default Screens	For a cloudsite, select **True** to enable the default screens security profile for the destination zone or **False** to disable default screening. Example: False You cannot configure this setting for an on-premise site.

Table 75: Fields for the vSRX Base Settings *(continued)*

Field	Description
Time Zone	Specify the time zone for the VM. Example: UTC
Right Interface	Specify the identifier of the VM interface that transmits data. Example: ge-0/0/1 For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.
Left Interface	Specify the identifier of the VM interface that receives data. Example: ge-0/0/0 For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.
SNMP Prefix List	If you set the Enable Re-filter field to **True**, specify the routes that the Junos Space Virtual Appliance uses for SNMP operations when it discovers the vSRX VNF. Example: 10.0.2.0/24
Ping Prefix List	If you set the Enable Re-filter field to **True**, specify the routes that the Junos Space Virtual Appliance uses for ping operations when it discovers the vSRX VNF. Example: 10.0.2.1/24
Space Servers	If you set the Enable Re-filter field to **True**, specify the IP addresses of the VMs that contain the Junos Space Virtual Appliances. Example: 10.0.2.50

Table 76: Fields for the vSRX Firewall Settings

Field	Description
Policy Name	Specify the name of the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols. Example: policy-1
Source Zone	Select the security zone from which packets originate. • **left**—Interface that transmits data to the host • **right**— Interface that receives data transmitted from the host Zone policies are applied to traffic traveling from one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a *context*. Example: left

Table 76: Fields for the vSRX Firewall Settings *(continued)*

Field	Description
Destination Zone	Select the security zone to which packets are delivered. • **left**—Interface that transmits data to the host • **right**—Interface that receives data transmitted from the host Zone policies are applied to traffic traveling from one security zone (source zone) to another security zone (destination zone). This combination of a source zone and a destination zone is called a *context*. Example: right
Source Address	Specify the source IP address prefixes that the network service uses as match criteria for incoming traffic. To add source addresses: 1. Click the **Source Address** column. The source-address page appears. 2. Select **any** to match any source IP address of packets or **ipp** to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select **ipp**, specify a prefix. 4. Click **OK**. Example: 10.0.2.30
Destination Address	Specify the destination IP address prefixes that the network service uses as match criteria for outgoing traffic. To add a destination address: 1. Click the **Destination Address** column. The destination-address page appears. 2. Select **any** to match any source IP address of packets or **ipp** to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select **ipp**, specify a prefix. 4. Click **OK**. Example: 192.0.2.0/24
Action	Select **permit** to transmit packets that match the rule or **deny** to drop packets that match the rule. Example: permit

Table 76: Fields for the vSRX Firewall Settings *(continued)*

Field	Description
Application	Specify the applications to which the policy applies. The applications are based on protocols and ports. To specify applications: 1. Click the **Application** column. The application page appears. 2. In the allowed_apps field, select **any** to match any application or **app** to choose specific applications. If you select **app**, press and hold the Ctrl key and click the required applications from the drop-down list. • junos-tcp-any • junos-udp-any • junos-ftp • junos-http • junos-https • junos-icmp-all • junos-icmp-ping • junos-telnet • junos-tftp 3. Click **OK**. Example: • junos-tcp-any • junos-udp-any

Table 77: Fields for the vSRX NAT Settings

Field	Guidelines
NAT Source Name	Specify the source IP address of packets that the policy rules match. Example: 10.0.2.2/24
NAT Destination Name	Specify the destination IP address of packets that the policy rules match. Example: 10.0.2.3/24
NAT policy settings—For information about the following policy settings, see the firewall policy settings in Table 2. • Policy Name • Source Zone • Destination Zone • Source Address • Destination Address • Action • Application	

Table 78: Fields for the vSRX UTM Settings

Field	Description
Antivirus	Select **True** to check for viruses in application layer traffic against a virus signature database. Select **False** to disable checking for viruses. Example: True
Antispam	Select **True** to block spam e-mails or **False** to allow spam e-mails. Example: True
Antispam Black List	Specify an address blacklist for local spam filtering. Blacklists contain e-mail addresses from which you do not want to receive messages. NOTE: When both the whitelist and blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked. Example: john@example.net
Antispam White List	Specify an address whitelist for local spam filtering. Whitelists contain e-mail addresses from which you want to receive messages. NOTE: When both the whitelist and blacklist are in use, the whitelist is checked first. If there is no match, then the blacklist is checked. Example: user@example.net
Antispam Action	Select the antispam action that you want the device to take when it detects spam: • **block**—Blocks the message • **tag-subject**—Tags the subject field with a preprogrammed string • **tag-header**—Tags the message header with a preprogrammed string Example: block
Content Filter	Select **True** to block different types of traffic based on the MIME type, file extension, protocol command, and embedded object type or **False** to permit these types of traffic. Example: True
Content Filter Extensions	Specify one or more file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Example: exe, pdf, js
Content Filter Mime	Specify the MIME types to be blocked or permitted over HTTP, FTP, SMTP, IMAP, and POP3 connections. Example: application, exe
Content Filter Protocol Commands	Specify commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols to block traffic based on these commands. Example: put, mput

Table 78: Fields for the vSRX UTM Settings *(continued)*

Field	Description
Content Filter Content Type	Press and hold the Ctrl key and click one or more of the following types of content to specify filtering of traffic that is supported only for HTTP and is not covered by file extensions or MIME types: • Active X • Windows executable files (.exe) • HTTP cookie • Java applet • Zip files Example: activex, exe
Content Filter Apply To	Press and hold the Ctrl key and click one or more of the following protocols in the drop-down list to specify filtering of traffic associated with these protocols: • HTTP • FTP • POP3 • IMAP • SMTP Example: http, ftp
Webfilter	Select **True** to prevent access to specific websites and embedded object types or **False** to permit access to all websites. Example: True
Web Filter Black List	Specify URLs to create a blacklist of websites to block. NOTE: A Web filtering profile can contain one whitelist or one blacklist with multiple user-defined categories, each with a permit or block action. Example: • www.example1.com • www.example2.com
Web Filter White List	Specify URLs to create a whitelist of websites that users can always access. With local Web filtering, the firewall intercepts every HTTP request in a TCP connection and extracts the URL. The network service then looks up the URL to determine whether it is in the whitelist or blacklist based on its user-defined category. NOTE: A Web filtering profile can contain one whitelist or one blacklist with multiple user-defined categories, each with a permit or block action. Example: www.example3.net

Table 78: Fields for the vSRX UTM Settings *(continued)*

Field	Description
Policy settings—For information about the following policy settings, see the firewall policy settings in Table 2. • Source Zone • Destination Zone • Source Address • Destination Address • Action • Application	

Related Documentation

- About the Network Services Page on page 142
- About the Service Overview Page on page 144
- Viewing a Service Configuration on page 148
- LxCIPtable VNF Configuration Settings on page 156
- Cisco CSR-1000v VNF Configuration Settings on page 159

LxCIPtable VNF Configuration Settings

You can configure the LxCIPtable virtualized network function (VNF) from **Configuration > Network Services > *Service Name* > Overview > Service Configuration**.

Your service provider usually configures base settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and you configure settings for the service, such as policies.

Use the information in the following tables to provide values for the available settings:

- Table 79 on page 156 shows the base settings you can configure for the Linux container.

  NOTE: **Your service provider usually configures the base settings and you should not need to change them.**

- Table 80 on page 157 shows the firewall settings you can configure.
- Table 81 on page 158 shows the Network Address Translation (NAT) settings you can configure.

Table 79: Fields for the LxCIP Base Settings

Field	Description
Loopback Address	Specify a loopback IP address. Example: 192.0.2.10

Table 79: Fields for the LxCIP Base Settings *(continued)*

Field	Description
Operation	Select **add** to apply the policies to a specific route or **del** to prevent use of the policies on specific routes. Example: add
Route	Specify the IP prefix of the route to which the policies should apply. Example: 192.0.2.20/24
NextHop	Specify the IP address of a Contrail gateway network to which the VM connects. Example: 192.0.2.20

Table 80: Fields for the LxCIP Firewall Policy Settings

Field	Description
Firewall Policies	
Prevent SSH Brute	Select **True** to prevent SSH brute attacks or **False** to allow SSH brute attacks. Example: False
Prevent Ping Flood	Select **True** to prevent ping flood attacks or **False** to allow ping flood attacks. Example: False
Forwarding Rule Settings	
Destination Address	Specify the destination IP address prefix that the network service uses as a match criterion for outgoing traffic. Example: 192.0.2.25/24
Operation	Select the operation, which applies to a chain of rules of the same type, from the drop-down list. The following options are available: • **append**—Append the rule to a rule chain. • **insert-before**—Insert the rule before a rule with the same name. • **delete**—Replace an existing rule with this name. Example: append
Source Address	Specify the source IP address prefix that the network service uses as a match criterion for outgoing traffic. Example: 192.0.2.20/24
Name	Specify the name for the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols. Example: vsrx-fw-policy

Table 80: Fields for the LxCIP Firewall Policy Settings *(continued)*

Field	Description
Action	Select the action for the rule, which applies to all traffic that matches the specified criteria. • **accept**—Transmit packets that match the policy parameters. • **drop**—Drop packets that match the policy parameters. • **reject**—Reject packets that match the policy parameters. Example: accept
Service	Specify the service that you want the rule to match. Example: • http • smtp
Type	Select the type of packet that the rule matches. • **input**—Packets that the network service receives that are addressed to this VM • **forward**—Packets that the network service receives that are addressed to other VMs • **output**—Packets that the network service transmits The application creates a chain of all rules with a particular type. Example: input

Table 81: Fields for the LxCIP NAT Policy Settings

Field	Description
Left Interface	Specify the name of the interface on which the network service enforces NAT for incoming traffic. Example: Eth1
Right Interface	Specify the name of the interface on which the network service enforces NAT for outgoing traffic. Example: Eth2

Related Documentation

- About the Network Services Page on page 142
- About the Service Overview Page on page 144
- Viewing a Service Configuration on page 148
- vSRX VNF Configuration Settings on page 149
- Cisco CSR-1000v VNF Configuration Settings on page 159

Cisco CSR-1000v VNF Configuration Settings

You can configure the Cisco CSR-1000v virtualized network function (VNF) from **Configuration > Network Services > *Service Name* > Overview > Service Configuration**. Your service provider usually configures base settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and you configure settings for the service, such as policies. Use the information in the following tables to provide values for the available settings:

- Table 82 on page 159 shows the base settings you can configure for the virtual machine (VM) that contains the VNF.

  NOTE: **Your service provider usually configures the base settings and you should not need to change them.**

- Table 83 on page 159 shows the firewall settings you can configure.

Table 82: Fields for the CSR-1000v Base Settings

Field	Description
Host Name	Specify the hostname of the VM. Example: host1
Loopback Address	Specify the IPv4 loopback IP address. Example: 10.0.2.50
Name Servers	Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers. Example: 10.0.2.15
NTP Servers	Specify the FQDNs or IP addresses of one or more NTP servers. Example: ntp.example.net

Table 83: Fields for the CSR-1000v Firewall Settings

Field	Description
Left Interface	Specify the identifier of the interface that transmits data to the host. Example: GigabitEthernet2
Right Interface	Specify the identifier of the interface receiving data transmitted by the host. Example: GigabitEthernet3

Table 83: Fields for the CSR-1000v Firewall Settings *(continued)*

Field	Description
Left to Right Allowed Apps	Select the applications from the drop-down list for which the policy is enforced in outgoing packets. The following applications are available: • http • https • telnet • ftp • tcp • udp • icmp Example: http, https
Right to Left Allowed Apps	Select the application from the drop-down list for which the policy is enforced for incoming packets. The following applications are available: • http • https • telnet • ftp • tcp • udp • icmp Example: ftp, udp

Related Documentation

- About the Network Services Page on page 142
- About the Service Overview Page on page 144
- Viewing a Service Configuration on page 148
- vSRX VNF Configuration Settings on page 149
- Cisco CSR-1000v VNF Configuration Settings on page 159

Riverbed Steelhead VNF Configuration Settings

You configure the Riverbed Steelhead VNF through its own software. See the Riverbed Steelhead documentation for information about how to configure the application. You can view the following setting:

Management IP—IP address of the sxe0 interface on JDM for the NFX250. For example: 192.0.2.25.

Related Documentation

- Viewing a Service Configuration on page 148

Managing a Single Service

Use the tabs on this page to view and manage information about services and service instances.

- About the Service Overview Page on page 144
- About the Service Instances Page on page 145

Related Documentation

- About the Network Services Page on page 142
- Viewing a Service Configuration on page 148

CHAPTER 12

Configuring Application SLA Profiles

- Application Quality of Experience (AppQoE) Overview on page 163
- About the Application Traffic Type Profiles Page on page 165
- Creating Traffic Type Profiles on page 168
- Editing and Deleting Traffic Type Profiles on page 171
- SLA Profiles and SD-WAN Policies Overview on page 172
- Local Breakout Overview on page 175
- About the Application SLA Profiles Page on page 176
- Creating SLA Profiles on page 177
- Editing and Deleting SLA Profiles on page 179

Application Quality of Experience (AppQoE) Overview

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. In Release 3.3, 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.

In Release 3.3 and later, 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.

- Limitations on page 164
- Workflow on page 164

Limitations

The AppQoE support in Release 3.3 is subject to the following limitations and restrictions:

- Only book-ended solutions, which have SRX devices or vSRX instances that run the same version of Junos OS with the same configuration on both ends, are supported.
- Multihoming is not supported.
- Dual CPE devices are not supported.

Workflow

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

1. Service provider administrators review the "Default Traffic Type Profiles" on page 165, enable the required profiles, "modify the default profiles" on page 171, or "create new profiles" on page 168.
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 194.
3. Service provide administrator or tenant administrator can create an application SLA profile and associate a traffic type profile with that. For more information about creating an application SLA profile, see "Creating SLA Profiles" on page 177.

4. Service provide administrator or tenant administrator can associate the SLA profile with an SD-WAN Policy and deploy the policy. For more information see *Creating SD-WAN Policy Intents* and *Deploying Policies*.
5. Service provider 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 40.

About the Application Traffic Type Profiles Page

To access this page from the Admininstration portal, select **Configuration** > **Application Traffic Type Profiles** . To access this page from the Customer portal, select **Configuration** > **SD-WAN** > **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 on page 165
- Tasks You Can Perform on page 167
- Field Descriptions on page 167

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. CSP administrators can review and enable the profiles on a need-basis.**

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

Table 84: 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)	10	
				Probe count	100	
				Burst size	10	
Premium-Internet	Low	10%	Minimum of 12% and Maximum of 15%	Data size (bytes)	64	af12
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	
Internet	Low	5%	Minimum of 15% and Maximum of 20%	Data size (bytes)	64	af11
				Probe interval (seconds)	10	
				Probe count	100	
				Burst size	10	
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	

Table 84: Default Traffic Type Profiles and Parameters *(continued)*

Traffic Type	Priority	Buffer Allocation	Bandwidth Allocation	Probe Parameters		DSCP Value
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	

CSP administrators can use the default traffic type profiles as is or modify the parameters based on your specific requirements. CSP administrators 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" on page 168.
- Edit or delete a traffic type profile. See "Editing and Deleting Traffic Type Profiles" on page 171.
- Show or hide columns that contain information about traffic type profiles. See "Sorting Objects" on page 15.
- 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 85 on page 167 shows the descriptions of the fields on the Application Traffic Type Profiles page.

Table 85: 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.

Table 85: Fields on the Application Traffic Type Profiles Page *(continued)*

Field	Description
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: • Data Size (in bytes) • Probe Interval (in seconds) • Probe Count • Burst Size
Created by	Shows the user that created the SLA profile.

Related Documentation

- Creating Traffic Type Profiles on page 168
- Editing and Deleting Traffic Type Profiles on page 171

Creating Traffic Type Profiles

You can use Traffic Type Profiles to configure class-of-service parameters for various types of traffic. Traffic type profiles enable you to configure class-of-service parameters based on your specific business requirements. Traffic type profiles enable you to assign priority and service level criteria for traffic types. You can link an application traffic type profile with an application SLA profile, which can be linked to an SD-WAN policy intent.

To create an "Application Traffic Type" on page 165 profile:

1. Select **Configuration** > **SD-WAN** > **Application Traffic Type Profiles**.

   The **Application Traffic Type Profiles** page appears.

2. Click the Add (+) icon to create a new traffic type profile.

   The **Create New Traffic Type Profile** page appears.

3. Configure the traffic type profile parameters as per the guidelines provide in Table 86 on page 169.

4. Click **OK** to save the traffic type profile configuration. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the traffic type profiles that you configured appear on the **Application Traffic Type Profiles** page.

Table 86: Fields on the Create Traffic Type Profiles page

Field	Description
General	
Name	Enter the name of the traffic type profile that you want to create. Can be a unique string of not more than 15 characters that contains alphanumeric characters and hyphen (-).
Priority	Select the priority value that you want to assign to the traffic type profile. Traffic type profiles with higher priority values takes precedence over the ones with lower values when network congestions occur. NOTE: You cannot create two traffic type profiles with S-High or High priority. The following list is arranged in the decreasing order of priority, where the first item indicates the highest priority and the fifth item, the lowest priority. 1. **S-High**, which denotes strict high or the highest priority. 2. **M-High**, which denotes medium high. 3. **High** 4. **M-Low**, which denotes medium low. 5. **Low**
Status	Click the toggle button to enable the traffic type profile. You can only have a maximum of six traffic profiles enabled at a time. You can assign only those traffic type profiles that are marked as enabled to application SLA profiles. NOTE: If there are more than six traffic type profiles enabled when you deploy a policy, the policy deployment fails.
Probe Parameters TIP: You can select one of the already configured traffic type profiles from the **Copy probe parameters from** list to populate the values in the probe parameters fields. When you select a traffic type profile, the probe parameter values associated with that profile are populated to the fields. You can edit the values if required. .	
Data Size	Specify the size of the data packets, in bytes, to be used for active probes. The range is 4 through 256.
Probe Interval	Specify the interval, in seconds, between two probes. The range is 1 through 10.
Probe Count	Specify the number of probes that form a test. The range from 10 through 1000.
Burst Size	Specify the maximum number of probes that can be sent in one go. The range is from 10 through 100. The value for this parameter must not exceed the value you configured for Probe Count.
Bandwidth	

Table 86: Fields on the Create Traffic Type Profiles page *(continued)*

Field	Description
DSCP Value	Choose the DSCP value that you want to assign to the traffic type profile. Differentiated Services Code Point (DSCP) values define the forwarding properties of the packet within the Differentiated Services framework. You can assign an Expedited Forwarding (ef), an Assured Forwarding (af), the Best Effort (be), or a Class Selector (CS) value. Class Selector value provides backward compatibility with IP Precedence. You can choose one of the following DSCP values: NOTE: You can assign a DSCP value to only one traffic type profile. • ef • af11 • af21 • af22 • af23 • af31 • af32 • af33 • af41 • af42 • af43 • be • cs1 • cs2 • cs3 • cs4 • cs5 • nc2/cs7
Minimum Bandwidth	(Optional) Move the slider button to choose the minimum bandwidth, as percentage of the total available bandwidth, that you want to allocate to the traffic type profile. The minimum bandwidth value denotes the guaranteed bandwidth allocation for the traffic type.
Maximum Bandwidth	(Optional) Move the slider button to choose the maximum bandwidth, as percentage of the total available bandwidth, that you want to allocate to the traffic type profile. The bandwidth allocation for the traffic type never exceeds the maximum bandwidth configured for the traffic type.
Buffer	
Allocation	Move the slider button to choose the bandwidth buffer that you want to allocate to the traffic type profile. NOTE: The total buffer allocation of all the traffic type profiles that are in enabled state must not exceed 100%.

Related Documentation

- About the Application Traffic Type Profiles Page on page 165

- Editing and Deleting Traffic Type Profiles on page 171

Editing and Deleting Traffic Type Profiles

You can edit and delete traffic type profile configuration.

The following sections explain the procedure for editing and deleting traffic type profiles:

- Editing Traffic Type Profiles on page 171
- Deleting Traffic Type Profiles on page 171

Editing Traffic Type Profiles

To edit a traffic type profile:

1. Select **Configuration** > **SD-WAN** > **Application Traffic Type Profiles** .

   The **Application Traffic Type Profiles** page appears.

2. Select the check box that corresponds to the traffic type profile that you want to modify and click the edit icon.

   The **Edit Traffic Type Profile** page appears Modify the configuration as required. For information about the parameters, see Table 86 on page 169.

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

Deleting Traffic Type Profiles

To delete a traffic type profile:

NOTE: **You cannot delete a traffic type profile if the profile is associated with an application SLA profile. You must first edit the application SLA profile and remove the association with the traffic type profile or delete the associated application SLA profile.**

1. Select **Configuration** > **SD-WAN** > **Application Traffic Type Profiles** .

   The **Application Traffic Type Profiles** page appears.

2. Select the check box that corresponds to the traffic type profile that you want to delete and click the delete icon.

   The **Confirm Delete** page appears.

3. Click **OK** to delete the selected profile.

If you do not want to delete the traffic type profile, click **Cancel** instead.

4. If the selected traffic type profile is associated with any application SLA profile, the following error message appears:

   The Traffic Type Profile is associated with 1 SLA Profile(s). It cannot be deleted.

   Click **OK** and either edit the SLA profile and delete the association or delete the SLA profile. Try deleting the traffic type profile after you modify the SLA profile association or delete the SLA profile.

See Also

- Creating SLA Profiles on page 177
- Editing and Deleting SLA Profiles on page 179

SLA Profiles and SD-WAN Policies Overview

Contrail Service Orchestration (CSO) enables you to create service-level agreement (SLA) profiles and map them to software-defined WAN (SD-WAN) policies for traffic management.

SLA Profiles

SLA profiles are created for applications or groups of applications for all tenants. An SLA profile consists of a set of configurable constraints that can be defined in the unified portal for both the Administration and Customer Portals. Table 87 on page 172 lists the categories of configurable constraints that are defined in an SLA profile.

Table 87: SLA Profile Categories

Category	Description
Path preference and priority	Paths are the WAN links to be used for the SLA profile. You can select an MPLS or Internet link as the preferred path. For SLA profiles that are used for local breakout, you must select a path preference. For SLA profiles that are not associated with local breakout, you must select a path preference or configure at least one SLA parameter. MPLS is more latency-sensitive than Internet. You can define priority or precedence for the SLA profile. A value of one (1) indicates highest priority. SLA profiles with higher priorities are given precedence over SLA profiles with lower priorities. Priority is used when SLA requirements are not met on a WAN link and the site switches WAN links to meet the SLA requirements.

Table 87: SLA Profile Categories *(continued)*

SLA parameters	For SLA profiles that are not used for local breakout, you can also define one or more than one of the following SLA parameters: • Throughput—Amount of data (in Mbps) that is sent upstream and received downstream by the site during the selected time period • Latency—Amount of time (in ms) that a packet of data takes to travel from one designated point to another • Packet loss—Percentage of data packets dropped by the network to manage congestion • Jitter—Difference between the maximum and minimum round-trip times (in ms) of a packet of data SLA parameters have precedence over path preference. Even if one SLA parameter is defined, then it is given a higher priority and will override the path preference. SD-WAN policies mapped to an SLA profile with defined SLA parameters are called dynamic policies. Dynamic policies applied to sites enable the site to override the path preference and switch WAN links when the preferred WAN link is not meeting SLA requirements as defined in the SLA parameters.
Class of service	Class of service (CoS) provides different levels of service assurances to various forms of traffic. CoS enables you to divide traffic into classes and offer an assured service level for each class. The classes of service listed in increasing order of priority and sensitivity to latency are best effort, voice, interactive video, streaming audio or video, control, and business essential. The default CoS is voice.
Rate limiters	Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters: • Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. • Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.

NOTE: **You must define at least one of the SLA parameters or path preference. You cannot leave both path preference and SLA parameters fields blank at the same time.**

SD-WAN Policies

SLA profiles are used by SD-WAN policy intents for traffic management. SD-WAN policies help in optimum utilization of the WAN links and efficient distribution of traffic. Every tenant has an SD-WAN policy and intents are created in the SD-WAN policy. Policy intents consist of the following parameters:

- Source—A source endpoint that you can choose from a list of sites, site groups, and departments or a combination of all of these. The SD-WAN policy intent is applied to the selected source endpoint.
- Destination—A destination endpoint that you can choose from a list of applications and predefined or custom application groups. You can select a maximum of 32 applications or application groups as destination endpoints. The SD-WAN policy intent is applied to the selected destination endpoint.

- SLA profile—An SLA profile that has the required constraints you want to apply to the policy intent.
- Intent name—A unique name for the SD-WAN policy intent.

SD-WAN supports advanced policy-based routing (APBR). APBR enables you to dynamically define the routing behavior of the SD-WAN network based on applications. Dynamic application-based routing makes it possible to define policies and to switch WAN links on the fly based on the application's defined SLA parameters. The APBR mechanism classifies sessions based on applications and application signatures and uses policy intents to identify the best possible route for the application. When the best possible route does not meet the application's defined SLA requirements, the SD-WAN network finds the next best possible route to meet SLA requirements.

For example, consider an application in a site. If you want the application group to use custom throughput, latency, or jitter, you can create an SLA profile with these custom values. You can then create an intent and configure the intent with the application and apply the custom SLA profile. When the intent is deployed, CSO determines the best suited WAN link to route traffic based in the application. If the WAN link fails to meet SLA requirements in runtime, the SD-WAN network switches WAN links to the next best suited path.

On the basis of the configured SLA profile constraints, you can categorize SD-WAN policies into two types:

- **Static policy**—If only the path preference is defined and none of the SLA parameters are defined in the SLA profile, then the policy is called a static policy. In static policies, if the defined WAN link under path preference is unable to meet the SLA requirements, link switching cannot occur and SLA performance deteriorates. The full mesh topology supports only static policies. Also, only static policies can be applied on links that have local breakout enabled.
- **Dynamic policy**—If one or more SLA parameters in the SLA profile are defined, then the policy is called a dynamic policy.

  In dynamic policies, because SLA parameters override the path preference, the SD-WAN network chooses the best possible WAN link for traffic management. When an intent is deployed on a site, if the WAN link chosen by the SD-WAN network does not meet the SLA requirements and the network performance deteriorates, then the site switches WAN links to meet the SLA requirements. The link switching is recorded as an SD-WAN event and displayed in the SD-WAN Events page in the customer portal and the *Tenant_name* SLA Performance pages in the administration and customer portals. Link switching occurs only when the SD-WAN policy is dynamic because SLA parameters override the path preference and the site is able to switch WAN links.

Related Documentation

- About the Application SLA Profiles Page on page 176
- Local Breakout Overview on page 175

Local Breakout Overview

The local breakout feature enables Contrail Service Orchestration (CSO) to route Internet traffic directly from a site in a software-defined WAN (SD-WAN) implementation. In the full mesh topology, local breakout is supported on the branch sites. In the hub-and-spoke topology, local breakout is supported on the on-premise hub site and the spoke site. If local breakout is not enabled on the spoke site, then Internet traffic is routed from the hub site if local breakout is enabled on the hub site. Local breakout is not supported on cloud hub sites.

When creating sites, you need to enable local breakout and configure the WAN links that are used for local breakout traffic on the site. You also need to specify whether the WAN links are used exclusively for local breakout traffic or for both local breakout and non-Internet traffic. If a specific WAN link is used exclusively for local breakout, then overlay tunnels for that WAN link are not created. Enabling a WAN link to be used exclusively for local breakout traffic reduces the number of overlay tunnels created between spoke and hub sites, thereby conserving bandwidth.

You can create a source Network Address Translation (NAT) rule while enabling local breakout on a spoke site. The source NAT rule is interface-based and is implicitly defined and applied to the site. This automatically created source NAT rule is not visible on the **NAT Policies** page. The automatically created source NAT rule has the least priority among rules and can be overridden by a user-created NAT policy. The automatically created source NAT rule can be enabled and disabled only from the **Configuring a Site** page. For an on-premise hub site, the option for automatic creation of source NAT rule is not available on the **Configuring a Site** page, and you need to create a source NAT rule.

You can enable SLA profiles to be associated with local breakout and map the SLA profile to static SD-WAN policies. For SLA profiles that are used for local breakout, you must select a path preference. Static SD-WAN policies are used to route the traffic of the applications defined in the static policies by using the preferred path in the attached SLA profile.

Applications are classified into the following categories:

- Cacheable applications—Cacheable applications are applications groups that are stored in the application cache when they are recognized by the device. After they are stored in the application cache, subsequent sessions are routed directly through the correct WAN link. Only cacheable applications and application groups are supported during the creation of local breakout-specific static SD-WAN policies.
- Noncacheable applications—Noncacheable applications are not stored in the application cache and all sessions are first routed through the default path, and then routed to the correct WAN link based on the SD-WAN policy. Noncacheable applications cannot be used for local breakout-specific static SD-WAN policies.

Related Documentation

- *SLA Profiles and SD-WAN Policies Overview*
- *Creating On-Premise Spoke Sites for SD-WAN Deployment*

- *Configuring a Single Site*
- *Creating SLA Profiles*

About the Application SLA Profiles Page

To access this page, select **Configuration** > **Application SLA Profiles** in the Administration Portal.

You can use the Application SLA Profiles page to view information about service-level agreement (SLA) profiles for all tenants.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details of SLA profiles for all tenants.
- Create an SLA profile for a tenant. See "Creating SLA Profiles" on page 177.
- Edit or delete an SLA profile. See "Editing and Deleting SLA Profiles" on page 179.
- Show or hide columns that contain information about SLA profiles. See "Sorting Objects" on page 15.
- Search for SLA 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 88 on page 176 shows the descriptions of the fields on the Application SLA Profiles page.

Table 88: Fields on the Application SLA Profiles Page

Field	Description
Priority	Displays the SLA profile priority.
Name	Displays the SLA profile name.
Traffic Type Profile	Displays the traffic type profile associated with the SLA profile.
Path Preference	Displays whether there is a preferred path for the SLA profile.
Failover	Shows whether failover is enabled for the SLA profile.
Local Breakout	Displays whether local breakout is enabled on the SLA profile.
Throughput Target	Displays the target throughput for the SLA profile.
Latency Target	Displays the target latency for the SLA profile.

Table 88: Fields on the Application SLA Profiles Page *(continued)*

Field	Description
Packet Loss Target	Displays the target packet loss for the SLA profile.
Jitter Target	Displays the target jitter for the SLA profile.
SLA Probe Match	Displays whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .
Created by	Displays the name of the user that created the SLA profile.

Related Documentation

- SLA Profiles and SD-WAN Policies Overview on page 172
- Local Breakout Overview on page 175
- Creating SLA Profiles on page 177
- Editing and Deleting SLA Profiles on page 179

Creating SLA Profiles

You can use the Create SLA Profile page to create a new service-level agreement (SLA) profile, configure target metrics, and associate tenants with the SLA profile.

To add an SLA profile to a tenant:

1. Click the add icon (**+**) on the **Configuration** > **Application SLA Profiles** page in the Administration Portal.

   The Create SLA Profile page appears.

2. Enter the SLA profile information according to the guidelines provided in Table 89 on page 177.

3. Click **OK** to create the SLA profile. The Application SLA Profile page appears with the new SLA profile information.

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

Table 89: Fields on the Create SLA Profile page

Field	Guidelines
General	
Name	Enter a name for the SLA profile. Can be a unique string of not more than 15 characters that contains alphanumeric characters and hyphen (-).

Table 89: Fields on the Create SLA Profile page *(continued)*

Field	Guidelines
SLA Configuration	
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.
Local Breakout	Enable local breakout for the SLA profile. Local breakout is the ability of the site to route Internet traffic directly from the site.
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are Any, MPLS, and Internet. Any is the default value. For SLA profiles that are used for local breakout, you must select a path preference. For SLA profiles that are not used for local breakout, you must select a path preference or configure at least one SLA parameter.
Failover	Enable failover to switch links 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. NOTE: The Failover option is supported only for bandwidth-optimized SD-WAN networks.
Path Failover Criteria	Choose one of the following options: • **Does not meet one or more SLA parameters**—This triggers the path failover if any of the SLA parameters is violated. • **Does not meet all SLA parameters**—This triggers the path failover only when all the SLA parameters are violated.
SLA Parameters	
Throughput	Enter the target throughput (in Mbps) for the SLA profile. Throughput is the amount of data that is sent upstream and received downstream by the site during the selected time period.
Latency	Enter the target latency (in ms) for the SLA profile. Latency is the amount of time that a packet of data takes to travel from one designated point to another. Target delay is calculated as two times the target latency.
Packet Loss	Enter the target packet loss (in %) for the SLA profile. Packet loss is the percentage of data packets dropped by the network to manage congestion.
Jitter	Enter the target jitter (in ms) for the SLA profile. Jitter is the difference between the maximum and minimum round-trip times of a packet of data.
Advanced Configuration—SLA Sampling	
Session-sampling %	Specify the matching percentage of sessions for which you want to run the passive probes.
SLA-violation-count	Specify the number of SLA violations after which you want CSO to switch paths. The range is 1 through 32.
Sampling-period	Specify the sampling period, in milliseconds, for which the SLA violations are counted. The range is 2000 through 60000.

Table 89: Fields on the Create SLA Profile page *(continued)*

Field	Guidelines
Switch-cool-off-period	Specify 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. The range is 5 through 300.
Advanced Configuration-Rate Limiting	
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile. The rate is in the range 64 through 10,485,760 Kbps.
Maximum Upstream Burst Size	Enter the maximum burst size (in bytes). The burst size is in the 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. The rate is in the range 64 through 10,485,760 Kbps.
Maximum Downstream Burst Size	Enter the maximum burst size (in bytes). The burst size is in the range 1 through 1,342,177,280 bytes.
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to **High**. Other available values are **Medium High**, **Medium Low**, and **Low**.

Related Documentation

- SLA Profiles and SD-WAN Policies Overview on page 172
- About the Application SLA Profiles Page on page 176
- Editing and Deleting SLA Profiles on page 179

Editing and Deleting SLA Profiles

You can use the Applications SLA Profiles page to edit and delete SLA profiles.

- Editing an SLA Profile on page 179
- Deleting SLA Profiles on page 180

Editing an SLA Profile

To edit an SLA Profile:

1. Select the check box for the SLA profile that you want to edit, and click the Edit icon on the **Configuration > Application SLA Profiles** page in the Administration Portal.

   The Edit Application SLA Profile page appears.

2. Update the general SLA profile information as needed according to the guidelines provided in "Creating SLA Profiles" on page 177. You cannot edit the SLA profile name.

3. Click **Next**.

   The Configuration tab appears.

4. Update the configuration parameters as needed according to the guidelines provided in "Creating SLA Profiles" on page 177.

5. Click **OK** to save the updated SLA profile configuration.

   The SLA profile information that you updated appears on the Application SLA Profiles page.

Deleting SLA Profiles

You can delete the SLA profile if it is no longer needed. To delete an SLA profile:

1. Select the check box for the SLA profile that you want to delete and click the delete icon (X) on the **Configuration > Application SLA Profiles** page in the Administration Portal. You can also select multiple SLA profiles.

   A page requesting confirmation for the deletion appears.

2. Click **Yes** to confirm that you want to delete the SLA profile.

   The SLA profile is deleted.

Related Documentation

- SLA Profiles and SD-WAN Policies Overview on page 172
- About the Application SLA Profiles Page on page 176
- Creating SLA Profiles on page 177

CHAPTER 13

Configuring Application Signatures

- Application Signatures Overview on page 181
- About the Application Signatures Page on page 182
- Creating Application Signature Groups on page 183
- Editing, Cloning, and Deleting Application Signature Groups on page 184

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 on page 182
- Creating Application Signature Groups on page 183
- Editing, Cloning, and Deleting Application Signature Groups on page 184

About the Application Signatures Page

To access this page, select **Configuration** > **Shared Objects** > **Application Signatures**.

Use the **Application Signatures** page to view application signatures that are already downloaded and to create, modify, clone, and delete custom application signature groups. The **Application Signatures** page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create 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 group. See "Creating Application Signature Groups" on page 183.
- Modify, clone, or delete an application signature group. See "Editing, Cloning, and Deleting Application Signature Groups" on page 184.
- View the configured parameters of an application signature or application signature group. Click the details icon that appears when you hover over the name of an image or click **More** > **Details**. See "Viewing Object Details" on page 14.
- Show or hide columns in the **Application Signatures**. See "Sorting Objects" on page 15.
- Search for a specific application signature or application signature group. See "Searching for Text in an Object Data Table" on page 15.
- Filter the application signature information based on select criteria. To do this, select the filter icon at the top right-hand corner of the table. The columns in the grid change to accept filter options. Select the filter options; the table displays only the data that fits the filtering criteria.

Field Descriptions

Table 90 on page 182 provides guidelines on using the fields on the **Application Signatures** page.

Table 90: 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.

Table 90: Fields on the Application Signatures Page *(continued)*

Field	Description
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, High, unsafe, and so on.
Characteristic	One or more characteristics of the application signature.
Predefined or Custom	A list of predefined application signatures and application signature groups, and a list of custom application signature groups that you created.

Related Documentation

- Application Signatures Overview on page 181
- Creating Application Signature Groups on page 183
- Editing, Cloning, and Deleting Application Signature Groups on page 184

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 the add icon (+).
3. Complete the configuration according to the guidelines provided in Table 91 on page 183.
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 91 on page 183 provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 91: 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.

Table 91: Fields on the Create Application Signature Group Page *(continued)*

Field	Description
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.

Related Documentation

- Application Signatures Overview on page 181
- About the Application Signatures Page on page 182
- Editing, Cloning, and Deleting Application Signature Groups on page 184

Editing, Cloning, and Deleting Application Signature Groups

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

- Editing Application Signature Groups on page 184
- Cloning Application Signature Groups on page 184
- Deleting Application Signature Groups on page 185

Editing Application Signature Groups

To modify the parameters configured for an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature group that you want to edit, and then select **More > Edit**, or click on the edit icon (pencil symbol), on the top right corner of the table, or right-click and select **Edit**.

   The **Edit** page appears, showing the same options as those displayed when you create a new application signature group.

3. Modify the parameters according to the guidelines provided in "Creating Application Signature Groups" on page 183.

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

The modified application signature group appears in the **Application Signatures** page.

Cloning Application Signature Groups

You can clone an application signature group when you want to reuse an existing application signature group, but with a few minor changes. This way, you can save time recreating the application signature group from the start.

To clone an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Right-click the application signature group that you want to clone and then select **Clone**, or select **More > Clone**.

   The **Clone** page appears with editable fields.

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

The cloned application signature group is displayed on the **Application Signatures** page.

Deleting Application Signature Groups

To delete an application signature group:

1. Select **Configuration > Shared Objects > Application Signatures**.

   The **Application Signatures** page appears.

2. Select the application signature group you want to delete and then click the delete icon **(X)** .

   An alert message appears, verifying that you want to delete the selected item.

3. Click **Yes** to delete the selected application signature group. If you do not want to delete, click **Cancel** instead.

Related Documentation

- Application Signatures Overview on page 181
- About the Application Signatures Page on page 182
- Creating Application Signature Groups on page 183

PART 6

Tenants

- Managing Tenants on page 189

CHAPTER 14

Managing Tenants

- Tenant Overview on page 189
- Full Mesh Topology Overview on page 189
- About the Tenants Page on page 192
- Adding a Single Tenant on page 194
- Editing Tenant Information on page 198
- Importing Data for Multiple Tenants on page 199
- Allocating Network Services to a Tenant on page 203
- Viewing the History of Imported Tenant Data on page 204
- Viewing the History of Deleted Tenant Data on page 205

Tenant Overview

A tenant in a Cloud CPE solution represents a customer who accesses virtualized network functions (VNFs) in a service provider's 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 on page 4
- About the Tenants Page on page 192
- Editing Tenant Information on page 198
- Adding a Single Tenant on page 194
- Importing Data for Multiple Tenants on page 199

Full Mesh Topology Overview

Cloud CPE Solution Release 3.2 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 topology is selected when the tenant is created and cannot be modified later. A tenant supports only one full mesh network

because all sites of the tenant are connected to one another. All sites in a full mesh network are branch sites of the on-premise type. The sites are connected to one another through GRE and GRE_IPsec overlay tunnels. The default overlay tunnel encapsulation is GRE_IPsec.

NOTE: **You cannot create a cloud hub site for a tenant in a full mesh topology. You can create only on-premise sites.**

In the full mesh topology, a WAN interface of one type is connected to a WAN interface of the same type. For instance, WAN interfaces of type MPLS can connect to WAN interfaces of type MPLS only, and WAN interfaces of type Internet can connect to WAN interfaces of type Internet only. Consider that a tenant has two sites with one WAN interface each. If the interface type on one site is MPLS and the interface type on the other site is Internet, then the two sites cannot be connected to each other through the full mesh topology.

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.
- For connections between MPLS WAN interfaces, the MPLS subscription for all sites must be from the same service provider. Also, the MPLS WAN interfaces must have IP reachability.

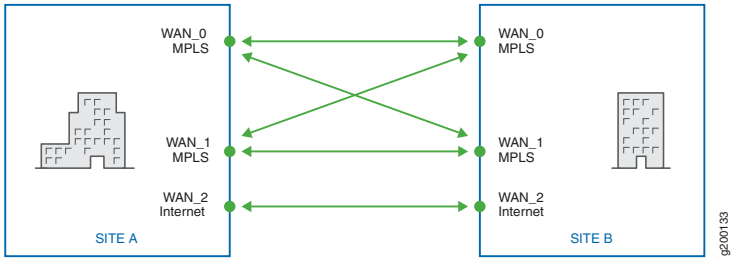
The full mesh topology supports static SD-WAN policies and static advanced policy-based routing (APBR). Full mesh topology also supports LAN segmentation, departments, and multiple VPNs.

Connection Modes in Full Mesh Topology

The following two connection modes are supported in the full mesh topology:

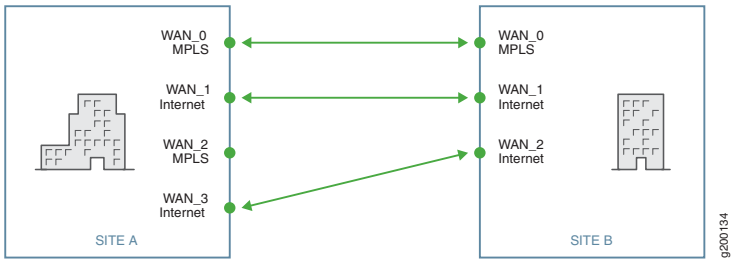
- Dense mode—In dense mode, a WAN interface of a specific type in one site is connected to all WAN interfaces of the same type in all other sites (see Figure 3 on page 191). By default, dense mode is enabled. Because all sites are connected to one another, the number of overlay tunnels formed is large and is difficult to maintain. However, losing connectivity in one tunnel does not negatively impact SD-WAN network performance as there are multiple tunnels to a site. Thus, full mesh topology in dense mode is more resilient to connectivity disruptions.

Figure 3: Dense Mode



- Sparse mode—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 4 on page 191). This configuration reduces the number of overlay tunnels formed and, thus, maintenance is easier than in dense mode. However, sparse mode is more 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 4: 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 by default, only two WAN interfaces that are not enabled exclusively for local breakout traffic are chosen for connecting to the full mesh network. For instance, consider a site has four WAN interfaces. If WAN_1 on the site is enabled exclusively for local breakout traffic, then only WAN_0 and WAN_2 are 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

- SLA Profiles and SD-WAN Policies Overview on page 172
- About the Tenants Page on page 192
- *Local Breakout Overview*

About the Tenants Page

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

You can use the Tenants page to create a tenant, import tenants and other objects associated with tenants, such as administrative users and sites, and view the history of imported tenant data and deleted tenant data. See "Tenant Overview" on page 189.

Before You Begin

Create all the resources required for the network point of presence (POP).

Tasks You Can Perform

You can perform the following tasks from this page:

- Quickly view important data about the tenants in the widgets that appear at the top of the page. For information about the widgets, see Table 92 on page 192.
- View details about a tenant. Click the details icon for the tenant. See "Viewing Object Details" on page 14.
- Add a single tenant. See "Adding a Single Tenant" on page 194.
- Edit tenant information. See "Editing Tenant Information" on page 198.
- Import multiple tenants. See "Importing Data for Multiple Tenants" on page 199.
- Assign Network Services. See "Allocating Network Services to a Tenant" on page 203.
- View tenant import history. See "Viewing the History of Imported Tenant Data" on page 204.
- View tenant delete history. See "Viewing the History of Deleted Tenant Data" on page 205.

Field Descriptions

Table 92 on page 192 shows the description of the widget that appears at the top of the Tenants page.

Table 92: Widget on the Tenants Page

Widget	Description
Tenants by Topology	View the numbers of tenants and their types.
Tenants with Alerts	View the tenants with alerts defined on them.

Table 93 on page 193 provides guidelines on using the fields on the Tenants page.

Table 93: Fields on the Tenants Page

Field	Description
Name	View the name of the tenant. Click the name to view full information about a tenant.
Type	View the type of tenant. The tenant type limits the number of service instances for a tenant. The following options are available: • Small • Medium • Large • Default
Topology	View the topology of the tenant. Example: • Standalone • Hub and Spoke
Plan	View the deployment scenario of the tenant. Example: • HYBRID WAN • SD WAN
Sites	View the total number of sites that are available for the tenant.
Assigned Services	View the number of services that are assigned to the tenant.
Activated Service Instances	View the number of services that have been deployed by the administrator on a connection in the network.
Administrator	View the administrative user for the tenant.
Last Login	View the date and time when the tenant was last logged into..

Related Documentation

- Allocating a Service to Tenants on page 147
- Importing Data for Multiple Tenants on page 199

Adding a Single Tenant

You can use the Add Tenant page to add tenant data and other objects associated with a tenant, such as administrative user, network details, deployment scenario, service profiles, and custom properties. A single tenant supports centralized deployment, distributed deployment, and hybrid (both centralized and distributed) deployment scenarios.

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

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

- **Local Authentication**—You can add the administrative user information as the first step from the Tenants page.
- **Authentication and Authorization with SSO Server**—The **Admin User** information is not displayed on the Tenants page because users are not created in CSO and they are managed in the SAML identity provider. In addition, users are dynamically authorized to the CSO role based on the mapping rules configured in the SAML authentication.
- **Authentication with SSO Server**—When you create the administrative user, the login page does not require you to configure a password because the user is created in the SSO without the password and you can 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 94 on page 194.

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

   If you click **OK**, the tenant that you configured appears on the Tenants page.

4. If you use the tenant for a hybrid WAN centralized deployment, access Contrail and add the following rule to the default security group in the Contrail project.

   ```
   Ingress IPv4 network 0.0.0.0/0 protocol any ports any
   ```

   This rule allows the network to accept traffic from all subnets.

Table 94: Fields on the Add Tenant Page

Field	Description
Tenant Info	

Table 94: Fields on the Add Tenant Page *(continued)*

Field	Description
Name	Enter the name of the tenant. You can use an unlimited number of alphanumeric characters, including special characters. Example: test-tenant
Plan	Select the deployment scenario. • **Hybrid WAN**—Supports both distributed and centralized deployments. NOTE: Intent policies are not applicable for hybrid WAN deployments. • **SD WAN**—Provides a flexible and automated way to route traffic through the cloud. SD-WAN supports both Hub-and-spoke and full mesh topologies and uses CPE devices located at on-premise sites to connect to the LAN segments. The CSO software uses SD-WAN policies and service-level agreement measurements to differentiate and route traffic for different applications. From Release 3.3 onward, you can also enable "Application Quality of Experience (AppQoE)" on page 163 if you set the SD-WAN mode to real-time optimized.
Type	Select the tenant type for a hybrid WAN deployment plan. The following options are available: • Small—1 vCPU, 20-GB disk space, and 2048-MB RAM • Medium—2 vCPUs, 40-GB disk space, and 4096-MB RAM • Large—4 vCPUs, 80-GB disk space, and 8192-MB RAM • X Large—8 vCPUs, 160-GB disk space, and 16384-MB RAM
SD-WAN Mode	Select the SD-WAN mode: • **Bandwidth-optimized SD-WAN**—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. • **Real time-optimized SD-WAN**—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. Click the **Compare** link in the UI to view more information about these modes.
Admin user	
First Name	Enter the first name of the administrative user.
Last Name	Enter the last name of the administrative user.
Username (Email)	Enter the email ID of the administrative user. The email ID is also the username for the administrative user. This field is automatically populated after you enter the tenant name. Example: test-tenant_admin@test-tenant.com
Password Policy	
User Password Expires	Select one of the following options: • **Never**—If you select this option, the password never expires. • **After specified number of days**—If you select this option, you must specify a duration in the **Password Expiration Days** field.

Table 94: Fields on the Add Tenant Page *(continued)*

Field	Description
Password Expiration Days	Specify the duration (in days) after which the password expires and must be changed. The range is from 1 through 365. The default value is 180 days.
Topology Info	
Full Mesh	Select the full mesh topology type. All sites in the tenant are connected to one another in a full mesh topology.
Hub and Spoke	Select the hub and spoke topology type. All hub sites in the tenant are connected to one another and all spoke sites are connected to at least one hub site in a hub and spoke topology. A spoke site can also be connected to multiple hub sites if multihoming is enabled on the spoke site.
Tenant Properties	
SSL Settings NOTE: This setting is applicable only to the SD-WAN deployment scenario.	
Default SSL Forward Proxy Profile	Click the toggle button to enable a default SSL proxy profile for the tenant. If you enable this option, the following items are created when a tenant is added: • A default root certificate with the certificate content specified (in the **Root Certificate** field) • A default SSL proxy profile • A default SSL proxy profile intent that references the default profile This option is disabled by default. NOTE: You use this option to create a tenant-wide default profile; enabling or disabling this option does *not* mean that SSL is enabled or disabled. If you enable this option, you must add a root certificate.

Table 94: Fields on the Add Tenant Page *(continued)*

Field	Description
Root Certificate	You can add a root certificate (X.509 ASCII format) by importing the certificate content from a file or by pasting the certificate content: • To import the certificate content directly from a file: 1. Click **Browse**. The **File Upload** dialog box appears. 2. Select a file and click **Open**. The content of the certificate file is displayed in the **Root Certificate** field. • Copy the certificate content from a file and paste it in the text box. After the tenant is successfully added, a default root certificate, a default SSL proxy profile, and a default SSL proxy profile intent are created. NOTE: • The root certificate must contain both the certificate content and the private key. • For full-fledged certificate operations, such as certificates that need a passphrase, or that have RSA private keys, you must use the Certificates page (**Administration > Certificates**) to import the certificates and install on one or more sites.
Network Segmentation	
Network Segmentation	Enable network segmentation on the tenant.
Service Profiles	
VIM Name	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. Example: test-vim
Service Profile Name	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. Example: service-profile-for-test-vim
Custom 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.
Name	Specify any information about the site that you want to pass to a third-party router. Example: Location
Value	Specify a value for the information about the site that you want to pass to a third-party device. Example: Boston

Related Documentation

- Tenant Overview on page 189
- Editing Tenant Information on page 198

Editing Tenant Information

From Release 3.3. onward, you can edit a tenant configuration to modify service profiles and custom properties.

To edit a tenant:

1. Click **Tenants**.

   The Tenants page appears.

2. Select the tenant for which you want to modify service profiles or custom properties, and click the edit icon.

   The Edit Tenant page appears.

3. Click **Next** twice to go to the Tenant Properties section. Note that you cannot edit the settings in the Tenant Info and Topology Info sections.

   The Tenant Properties section appears.

4. Click > next to Service Profiles to add, edit, or delete service profiles information if you use a dedicated OpenStack Keystone for Contrail Service Orchestration in a centralized deployment.

VIM Name	Select the virtualized infrastructure manager (VIM) for the tenant. A tenant can be associated with multiple VIMs. Example: test-vim
Service Profile Name	Select the service profile that specifies the authentication information for the tenant. You configure the service profile when you create the VIM. Example: service-profile-for-test-vim

5. Click > next to Custom Properties to add or delete custom properties information if you have set up a third-party provider edge (PE) device by using software other than Contrail Service Orchestration.

Name	Specify any information about the site that you want to pass to a third-party router. Example: Location

Value	Specify a value for the information about the site that you want to pass to a third-party device. Example: Boston

6. After you make the changes, click **Next** to view the changes in the Summary section.

   The Summary section appears.

7. Review the changes and click **OK** to save the changes. To discard the changes, click **Cancel**.

Related Documentation

- Tenant Overview on page 189
- Adding a Single Tenant on page 194

Importing Data for Multiple Tenants

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 on page 199
- Importing Tenant Data on page 202

Creating a Tenant Data File

To create a tenant data file:

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

   The Import Tenants page appears.

2. Click **Download Sample JSON** to download a JSON template.

   The tenant template file is downloaded to your system.

3. In 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 95 on page 200 as a reference.

7. Save the customized tenant data file.

Table 95: Tenant Configuration Fields

Field	Description
tenant_name	Specify the name of the tenant. You can use an unlimited number of alphanumeric characters, including symbols. Example: tenant-a
tenant_type	Specify the type of tenant. The following options are available. • Small • Medium • Large • X Large • Default Example: Default
admin_user_name	Specify a unique name for the tenant administrator. Example: admin-tenant-a
admin_user_password	Specify a password for the tenant administrator. Example: pwd123
managed_wan_topology	
network_name	Specify a unique name for the customer Layer 3 VPN network. You can use an unlimited number of alphanumeric characters, including symbols. Example: vcpe-tenant-a-l3vpn
site	
site_name	Specify a unique alphanumeric name for the site. You can use an unlimited number of alphanumeric characters, including symbols. Example: site1
site_description	Specify the description for the site. You can use an unlimited number of alphanumeric characters, including symbols. Example: vcpe payload
street	Specify the street name of the site. Example: site1-street
city	Specify the city name of the site. Example: site1-city

Table 95: Tenant Configuration Fields *(continued)*

Field	Description
state	Specify the name of the state where the site is located. Example: site1-state
zip_code	Specify the zip code of the site location. Example: 99990
country	Specify the name of the country where the site is located. Example: site1-country
router_info (cloud_site_info)	
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
pop_info (cloud_site_info)	
pop_name	Specify the name of the POP that manages the site. You can use an unlimited number of alphanumeric characters, including symbols. Example: pne-pop10
route_target	Specify the route target of the transit network for the tenant. Example: 8828:889

Table 95: 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
pop_info (data_center_site_info)	
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.

NOTE: **If you use the tenants for a hybrid WAN centralized deployment, access Contrail and add the following rule to the default security group in the Contrail project.**

```
Ingress IPv4 network 0.0.0.0/0 protocol any ports any
```

This rule allows the network to accept traffic from all subnets.

Related Documentation

- Viewing the History of Imported Tenant Data on page 204

Allocating Network Services to a Tenant

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

Before You Begin

- Create network services in Network Service Designer. See *Configuring Network Services* topic.

To assign network services:

1. Click **Tenants**.

   The Tenants page appears.

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

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

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

   The network services are assigned to the tenant.

Related Documentation

- About the Tenants Page on page 192

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 96 on page 204 describes the fields on the Import History page.

2. Click the task name.

   The Import Tenants Task page appears. Table 97 on page 205 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 98 on page 205 describes the fields on the Job Status page for imported tenant data.

Table 96: 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 97: 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 98: 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 on page 199

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 99 on page 206 describes the fields on the Delete History page.

2. Click the task name.

   The Delete Tenants Tasks page appears. Table 100 on page 206 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 101 on page 206 describes the fields on the Job Status page for deleted tenant data.

Table 99: 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 100: 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 101: Fields on the Job Status Page for Deleted Tenant Data

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

Table 101: Fields on the Job Status Page for Deleted Tenant Data *(continued)*

Field	Description
End Time	View the end date and time of the task.

Related Documentation

- Importing Data for Multiple Tenants on page 199
- Viewing the History of Imported Tenant Data on page 204

PART 7

Administration

- Configuring MSP Users on page 211
- Configuring Authentication on page 217
- Configuring Licenses on page 227
- Customizing the Unified Portal on page 233
- Managing Signature Database on page 237

CHAPTER 15

Configuring MSP Users

- Role-Based Access Control Overview on page 211
- About the Service Provider Users Page on page 212
- Adding Service Provider Users on page 213
- Editing and Deleting Service Provider Users on page 214

Role-Based Access Control Overview

Contrail Service Orchestration supports the authentication and authorization of users. Both MSP and tenant users access the pages within the unified Administration and Customer Portal based on their role and access permissions.

Table 102 on page 211 shows MSP and Tenant roles and their access privileges.

Table 102: Roles and Access Privileges

Role	Access Privileges
MSP Administrator	Users with the MSP Administrator role have full access to the Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with MSP Administrator or MSP Operator roles, onboard tenants, and add the first tenant administrator during the onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant.
MSP Operator	Users with the MSP Operator role have read-only access to the Administration Portal UI and APIs.
Tenant Administrator	Users with the Tenant Administrator 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	Users with the Tenant Operator role have read-only access to the Customer Portal UI and APIs.

Related Documentation

- Authentication Methods Overview on page 217

About the Service Provider Users Page

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

Use this page to add, edit, and delete users for a service provider. You can also assign roles to service provider users. To know more about MSP users roles and access permissions, see "Role-Based Access Control Overview" on page 211.

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 local users
- **Authentication with SSO Server**—The **Add User** page does not display the password field because you can only assign a role only to an external user.
- **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

The MSP administrator can perform the following tasks from this page:

- Add a service provider user. See "Adding Service Provider Users" on page 213.
- Edit and delete a service provider user. See "Editing and Deleting Service Provider Users" on page 214.

Field Descriptions

Table 103 on page 212 provides guidelines on using the fields on the Users page.

Table 103: Fields on the Users Page

Field	Description
Username	Username of the service provider user. Example: *xyz@example.com*
First Name	First name of the service provider user.
Last Name	Last name of the service provider user.
Role	Role assigned to the service provider user. Example: MSP Admin
Last Login	Date and time of the last login. The format is MM/DD/YYYY HH:MIN. Example: 07/22/2017 20:07

Related Documentation

- Adding Service Provider Users on page 213
- Editing and Deleting Service Provider Users on page 214

Adding Service Provider Users

Use this page to add service provider users and assign roles to service provider users. After the service provider administrator adds the user, the user account is created in the Contrail Service Orchestration (CSO) and the user receives an e-mail with the initial login credentials.

NOTE: **Users with the MSP Operator role have read-only access to Customer Portal and APIs and they cannot add new users.**

To add a service provider user:

1. Select **Administration > Users**.

   The Users page appears.

2. Click the plus icon (+) or click **Add User**.

   The Add User page appears.

3. Complete the configuration as described in Table 104 on page 213.

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

   The service provider user account is created in CSO.

   To enhance the security related to your login credentials, an automatically generated password is sent to the e-mail address that you have specified on the Add User page. You are prompted to change the password after you login with the automatically generated password. For more information about changing the password on first login, see "Changing the Password on First Login" on page 7.

Table 104: Fields on the Add User Page

Field	Description
First Name	Enter the first name as a string of alphanumeric characters and the special characters space, underscore (_), and period (.). The maximum length is 32 characters.
Last Name	Enter the last name as a string of alphanumeric characters and the special characters space, underscore (_), or period (.). The maximum length is 32 characters.
Username (E-mail)	Enter a valid e-mail address in the *user@domain* format.

Table 104: Fields on the Add User Page *(continued)*

Field	Description
Role	Select the role—MSP Operator (default) or MSP Administrator—that you want to assign to the user. • **MSP Administrator**—Users with the MSP Administrator role have full access to the Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with MSP Administrator or MSP Operator roles, onboard tenants, and add the first tenant administrator during the onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant. • **MSP Operator**—Users with the MSP Operator role have read-only access to Administration Portal and APIs. NOTE: Users with the MSP Operator role cannot add, edit, and delete users.

Related Documentation

- About the Service Provider Users Page on page 212
- Editing and Deleting Service Provider Users on page 214

Editing and Deleting Service Provider Users

You can edit the information of a service provider user, and delete one or more users.

NOTE: **Users with the MSP Operator role have read-only access to Administration Portal and APIs, and they cannot edit and delete users.**

- Editing Service Provider Users on page 214
- Deleting Service Provider Users on page 215

Editing Service Provider Users

To modify a service provider 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 User page appears. The options available on the Add User page are available for editing.

   NOTE: **You cannot modify the Username (E-mail) field.**

3. Update the fields as required.

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

The modified service provider user information is saved in CSO.

Deleting Service Provider Users

To delete service provide users:

1. Select **Administration > Users**.

   The Users page appears.

2. Select the users that you want to delete and click the delete icon (X).

   The Confirm Delete page appears.

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

   If you click **Yes**, then the user is deleted and the user account is removed from the CSO.

Related Documentation

- About the Service Provider Users Page on page 212
- Adding Service Provider Users on page 213

CHAPTER 16

Configuring Authentication

- Authentication Methods Overview on page 217
- About the Authentication Page on page 218
- Editing the Authentication Method on page 219
- Configuring a Single Sign-On Server on page 221
- Editing and Deleting SSO Servers on page 223
- Configuring SMTP Settings on page 224

Authentication Methods Overview

Contrail Service Orchestration supports single sign-on (SSO) authentication for the unified portal. You can configure one SSO server for a service provider and another for all its tenants.

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 service provider'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 service provider'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.

Related Documentation

- About the Authentication Page on page 218
- Editing the Authentication Method on page 219

- Configuring a Single Sign-On Server on page 221

About the Authentication Page

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

Use this page to configure the authentication method for service provider and tenant users. You can also use this page to add, edit, and delete SSO servers, and modify the authentication method. You can also configure one SSO server for a service provider and another for all its tenants.

Tasks You Can Perform

You can perform the following tasks from this page:

- Edit the authentication method. See "Editing the Authentication Method" on page 219.
- Configure an SSO server. See "Configuring a Single Sign-On Server" on page 221.
- Edit and delete an SSO server. See "Editing and Deleting SSO Servers" on page 223.

Field Descriptions

Table 105 on page 218 provides guidelines on using the fields on the Authentication page.

Table 105: Fields on the Authentication Page

Field	Description
Authentication Method	
Users	View the user's type. Example : MSP Users or Tenant Users
Authentication Method	View the type of authentication method. Example: Local Authentication
Username Pattern	View the username pattern. Example: *@aaa-example.com*
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 105: Fields on the Authentication Page *(continued)*

Field	Description
Usage	View the information about whether the SSO server is used for authenticating MSP users or tenant users. Example: MSP Users

Related Documentation

- Authentication Methods Overview on page 217
- Configuring a Single Sign-On Server on page 221
- Editing the Authentication Method on page 219

Editing the Authentication Method

Use the Authentication page to modify the authentication method for service provider and tenant users.

To modify the authentication method:

1. Select **Administration** > **Authentication**.

   The Authentication page appears.

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

   The Authentication Type page appears.

3. Select any one of the following authentication methods that you want to configure for the user.
   - Local Authentication
   - Authentication with SSO Server
   - Authentication and Authentication with SSO Server
4. When you select the **Authentication with SSO Server** or **Authentication and Authorization with SSO Server** method, you must enter the configuration described in Table 106 on page 219.

Table 106: Fields on the Authentication Type Page

Field	Description
SSO Server	Select the SSO server name from the list.

Table 106: Fields on the Authentication Type Page *(continued)*

Field	Description
SSO Initiated By	Select the SSO initiation method. • **Service Provider (CSO)**—Select this method if SSO authentication is initiated by CSO. For example, when the user tries to use CSO application without authentication, the user is redirected to the SSO Server. After authentication with the SSO Server, the user is directed to CSO. • **Identity Provider (SSO Server)**—Select this method to authenticate users by using the identity provider. When you login to the identity provider, it provides a list of applications that are integrated with the identity provider and you can access any of the applications. For example, if you click on the CSO application, you are directed to CSO and you can access the CSO application.
When you select **Service Provider (CSO)** method, the following field is displayed:	
Username Pattern	Enter a list of username patterns separated by a comma, space, or semicolon. For example, **@aaa-example.com*; *@xyz-example.com. NOTE: If the username matches the username pattern, the user is redirected to the SSO server to complete the authentication process. If the username does not match with any of the username patterns, then the local authentication is assumed.
When you select **Identity Provider (SSO Server)** method, the following fields are displayed:	
Direct CSO Login Message	Enter the message to be displayed when the user tries to login to CSO without the Identity Provider (IdP) authentication.
Logout Message	Enter the message to be displayed when the user logs out from CSO.
Tenant Identifier	Select the identifier to correlate the tenant Security Assertion Markup Language (SAML) attribute with the tenant. Whenever the tenant is onboarded into the system, the tenant is uniquely identified by any one of the following identifiers: • **Use Tenant Name**—Select this option to identify the tenants by using the tenant name. • **Use OSS Tenant ID**—Select this options to identify the tenants by using the tenant ID.

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

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

Related Documentation

- About the Authentication Page on page 218
- Configuring a Single Sign-On Server on page 221
- Editing and Deleting SSO Servers on page 223

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. When a Security Assertion Markup Language (SAML) assertion is sent from the customer identity provider to CSO, a RelayState parameter is passed to the CSO along with the SAML assertion.

  Currently, the user is redirected to the dashboard page after the SAML assertion process. From Cloud CPE Solution Release 3.3 onward, the user is redirected to the particular page in CSO after the SAML assertion process. For example, if the RelayState parameter path is SD-WAN policy, then the user is redirected to the SD-WAN page.

- **Service Provider**—Acts as an SP and receives the SAML assertion sent by the SSO server in a response to a login request.

Both the identity provider and service provider 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, and the MSP administrator then adds the SSO server in CSO, and enters 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 107 on page 222.

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 107: 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.
SAML Settings	
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**.

Table 107: Fields on the Single Sign-On Server Page *(continued)*

Field	Description
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. NOTE: This field is not required for users with the MSP Admin and MSP Operator roles.
role	This attribute has four values. See Table 108 on page 223.

Table 108: Attribute Values and Roles

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

Related Documentation

- About the Authentication Page on page 218
- Editing and Deleting SSO Servers on page 223

Editing and Deleting SSO Servers

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 on page 223
- Delete SSO Server Configurations on page 224

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 on page 218
- Configuring a Single Sign-On Server on page 221

Configuring SMTP Settings

Use this page to configure an SMTP e-mail 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 109 on page 225.

3. Click **Save**.

   The status of the save operation is displayed.

Table 109: SMTP Settings

Field	Description
Server Address	Specify the hostname for the SMTP e-mail server.
TLS	Enable this option to protect the transmission of the content of e-mail messages. This setting ensures that the information will be transmitted over an encrypted channel.
Port Number	Specify the port number to use for the mail server. Check with your e-mail service provider for this port number. Generally, the port number 587 is used for a Transport Layer Security (TLS) connection and the port number 25 is used for unencrypted connections.
SMTP Authentication	Use this option if the e-mail server requires authentication. The **Username** and **Password** fields are displayed when you enable this option. Disable this option if you want to configure an unauthenticated e-mail server. The **From Name** and **From E-Mail Address** fields are displayed when you disable this option.
Username	Enter a username for the SMTP server.
Password	Enter a password for the SMTP server.
From Name	Enter your username. Example: John Doe
From E-Mail Address	Enter your e-mail address.

Related Documentation

- Authentication Methods Overview on page 217
- About the Authentication Page on page 218

CHAPTER 17

Configuring Licenses

- About the License Files Page on page 227
- Uploading a License File on page 228
- Editing and Deleting Licenses on page 229
- Pushing a License to Devices on page 230

About the License Files Page

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

You can use the License Files page to upload licenses for devices and virtual network services from your local file system. Each 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 License Files. See "Uploading a License File" on page 228.
- Edit and delete license entries. See "Editing and Deleting Licenses" on page 229.
- Push Licenses to devices. See "Pushing a License to Devices" on page 230
- View details of a license. Click the details icon that appears when you hover over the name of an image or click **More > Details**. See "Viewing Object Details" on page 14.
- Show or hide columns about the VNF. See "Sorting Objects" on page 15.
- Search an object about the VNF. See "Searching for Text in an Object Data Table" on page 15.

Field Descriptions

Table 110 on page 228 describes the fields on the License Files page.

Table 110: Fields on the License Files Page

Field	Description
File Name	Displays the filename of the license. Example: license_Image_v1
Description	Displays the description of the license. Example: License file for application routing.
Tenant	Displays the name of the tenant if the license is associated with a tenant. Example: Tenant 1
Uploaded By	Displays the administrator who uploaded the license. Example: test_admin
Uploaded	Displays the date and time when the license was uploaded. Example: 11/18/2016 19:15

Related Documentation

- Uploading a License File on page 228

Uploading a License File

To upload a license file:

1. Click **Administration > Licenses**.

   The License Files page appears.

2. Click the plus icon (+).

   The Add Licenses page appears.

3. In the 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 it, when a device is

activated during ZTP, a matching license from the tenant's licenses is downloaded to the device.

If you do not assign a tenant to a license you can apply that license 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 License Files page.

Related Documentation

- About the License Files Page on page 227
- Device Images Overview on page 131

Editing and Deleting Licenses

The following sections describe the procedure for editing and deleting uploaded licenses:

- Editing a License Entry on page 229
- Deleting a License on page 229

Editing a License Entry

You can edit a license entry to modify the description for the license file.

1. Click **Administration > Licenses**.

   The License Files page appears.

2. Select the license for which you want to modify the description and click the Edit icon.

   The Update 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 License

To delete a license:

1. Click **Administration > Licenses**.

The License Files page appears.

2. Select the license that you want to delete and click the delete icon.

3. In the confirmation message, click **Yes** to delete the license.

   To cancel the delete operation, click **No**.

Pushing a License to Devices

From Release 3.3 onward, you can push licenses on to devices from the Licenses page. If a license is associated with a tenant, you can push the 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 device returns an error at the device level. Similarly, if a pushed license does not match a device, a device-level error is generated.

To push a license to a device:

1. Click **Administration > Licenses**.

   The License Files page appears.

2. Select the license that you want to push on 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 License Files Page on page 227
- Editing and Deleting Licenses on page 229

CHAPTER 18

Customizing the Unified Portal

- Personalizing the Unified Administration and Customer Portal on page 233

Personalizing the Unified Administration and Customer Portal

Use this page to personalize the unified Administration and Customer portal. You can personalize the login page, top-left logo, reports, and apply a font style and color palette to the left navigation bar and menu. You can create, edit, and delete custom color palette. You can also upload custom font styles and preview the custom color palette before you apply the settings.

To personalize the portal:

1. Click **Administration > Preferences**.

   The Preferences page appears.

2. Complete the configuration according to the guidelines in Table 111 on page 233.

Table 111: Fields on the Preferences Page

Field	Action
Logo	
Portal (top left corner)	Click **Select** to upload a logo for the portal. This logo appears at the top left corner of the portal. PNG and SVG file formats are supported. The recommended image size is 25x25 pixel.
Reports	Click **Select** to upload a logo for the report. This logo appears in the security and SD-WAN reports. PNG file format is supported. The recommended image size is 111x116 pixel.
Login Page	
Logo	Click **Select** to upload a logo for the login page of the portal. This logo appears at the top left corner of the login page. PNG and SVG file formats are supported. The recommended image size is 240x25 pixel.

Table 111: Fields on the Preferences Page *(continued)*

Field	Action
Background Image	Select a background image or background color for the login page of the portal. • **Image**—Click **Select** to upload a background image. This image appears in the background of the login page. PNG and SVG file formats are supported. The recommended image size is 1440x780 pixel.
Font	
Typeface	Select a font style for the navigation menu. If you want to upload a custom font style, click **Upload Custom Font**. • The **Upload Custom Fonts** page appears. • Click **Select** to upload custom font style file (zip file). The zip file contains four formats of custom font styles (EOT, SVG, WOFF, and WOFF2) and a CSS file. You must add all four font files to the CSS file. The zip filename should be same as the CSS filename. • Click **Ok**. A confirmation message is displayed and the custom font file is saved in CSO.
Color Palette	Click **Create Custom Palette** to a create custom color palette. The **Create Custom Palette** page is displayed.
Create Custom Palette	
Color Palette Name	Enter a unique name for your color palette. You can use alphanumeric characters, space, and underscore (_). The maximum length is 32 characters.
Primary Navigation Background	Select a background color for the primary left navigation bar and the left navigation menu.
Primary Navigation Active Background	Select the background color for the menu icon and color for the menu.
Primary Navigation Hover Background	Select the color for the navigation bar hover background.
Secondary Navigation Background	Select the background color for the secondary navigation bar.

3. Click **Save Palette** to save the color palette.

   The color palette is saved and a confirmation message is displayed. If you want to discard your changes, click **Cancel**.

   - If you want to modify the custom color palette settings, click on the edit icon (pencil symbol) and update the settings as needed.

- If you want to delete the custom color palette, click the delete icon (X) next to the color palette.
  - The Confirm Color Palette Delete page appears.
  - Click **Yes** to confirm the deletion. The custom color palette is deleted.

4. Click **Preview** to preview the color palette before you apply the settings.

   A confirmation message is displayed and you can preview the theme applied to the portal.

5. Click **Apply** to apply the settings.

   The settings are applied to the portal.

   If you want to discard your changes, click **Cancel**.

Related Documentation

- Logging in to Administration Portal on page 5

CHAPTER 19

Managing Signature Database

- Signature Database Overview on page 237
- About the Active Database Page on page 238
- Downloading a Signature Database on page 239
- Download Locations for Signature Database on page 240
- Installing Signatures on page 241

Signature Database Overview

The Application Firewall signature database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies and quality-of-service (QoS) prioritization.

Contrail Service Orchestration (CSO) enables you to download the signature database. During a download, the complete signature database is downloaded, and the download might take some time to complete. You can track the progress of the download by using job details.

All of the downloaded signatures are created as a default project in read-only mode. The configurations that are downloaded are also saved as a default project.

Related Documentation

- About the Active Database Page on page 238
- Downloading a Signature Database on page 239
- Installing Signatures on page 241

About the Active Database Page

To access this page, select **Administration** > **Signature Database**. The **Active Database** page appears.

Use the **Active Database** page to download and install the Application Firewall signature database to security devices. This database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies, SD-WAN flows, and QoS prioritization.

Tasks You Can Perform

You can perform the following tasks from this page:

- Schedule signature downloads. See "Downloading a Signature Database" on page 239.
- Install signatures. See "Installing Signatures" on page 241.

Field Descriptions

The **Active Database** page provides an overall, high-level view of your signature database settings. The **Latest List of Signatures** table provides a search option that you can use to search for the signature you want. Table 112 on page 238 describes the fields on this page.

Table 112: Fields on the Active Database Page

Field	Description
Active Database	
Database Version	Version of signature database.
Publish Date	Date when the signature database was published.
Update Job	Job ID of the last successful download signatures job.
Installed Device Count	Number of devices installed.
Detectors	Version number of the protocol detector currently running on the device.
Action	Install signature database configuration.
Latest List of Signatures	
Database Version	Version of latest signature database.
Publish Date	Date when the signature database was published.
Update Summary	List of updated signature details for the selected database.
Detectors	Version number of the protocol detector currently running on the device.

Table 112: Fields on the Active Database Page *(continued)*

Field	Description
Action	Full Download—Download the complete signature database; the download might take a while to complete.

Related Documentation

- Signature Database Overview on page 237
- Downloading a Signature Database on page 239
- Installing Signatures on page 241

Downloading a Signature Database

Use this page to schedule a full download of the signature database. During a full download, the complete signature database is downloaded; the download might take some amount of time.

To download the signature database:

1. Select **Administration > Signature Database**.

   The **Active 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 113 on page 239.

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

Table 113 on page 239 describes the fields on the **Signature Download Setting** page.

Table 113: Fields on the Signature Download Settings Page

Field	Description
Download URL	Specifies the location of the Juniper hosted server from which the signature database is downloaded to the CSO server. The default download URL is https://signatures.juniper.net/. To download signatures from this location, you need an internet connection to be available to CSO. In case CSO does not have an internet connection, 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. 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 must also start a local web server to host the signature database. For more information on the locations to which you can download the signature database on various servers, see "Download Locations for Signature Database" on page 240.

Table 113: Fields on the Signature Download Settings Page *(continued)*

Field	Description
Signature Version	NOTE: The **Signature Version** field is enabled only when you change the value of **Download URL** from https://signatures.juniper.net/ to any other value. Enter the 4 digit numeric value of the signature database version. The value must only contain numbers and not have any special characters or negative values.

Type	You can chose to download the signature database immediately or schedule the download for a later time and date.
	
	• Select **Run now** to automatically download the signature database immediately.
	• Select **Schedule at a later time** to download the signature database at the specified date and time, as follows:
	  ◦ Click on the calendar icon to choose the date for the download.
	  ◦ Enter the time for the download. You can choose the 12 hour (AM or PM) or 24 hour format to specify the time by selecting the option from the drop-down list provided beside the time field.
	
	NOTE: The time-zone is picked-up based on the time-zone specified when CSO is installed.

Related Documentation

- Signature Database Overview on page 237
- About the Active Database Page on page 238
- Installing Signatures on page 241

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

- Application Signatures Overview on page 181
- *Signature Database Overview*

Installing Signatures

After the signature database is downloaded, you can install the active database.

NOTE: You must install the application identification license before installing the signature database. For the installation procedure, refer to the *Known Behavior* section of the *Cloud CPE Solution Release Notes* (available at https://www.juniper.net/documentation/en_US/release-independent/nfv/information-products/pathway-pages/index.html).

To install the signature database:

1. Select **Administration > Signature Database**.
2. Click **Install Signatures**.

   The **Install Signatures** page appears.
3. You can view the summary of active signature database version, which will be installed on your device.
4. Click the check box next to the devices on which you want to install the signature database.

   You can also search, sort, or filter this information.
5. Select **Run now** to set the signature database to automatically install immediately.
6. Select **Schedule at a later time** to set the signature database to automatically download at the specified time and to take the following actions:
   a. Choose a date by clicking the date picker icon.
   b. Enter the time.
   c. Select the time format from the drop-down list.
7. Click **OK**.

The signature database installation is complete.

Related Documentation

- Signature Database Overview on page 237
- About the Active Database Page on page 238
- Downloading a Signature Database on page 239