

# Contrail Service Orchestration Customer Portal User Guide

Published  
2020-11-10

Release  
5.0.3

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

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

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

*Contrail Service Orchestration Customer Portal User Guide*

5.0.3

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

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

## YEAR 2000 NOTICE

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

## END USER LICENSE AGREEMENT

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

# Table of Contents

## About the Documentation | xxvi

Documentation and Release Notes | xxvi

Documentation Conventions | xxvi

Documentation Feedback | xxix

Requesting Technical Support | xxix

Self-Help Online Tools and Resources | xxx

Creating a Service Request with JTAC | xxx

## 1

## Introduction

### Contrail Service Orchestration Overview | 2

Contrail Service Orchestration Release 5.0.0 | 2

### Customer Portal Overview | 3

Customer Portal Overview | 3

Accessing Customer Portal | 4

Switching the Tenant Scope | 6

Setting Up Your Network with Customer Portal | 7

About the Customer Portal Dashboard | 8

Tasks You Can Perform | 8

Field Descriptions | 8

Changing the Customer Portal Password | 11

Resetting the Password | 12

Extending the User Login Session | 14

Reviewing the Tenant Settings | 14

## **Users and Roles | 16**

Role-Based Access Control Overview | 16

About the Users Page in Customer Portal | 17

Tasks You Can Perform | 18

Field Descriptions | 18

Adding Tenant and OpCo Tenant Users | 19

Editing and Deleting Tenant and OpCo Tenant Users | 21

Editing Tenant and OpCo Tenant Users | 21

Deleting Tenant and OpCo Tenant Users | 22

Resetting the Password for Tenant Users | 22

Roles Overview | 23

Types of Roles | 23

Role Scopes | 24

Access Privileges | 24

Relationship Between User, Roles, and Access Privileges | 24

Benefits of role-based access control (RBAC) | 25

About the Tenant Roles Page | 26

Tasks You Can Perform | 26

Field Descriptions | 26

Adding User-Defined Roles for Tenant Users | 27

Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 28

Editing Roles | 29

Cloning Roles | 29

Deleting Roles | 30

Access Privileges for Role Scopes (Tenant and Operating Company) | 31

## **2**

## **Managing Sites, Site groups, and Site Templates**

### **Managing Sites | 39**

About the Sites Page | 40

Tasks You Can Perform | 40

Field Descriptions | 40

Multihoming Overview | 42

Enterprise Hubs Overview | 42

Benefits of Enterprise Hubs | 44

Adding and Provisioning Switches to Provide LAN Capability to a Site Overview	44
Standalone Switch Overview	44
Switch Behind a CPE or Next Generation Firewall Overview	45
Monitoring Switches Overview	48
Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities	48
Adding Provider Hub Sites for SD-WAN Deployment	63
Adding Cloud Spoke Sites for SD-WAN Deployment	64
Provisioning a Cloud Spoke Site in AWS VPC	72
Add a Cloud Spoke Site	72
Download the Cloud Formation Template	73
Provision the Device on AWS Server	74
Activate the Device	75
Manually Adding On-Premise Spoke Sites	76
Adding an On-Premise Spoke Site with Hybrid WAN Capability	76
Adding an On-Premise Spoke Site with SD-WAN Capability	81
Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities	94
Adding an On-Premise Spoke Site with LAN Capability	110
Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities	114
Adding and Provisioning a Next Generation Firewall Overview	121
Overview	121
Topology	122
Workflow	122
Adding a Switch to an Existing Site	123
Enabling Integration with Mist Access Points	128
Adding a Standalone Firewall Site	128
Managing LAN Segments on a Tenant Site	133
Adding LAN Segments	133
Deploying LAN Segments	137
Reassigning a Department to a LAN Segment	138
Deleting LAN Segments	138
Managing a Single Site	139
Viewing the Sites History	140
Viewing Jobs Initiated to Add and Configure Sites	140
Viewing Jobs Initiated to Delete Sites	141

Deleting a Site | 142

## **Managing Site Groups | 144**

About the Site Groups Page | 144

Tasks You Can Perform | 144

Field Descriptions | 144

Creating Site Groups | 145

## **Managing Site Templates | 146**

About the Site Templates Page | 146

Tasks You Can Perform | 146

Adding On-Premise Spoke Sites by Using a Site Template | 147

Adding a Site Template | 149

Cloning, Editing, and Deleting Site Templates | 162

Cloning Site Templates | 163

Editing Site Templates | 163

Deleting Site Templates | 164

Adding and Configuring Sites by Importing a JSON File | 165

## **Managing Mesh Tags | 167**

Mesh Tags Overview | 167

About the Mesh Tags Page | 168

Tasks You Can Perform | 168

Field Descriptions | 168

Creating User-defined Mesh Tags | 169

## **Managing Dynamic VPN | 170**

Dynamic VPN Tunnels Overview | 171

Configuring Dynamic VPN Tunnels Thresholds for all Sites in a Tenant | 172

Adding On-Demand VPN Tunnels | 173

Deleting On-Demand VPN Tunnels | 175

## Managing Devices and Resources

### Managing Devices | 178

#### Device Redundancy Support Overview | 179

- Prerequisites for SRX Series Devices | 179

- Supported Connection Plans | 179

- Create and Configure an SD-WAN Site | 180

- Dual CPE Devices Logical Topology for NFX Network Services Platform | 180

- Dual CPE Devices Logical Topology for SRX Series Gateway Devices | 180

#### Activating a CPE Device | 181

#### Manually Activating a Switch | 184

#### Managing an EX Series Switch | 186

- Viewing the Chassis Information of an EX Series Switch | 187

- Viewing Information about an EX Series Switch | 190

- Viewing Information about Ports on an EX Series Switch | 192

#### Activating Dual CPE Devices (Device Redundancy) | 195

#### Viewing the History of Tenant Device Activation Logs | 198

#### Zero Touch Provisioning Overview | 200

- Devices Supported | 201

- Benefits | 201

#### Workflow for Onboarding a Device Using ZTP | 201

### Managing Device Images | 205

#### Device Images Overview | 205

#### About the Device Images Page | 205

- Tasks You Can Perform | 205

- Field Descriptions | 206

#### Deleting Device Images | 206

## **Managing Resources | 208**

Multidepartment CPE Device Support | 209

About the Devices Page | 210

Tasks You Can Perform | 210

Field Descriptions | 211

Perform Return Material Authorization (RMA) for a Single-CPE Device | 213

Performing Return Material Authorization (RMA) for Dual-CPE Devices | 215

Performing RMA for an NFX Cluster | 216

Performing RMA for an SRX Cluster | 218

Granting RMA for a Device | 220

Grant RMA for a Single-CPE Device | 220

Grant RMA for a Dual-CPE Device | 222

Grant RMA for an SRX Device within an SRX Cluster | 224

Managing a Single CPE Device | 226

Rebooting a CPE Device | 229

Configuring APN Settings on CPE Devices | 230

Configuring APN Settings with SIM Change on CPE Devices | 230

Configuring APN Settings without SIM Change on CPE Devices | 232

Identifying Connectivity Issues by Using Ping | 233

Identifying Connectivity Issues by Using Traceroute | 237

Remotely Accessing a Device CLI | 239

Configuring the Firewall Device | 240

About the Physical Interfaces Page | 242

Tasks You Can Perform | 242

Field Descriptions | 243

About the Logical Interfaces Page | 243

Tasks You Can Perform | 243

Field Descriptions | 244

Adding a Logical Interface | 244

Editing, Deleting, and Deploying Logical Interfaces | 247

Editing Logical Interfaces | 247

Deleting Logical Interfaces | 248

Deploying Logical Interfaces | 248

Adding a Security Zone | 248



[Adding a Routing Instance | 251](#)

[About the Static Routes Page | 252](#)

[Tasks You Can Perform | 252](#)

[Field Descriptions | 253](#)

[Adding a Static Route | 253](#)

[Editing, Deleting, and Deploying Static Routes | 256](#)

[Editing Static Routes | 256](#)

[Deleting Static Routes | 257](#)

[Deploying Static Routes | 257](#)

## **Managing Licenses | 258**

[About the Device Licenses Page | 258](#)

[Tasks You Can Perform | 258](#)

[Field Descriptions | 258](#)

[About the CSO Licenses Page | 259](#)

[Tasks You Can Perform | 260](#)

[Field Descriptions | 260](#)

## **Managing Signature Database and Certificates | 262**

[Signature Database Overview | 262](#)

[About the Signature Database Page | 263](#)

[Tasks You Can Perform | 263](#)

[Field Descriptions | 263](#)

[Installing Signatures | 264](#)

[Certificates Overview | 265](#)

[About the Certificates Page | 266](#)

[Tasks You Can Perform | 266](#)

[Field Descriptions | 266](#)

[Importing a Certificate | 268](#)

[Installing and Uninstalling Certificates | 270](#)

[Installing a Certificate | 270](#)

[Uninstalling a Certificate | 271](#)

About the VPN Authentication Page | 271

Task You Can Perform | 272

Field Descriptions | 272

## Managing Juniper Identity Management Service | 274

Juniper Identity Management Service Overview | 274

Access Token Query | 275

Batch or Periodic Query | 275

IP Address Query | 276

User Mapping Query | 276

About the Identity Management Page | 277

Tasks You Can Perform | 277

Configuring CSO and JIMS Connection | 278

Configuring JIMS for an SRX Device | 280

## 4

## Managing Policies, Profiles, and Proxies

### Managing Firewall Policies | 284

Firewall Policy Overview | 285

About the Firewall Policy Page | 287

Tasks You Can Perform | 287

Field Descriptions | 287

Adding a Firewall Policy | 288

Editing and Deleting Firewall Policies | 290

Editing Firewall Policies | 290

Deleting Firewall Policies | 290

Adding Firewall Policy Intents | 291

Editing, Cloning, and Deleting Firewall Policy Intents | 297

Editing Firewall Policy Intents | 298

Cloning Firewall Policy Intents | 298

Deleting Firewall Policy Intents | 299

Selecting Firewall Source | 299

Adding an End Point as Firewall Source | 300

Selecting Firewall Source Using Abbreviations | 301

Selecting a Firewall Source from the End Points Panel | 301

Creating and Selecting a Firewall Source from the End Points Panel | 302

Creating Addresses from Source | 302

Selecting Firewall Destination | 303

Adding an End Point as Firewall Destination | 303

Selecting Firewall Destination Using Abbreviations | 304

Selecting a Firewall Destination from the End Points Panel | 304

Creating and Selecting a Firewall Destination from the End Points Panel | 305

Creating Addresses from Destination | 305

Firewall Policy Examples | 306

Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B | 308

Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B | 310

Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B | 313

Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A | 314

Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments | 316

Example 6: Firewall Policy that Denies Access to Social Networking Sites | 324

Example 7: Firewall Policy that Controls Access to an Address over the Internet (HTTP) | 327

Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service | 333

Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B | 335

Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A | 338

Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled | 342

Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive. | 345

Firewall Policy Schedules Overview | 346

About the Firewall Policy Schedules Page | 347

Tasks You Can Perform | 347

Field Descriptions | 347

Creating Schedules | 348

Editing, Cloning, and Deleting Schedules | 350

Editing Schedules | 350

Cloning Schedules | 350

- Deleting Schedules | 351

Deploying Firewall Policies | 351

About the Default Profiles for Unified Firewall Policy Page | 352

- Tasks You Can Perform | 353

- Field Descriptions | 353

Editing Default Settings for the Unified Firewall Policy | 354

## **Managing UTM Profiles | 357**

UTM Overview | 358

- UTM Licensing | 359

- UTM Components | 359

Configuring UTM Settings | 360

About the UTM Profiles Page | 362

- Tasks You Can Perform | 362

- Field Descriptions | 362

Creating UTM Profiles | 364

Editing, Cloning, and Deleting UTM Profiles | 367

- Editing UTM Profiles | 367

- Cloning UTM Profiles | 368

- Deleting UTM Profiles | 368

About the Web Filtering Profiles Page | 369

- Tasks You Can Perform | 369

- Field Descriptions | 370

Creating Web Filtering Profiles | 371

Editing, Cloning, and Deleting Web Filtering Profiles | 375

- Editing Web Filtering Profiles | 376

- Cloning Web Filtering Profiles | 376

- Deleting Web Filtering Profiles | 377

About the Antivirus Profiles Page | 377

- Tasks You Can Perform | 378

- Field Descriptions | 378

Creating Antivirus Profiles | 379

**Editing, Cloning, and Deleting Antivirus Profiles | 382****Editing Antivirus Profiles | 382****Cloning Antivirus Profiles | 382****Deleting Antivirus Profiles | 383****About the Antispam Profiles Page | 384****Tasks You Can Perform | 384****Field Descriptions | 384****Creating Antispam Profiles | 385****Editing, Cloning, and Deleting Antispam Profiles | 387****Editing Antispam Profiles | 388****Cloning Antispam Profiles | 388****Deleting Antispam Profiles | 389****About the Content Filtering Profiles Page | 389****Tasks You Can Perform | 389****Field Descriptions | 390****Creating Content Filtering Profiles | 391****Editing, Cloning, and Deleting Content Filtering Profiles | 395****Editing Content Filtering Profiles | 395****Cloning Content Filtering Profiles | 395****Deleting Content Filtering Profiles | 396****About the URL Patterns Page | 397****Tasks You Can Perform | 397****Field Descriptions | 397****Creating URL Patterns | 398****Editing, Cloning, and Deleting URL Patterns | 399****Editing URL Patterns | 400****Cloning URL Patterns | 400****Deleting URL Patterns | 401****About the URL Categories Page | 401****Tasks You Can Perform | 401****Field Descriptions | 402****Creating URL Categories | 402**

**Editing, Cloning, and Deleting URL Categories | 404****Editing URL Categories | 404****Cloning URL Categories | 404****Deleting URL Categories | 405****Managing SLA Profiles and SD-WAN Policies | 406****SLA Profiles and SD-WAN Policies Overview | 406****SLA Profiles | 407****SD-WAN Policies | 408****About the SD-WAN Policy Page | 410****Tasks You Can Perform | 410****Field Descriptions | 410****Creating SD-WAN Policy Intents | 412****Editing and Deleting SD-WAN Policy Intents | 419****Editing SD-WAN Policy Intents | 419****Deleting SD-WAN Policy Intents | 420****About the SLA-Based Steering Profiles Page | 420****Tasks You Can Perform | 420****Field Descriptions | 421****Adding SLA-Based Steering Profiles | 424****Editing and Deleting SLA-Based Steering Profiles | 431****Editing an SLA-Based Steering Profile | 431****Deleting SLA-Based Steering Profiles | 432****About the Path-Based Steering Profiles Page | 432****Tasks You Can Perform | 433****Field Descriptions | 433****Adding Path-Based Steering Profiles | 435****Editing and Deleting Path-Based Steering Profiles | 437****Editing a Path-Based Steering Profile | 438****Deleting a Path-Based Steering Profile | 439****Breakout and Breakout Profiles Overview | 439****Breakout Profiles | 440****SD-WAN Policy Intents for Breakout | 440****Benefits of Breakout Profiles | 441**

About the Breakout Profiles Page	441
Tasks You Can Perform	442
Breakout Profiles Field Descriptions	443
Cloud Breakout Settings Field Descriptions	444
Adding Breakout Profiles	445
Adding Cloud Breakout Settings	447
Assigning Cloud Breakout Settings to Sites	449
Editing Breakout Profiles and Cloud Breakout Settings	450
Editing Breakout Profiles	451
Editing Cloud Breakout Settings	451
Deleting Breakout Profiles and Cloud Breakout Settings	452
Deleting Breakout Profiles	452
Deleting Cloud Breakout Settings	453
Configuring Breakout on SD-WAN Sites	453
<b>Managing NAT Policies  </b>	<b>456</b>
NAT Policies Overview	457
About the NAT Policies Page	460
Tasks You Can Perform	460
Field Descriptions	460
Creating NAT Policies	461
Editing and Deleting NAT Policies	463
Editing NAT Policies	463
Deleting NAT Policies	463
About the Single NAT Policy Page	464
Tasks You Can Perform	464
Field Descriptions	465
Creating NAT Policy Rules	466
Editing, Cloning, and Deleting NAT Policy Rules	473
Editing NAT Policy Rules	473
Cloning NAT Policy Rules	473
Deleting NAT Policy Rules	474
Deploying NAT Policy Rules	475

## Selecting NAT Source | 476

- Adding an Endpoint as NAT Source | 476

- Selecting Interfaces when GWR Resides Inside an NFX Box | 476

- Selecting NAT Source Using Abbreviations | 477

- Selecting a NAT Source from the End Points Panel | 478

- Creating and Selecting a NAT Source from the End Points Panel | 478

- Creating Addresses from Source Field | 479

## Selecting NAT Destination | 480

- Adding an Endpoint as NAT Destination | 480

- Selecting Interfaces when GWR Resides Inside an NFX Box | 480

- Selecting NAT Destination Using Abbreviations | 481

- Selecting a NAT Destination from the End Points Panel | 482

- Creating and Selecting a NAT Destination from the End Points Panel | 482

- Creating Addresses from Destination Field | 483

- Creating Services from Destination Field | 483

## NAT Pools Overview | 484

### About the NAT Pools Page | 484

- Tasks You Can Perform | 485

### Creating NAT Pools | 486

### Editing, Cloning, and Deleting NAT Pools | 488

- Editing NAT Pools | 488

- Cloning NAT Pools | 489

- Deleting NAT Pools | 489



## **Managing IPS Signatures and Profiles | 491**

### **About the IPS Signatures Page | 491**

Tasks You Can Perform | 492

Field Descriptions | 492

### **About the IPS Profiles Page | 496**

Tasks You Can Perform | 497

Field Descriptions | 497

### **Create IPS Profiles | 498**

### **Edit, Clone, and Delete IPS Profiles | 499**

Edit IPS Profiles | 499

Clone IPS Profiles | 500

Delete IPS Profiles | 500

### **About the <IPS-Profile-Name> / Rules Page | 501**

Tasks You Can Perform | 501

Field Descriptions | 501

### **Create IPS or Exempt Rules | 502**

Create IPS Rules | 503

Create Exempt Rules | 510

### **Edit, Clone, and Delete IPS or Exempt Rules | 511**

Edit IPS or Exempt Rules | 511

Clone IPS or Exempt Rules | 512

Delete IPS or Exempt Rules | 512

## **Managing SSL Proxies | 514**

### **SSL Forward Proxy Overview | 514**

Supported Ciphers in Proxy Mode | 516

Server Authentication | 517

Root CA | 518

Trusted CA List | 518

Session Resumption | 519

SSL Proxy Logs	519
About the SSL Proxy Policy Page	520
Tasks You Can Perform	521
Field Descriptions	521
Creating SSL Proxy Policy Intents	522
Editing, Cloning, and Deleting SSL Proxy Policy Intents	526
Editing SSL Proxy Policy Intents	527
Cloning SSL Proxy Policy Intents	527
Deleting SSL Proxy Policy Intents	528
Understanding How SSL Proxy Policy Intents Are Applied	529
Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match	529
Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match	530
Example 3: Applying SSL Proxy Policy Intents on Internal (Site-to-Site) Traffic	530
About the SSL Proxy Profiles Page	531
Tasks You Can Perform	531
Widget Descriptions	532
Creating SSL Forward Proxy Profiles	533
Editing, Cloning, and Deleting SSL Forward Proxy Profiles	539
Editing SSL Forward Proxy Profiles	540
Cloning SSL Forward Proxy Profiles	540
Deleting SSL Forward Proxy Profiles	541
Configuring and Deploying an SSL Forward Proxy Policy	542
<b>Deploying Policies  </b>	<b>544</b>
Deploying Policies Overview	544
About the Deployments Page	545
Tasks You Can Perform	545
Field Descriptions	545
Using the Deployment Icon to Deploy Policies	547
Deploying Policies	548

## Managing Network Services and Shared Objects

### Configuring Network Services in a Distributed Deployment | 551

Network Service Overview | 551

About the Network Services Page | 552

Tasks You Can Perform | 552

Field Descriptions | 552

About the Service Overview Page | 554

Tasks You Can Perform | 554

Field Descriptions | 554

About the Service Instances Page | 556

Tasks You Can Perform | 556

Field Descriptions | 557

Configuring VNF Properties | 558

vSRX VNF Configuration Settings | 558

LxCIPtable VNF Configuration Settings | 564

Cisco CSR-1000v VNF Configuration Settings | 566

Riverbed Steelhead VNF Configuration Settings | 568

### Managing Shared Objects | 570

Addresses and Address Groups Overview | 571

About the Addresses Page | 571

Tasks You Can Perform | 571

Field Descriptions | 572

Creating Addresses or Address Groups | 573

Editing, Cloning, and Deleting Addresses and Address Groups | 575

Editing Addresses and Address Groups | 576

Cloning Addresses and Address Groups | 576

Deleting Addresses and Address Groups | 577

Services and Service Groups Overview | 577

About the Services Page | 578

Tasks You Can Perform | 578

Field Descriptions | 578

Creating Services and Service Groups | 579

Creating Protocols	581
Editing and Deleting Protocols	584
Editing Protocols	585
Deleting Protocols	585
Editing, Cloning, and Deleting Services and Service Groups	586
Editing Services and Service Groups	586
Cloning Services or Service Groups	587
Deleting Services and Service Groups	587
Application Signatures Overview	588
About the Application Signatures Page	589
Tasks You Can Perform	589
Field Descriptions	589
Understanding Custom Application Signatures	590
Adding Application Signatures	592
Editing, Cloning, and Deleting Application Signatures	597
Editing Application Signatures	597
Cloning Application Signatures	598
Deleting Application Signatures	598
Adding Application Signature Groups	599
Editing, Cloning, and Deleting Application Signature Groups	600
Editing Application Signature Groups	600
Cloning Application Signature Groups	600
Deleting Application Signature Groups	601
About the Departments Page	601
Tasks You Can Perform	602
Field Descriptions	602
Adding a Department	602
Deleting a Department	603

## Monitoring Jobs and Audit Logs

### Managing Jobs | 606

#### About the Jobs Page | 606

Tasks You Can Perform | 606

Field Descriptions | 606

Field Descriptions | 607

Editing and Deleting Scheduled Jobs | 608

Editing Scheduled Jobs | 609

Deleting Scheduled Jobs | 609

Viewing Job Details | 610

Retrying a Failed Job on Devices | 611

## Managing Audit Logs | 612

Audit Logs Overview | 612

About the Audit Logs Page | 613

Tasks You Can Perform | 613

Viewing the Details of an Audit Log | 614

Exporting Audit Logs | 617

Purging Audit Logs (After Archiving or Without Archiving) | 618

## Monitoring Alarms, Events, and Threats

### Monitoring Security Alerts and Alarms | 623

About the Monitor Overview Page | 623

Tasks You Can Perform | 623

Field Descriptions | 624

Alerts Overview | 625

About the Generated Alerts Page | 625

Tasks You Can Perform | 626

Field Descriptions | 626

About the Alert Definitions Page | 627

Tasks You Can Perform | 627

Field Descriptions | 627

**Managing Security Alerts Definitions | 628****Tasks You Can Perform | 628****Field Descriptions | 628****Creating Security Alert Definitions | 629****Editing, Cloning, and Deleting Security Alert Definitions | 631****Editing Security Alert Definitions | 631****Cloning Security Alert Definitions | 631****Deleting Security Alert Definitions | 632****About the Alarms Page | 633****Tasks You Can Perform | 633****Field Descriptions | 634****Monitoring Security and Device Events | 635****About the All Security Events Page | 635****Tasks You Can Perform | 635****Summary View | 636****Detail View | 636****About the Firewall Events Page | 640****Tasks You Can Perform | 640****Summary View | 640****Detail View | 641****About the Web Filtering Events Page | 643****Tasks You Can Perform | 643****Summary View | 643****Detail View | 644****About the IPsec VPNs Events Page | 646****Tasks You Can Perform | 646****Summary View | 646****Detail View | 647****About the Content Filtering Events Page | 648****Tasks You Can Perform | 648****Summary View | 648****Detail View | 649**

**About the Antispam Events Page | 650****Tasks You Can Perform | 650****Summary View | 651****Detail View | 651****About the Antivirus Events Page | 652****Tasks You Can Perform | 652****Summary View | 653****Detail View | 653****About the IPS Events Page | 655****Tasks You Can Perform | 655****Summary View | 655****Detail View | 656****About the Device Events Page | 658****Tasks You Can Perform | 658****Advanced Search | 658****Field Descriptions | 659****About the Screen Events Page | 662****Tasks You Can Perform | 662****Summary View | 662****Detail View | 663****Monitoring SD-WAN Events | 667****SD-WAN Events Overview | 667****About the SD-WAN Events Page | 668****Tasks You Can Perform | 668****Field Descriptions | 668****Monitoring Applications | 670****About the SLA Performance of a Single Tenant Page | 670****Tasks You Can Perform | 670****Field Descriptions | 671****Viewing the SLA Performance of a Site | 673****SLA Not Met by SLA Profiles | 673****Applications SLA Performance by Throughput | 674**

SLA Performance for ALL | 676

Viewing the SLA Performance of an Application or Application Group | 677

Application Visibility Overview | 679

About the Application Visibility Page | 679

Tasks You Can Perform | 679

Chart View | 679

Grid View | 681

About the User Visibility Page | 683

Tasks You Can Perform | 683

Chart View | 683

Grid View | 685

Viewing Application or User Visibility Data for Specific Sites | 686

Viewing Application Visibility Data for Specific Sites | 686

Viewing User Visibility Data for Specific Sites | 687

## Monitoring Threats | 688

About the Threats Map (Live) Page | 688

Tasks You Can Perform | 689

Field Descriptions | 690

Threat Types | 691

## 8

## Managing Reports

### Security Reports | 695

Reports Overview | 695

About the Security Report Definitions Page | 696

Tasks You Can Perform | 697

Field Descriptions | 697

Scheduling, Generating, Previewing, and Sharing Security Reports | 699

Editing Report Generation Schedule | 699

Generating Reports | 700

Previewing Reports in PDF | 701

Sharing Reports through E-mail | 701



**About the Security Generated Reports Page | 702****Tasks You Can Perform | 702****Field Descriptions | 702****Creating Log Report Definition | 703****Creating Bandwidth Report Definition | 707****Creating ANR Report Definition | 709****Editing, Deleting, and Cloning Log Report Definitions | 712****Editing the Log Report Definition | 712****Deleting Log Report Definitions | 712****Cloning Log Report Definitions | 713****Editing, Deleting, and Cloning Bandwidth Report Definitions | 714****Editing Bandwidth Report Definitions | 714****Deleting Bandwidth Report Definitions | 715****Cloning Bandwidth Report Definitions | 715****Editing, Deleting, and Cloning ANR Report Definitions | 716****Editing ANR Report Definitions | 716****Deleting ANR Report Definitions | 717****Cloning ANR Report Definitions | 717****SD-WAN Reports | 719****About the SD-WAN Report Definitions Page | 719****Tasks You Can Perform | 719****Field Descriptions | 720****Editing, Deleting, and Cloning SD-WAN Report Definitions | 721****Editing the SD-WAN Report Definition | 721****Deleting SD-WAN Report Definitions | 722****Cloning SD-WAN Report Definitions | 722****Creating SD-WAN Tenant Performance Report Definitions | 723****Creating SD-WAN Site Performance Report Definitions | 727****About the SD-WAN Generated Reports Page | 730****Tasks You Can Perform | 730****Field Descriptions | 730**

# About the Documentation

## IN THIS SECTION

- Documentation and Release Notes | xxvi
- Documentation Conventions | xxvi
- Documentation Feedback | xxix
- Requesting Technical Support | xxix

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

## Documentation and Release Notes

To obtain the most current version of all Juniper Networks<sup>®</sup> 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 xxvii 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 xxvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  user@host> <b>configure</b>
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> <b>show chassis alarms</b>  No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies guide names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS CLI User Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>

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

Convention	Description	Examples
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  [edit] root@# <b>set system domain-name</b> <i>domain-name</i>
<b>Text like this</b>	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the [edit <b>protocols ospf area area-id</b>] hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub</b> <default-metric <i>metric</i> >;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  ( <i>string1</i>   <i>string2</i>   <i>string3</i> )
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	

## GUI Conventions

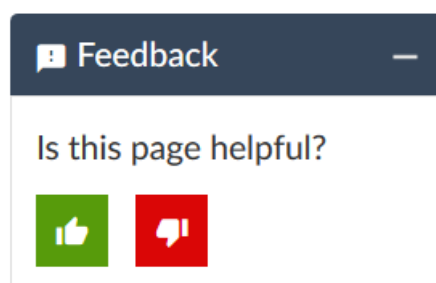
Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

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



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

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

## Self-Help Online Tools and Resources

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

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

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

## Creating a Service Request with JTAC

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

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

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

# 1

PART

## Introduction

---

[Conrail Service Orchestration Overview](#) | 2

[Customer Portal Overview](#) | 3

[Users and Roles](#) | 16

---

# Contrail Service Orchestration Overview

## IN THIS CHAPTER

- [Contrail Service Orchestration Release 5.0.0 | 2](#)

## Contrail Service Orchestration Release 5.0.0

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

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

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

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

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

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



# Customer Portal Overview

## IN THIS CHAPTER

- Customer Portal Overview | 3
- Accessing Customer Portal | 4
- Switching the Tenant Scope | 6
- Setting Up Your Network with Customer Portal | 7
- About the Customer Portal Dashboard | 8
- Changing the Customer Portal Password | 11
- Resetting the Password | 12
- Extending the User Login Session | 14
- Reviewing the Tenant Settings | 14

## Customer Portal Overview

You use Customer Portal to activate and manage sites, customer premises equipment (CPE) devices, and network services in your network. Your service provider sets up the network topology, assigns network services to you, and provides initial login credentials for Customer Portal. You can change your password through Customer Portal after you log in for the first time.

Your network uses one of the following deployment topologies:

- A centralized deployment

In a centralized deployment, virtualized network functions (VNFs) reside in a service provider's cloud in a network point of presence (POP). Sites that access network services in this way are called *cloud sites* in this documentation.

- A distributed deployment

In the distributed deployment, VNFs reside on a CPE device located at a customer's site. These sites are called *on-premise sites* in this documentation.

- A combined centralized and distributed deployment

In this deployment, your network contains both cloud sites and on-premise sites. VNFs for a cloud site reside in the service provider's cloud and VNFs for an on-premise sites reside on the CPE device.

Each connection for a cloud site and each on-premise site can support one network service, although use of a network service on any connection or device is optional.

**NOTE:** NFX250 devices activate automatically when you power them up and configure basic connectivity settings, and you do not need to activate these devices through Customer Portal.

See the NFX250 documentation at:

[https://www.juniper.net/documentation/en\\_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/](https://www.juniper.net/documentation/en_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/)

## RELATED DOCUMENTATION

[Accessing Customer Portal | 4](#)

[Changing the Customer Portal Password | 11](#)

## Accessing Customer Portal

To access Customer Portal:

1. If you are logging in to Customer Portal for the first time, do the following. If not, skip to [2](#).

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

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

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

- b. Change your password following the guidelines provided in [Table 3 on page 5](#).
- c. (Optional) Click the Terms of Use link to view the Terms of Use document.

- d. Click the check box to accept CSO terms of use.
- e. Click **Ok**.

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

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

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

3. Enter your username (E-mail ID) and password.

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

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

5. (Optional) If you want to review the tenant setting, select **Review Settings**.

The Review Settings page appears. For more information see, [“Reviewing the Tenant Settings” on page 14](#).

6. Click **Go to Dashboard**. The menu bar on the left-hand side of the every page allows you to access the different tasks easily. The top-level menu items are listed in [Table 4 on page 6](#).

**Table 3: Fields on the Change Password Page**

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

Table 4: Customer Portal Menu

Menu Name	Description
<b>Dashboard</b>	Configurable dashboard that offers you a customized view of network services through its widgets
<b>Monitor</b>	Monitor alerts and alarms, security, device, and software-defined WAN (SD-WAN) events; applications and jobs
<b>Resources</b>	Manage device and software image, sites, site templates, mesh tags, and site groups
<b>Configuration</b>	Configure network services, shared objects, and policies (firewall, NAT, SD-WAN), and view and manage configuration deployments
<b>Reports</b>	Create report definitions and view reports
<b>Administration</b>	Manage users, licenses, audit logs, tenant settings, certificate management, Identity Management, and the signature database

## RELATED DOCUMENTATION

[Changing the Customer Portal Password | 11](#)

[Customer Portal Overview | 3](#)

## Switching the Tenant Scope

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

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

To switch from one scope to another:

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

## RELATED DOCUMENTATION

*Unified Administration and Customer Portal Overview*

[Role-Based Access Control Overview](#) | 16

## Setting Up Your Network with Customer Portal

Your service provider specifies which sites appear in your network and the network services that you can use. When you start working in Customer Portal, you must set up your network using the available sites and network services.

To set up your network with Customer Portal:

1. You can add an on-premise site from the **Sites** page. Two types of on-premise sites can be added: spoke site and on-premise hub. See [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81](#).
2. Activate the on-premise site.
3. Deploy network services. See [“Managing a Single Site” on page 139](#).
4. View and manage policies.
  - View and manage a firewall policy. See [“Adding Firewall Policy Intents” on page 291](#) and [“Deploying Policies” on page 548](#).
  - View and manage an SD-WAN policy. See *Creating SLA Profiles*, [“Creating SD-WAN Policy Intents” on page 412](#), and [“Deploying Policies” on page 548](#).

## RELATED DOCUMENTATION

[Accessing Customer Portal](#) | 4

## About the Customer Portal Dashboard

To access the dashboard, select **Customer Portal > Dashboard**.

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

You can drag these widgets from the top of the dashboard to your workspace, where you can add, remove, and rearrange them to meet your needs.

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 by using the drag and drop option. In addition, you can press and hold the top portion of the widget to move it to a new location.

### Tasks You Can Perform

You can perform the following tasks from this page:

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

You can then add widgets to the dashboard as needed.

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

### Field Descriptions

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

[Table 5 on page 9](#) describes the dashboard widgets.

Table 5: Widgets on the Customer Portal Dashboard

Widget	Description
Tenant Sites: Total Alerts	<p>Displays the total number of alerts grouped by severity level.</p> <p>Click each alert name to view the total number of tenant sites receiving alerts that are critical, major, or minor.</p>
Top 5 Sites with Alerts	<p>Displays the top five sites in the tenant receiving alerts.</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the tenant site.</li> <li>• <b>Location</b>—Location of the tenant site.</li> <li>• <b>Status</b>—Type of alerts received: critical, major, or minor.</li> </ul>
Top Sites not meeting SLA	<p>Displays a bar chart of the top sites in the tenant that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles not meeting SLA	<p>Displays a bar chart of the top SLA profiles that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on location and period ranging from the last hour to the last month.</p>
Top Sites Switching Links	<p>Displays a column chart of the top sites in the tenant that switched WAN links to meet SLA requirements and the number of link-switch events for the sites.</p> <p>You can sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles Switching Links	<p>Displays a column chart of the top SLA profiles that switched WAN links and the number of link-switch events for the SLA profiles.</p> <p>You can sort the information based on location and period ranging from the last hour to the last month.</p>
Top Applications by Throughput	<p>Displays a bar chart of the top sites in the tenant that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>You can sort the information based on profile, location, and time period.</p>
Firewall: Top Denials	<p>Displays a column chart of the top requests denied by the firewall based on their source IP addresses, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>

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

Widget	Description
Firewall: Top Events	<p>Displays a bar chart of the top firewall events of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IPS: Top Events	<p>Displays the top IPS events of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Applications: Top by Sessions	<p>Displays a bar chart of the top applications with a maximum number of sessions, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Destinations	<p>Displays the top IP destination addresses of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Sources	<p>Displays the top IP source addresses of the network traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Spams by Source IPs	<p>Displays the number of spams detected by the source IPs.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Virus: Top Blocked	<p>Displays viruses with the maximum number of blocks, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
Web Filtering: Top Blocked Websites	<p>Displays a bar chart of websites with the maximum number of blocks, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days.</p>
IP: Top Source IPs by Volume	<p>Displays the top source IP addresses based on volume of traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 15 minutes to 7 days.</p>
Application: Top Application by Volume	<p>Displays the applications based on volume of traffic, sorted by count.</p> <p>You can sort the information based on time period ranging from 5 minutes to 7 days and view the information in a bar chart or a bubble chart.</p>



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

Widget	Description
IP: Top Users/IP by Sessions	<p>Displays the top source IP addresses by sessions, sorted by count.</p> <p>You can sort the information based on time period ranging from 15 minutes to 7 days.</p>
Threat Map: Virus	<p>Displays a world map showing total virus event count across countries.</p> <p>You can sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.</p>
Threat Map: IPS	<p>Displays a world map showing total IPS event count across countries.</p> <p>You can sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.</p>

## RELATED DOCUMENTATION

[Customer Portal Overview](#) | 3

## Changing the Customer Portal Password

To change the Customer Portal password:

1. Click the customer username that is located at the right side of the Customer Portal banner.

The drop-down list appears.

2. Click **Change Password**.

The Change Password page appears.

3. Specify the current password.

4. In the New Password text box, specify 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.

You must change the password periodically (every 90 days) and you cannot reuse the old password. Your user account will be locked after five consecutive unsuccessful login attempts.

5. In the Confirm Password text box, specify your new password again.

Select the Show Password option to view the password.

6. Click **OK**.

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

## RELATED DOCUMENTATION

[Customer Portal Overview | 3](#)

[Accessing Customer Portal | 4](#)

## Resetting the Password

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

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

To reset the password:

1. On the login page, enter the username , and then press **Enter**.
2. 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.

3. 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.

- 4. Click **OK**.  
The Reset Password page appears.
- 5. Change your password following the guidelines provided in [Table 6 on page 13](#).
- 6. Click **OK**.

Your password is reset.

**Table 6: Fields on the Reset Password Page**

Field	Description
Username	Enter your username.
New Password	<p>Enter your new password.</p> <p>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.</p> <p><b>NOTE:</b> The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select <b>Show Password</b> to view the password.</p>

RELATED DOCUMENTATION

<a href="#">Accessing Customer Portal   4</a>
<a href="#">Changing the Password on First Login</a>
<a href="#">Changing the Customer Portal Password   11</a>

## 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 Customer Portal Password](#) | 11

## Reviewing the Tenant Settings

In Customer Portal you can review or modify the tenant settings before you proceed to add a site.

To review the tenant settings:

1. Select **Administration > Tenant Settings**.

The Review Settings page appears.

**NOTE:** If you are logging in to Customer Portal for the first time, on the Welcome Screen page select **Review Settings**.

2. Modify the tenant settings.

[Table 7 on page 15](#) describes the tenant settings that you can modify.

**Table 7: Tenant Settings That Can be Modified**

Tenant Capability	Tenant settings that can be modified
Tenant with SD-WAN capability	<p>You can modify the following settings only before adding a site for a tenant:</p> <ul style="list-style-type: none"><li>• SSL Settings</li><li>• VPN authentication</li><li>• Overlay Tunnel Encryption</li><li>• Network Segmentation</li></ul> <p>You can modify the following settings even after you add sites for a tenant:</p> <ul style="list-style-type: none"><li>• Dynamic VPN Threshold</li><li>• Tenant-Specific Attributes</li></ul> <p><b>NOTE:</b> The changed settings are applicable to only newly-added sites.</p> <p>For more information on these settings, see <i>Adding a Single Tenant</i>.</p>
Tenant with Hybrid WAN capability	Tenant-Specific Attributes
Tenant with Next Gen Firewall capability	Tenant-Specific Attributes
Tenant with LAN capability	Tenant-Specific Attributes

3. Click **Save**.

The changes that you made for the tenant are saved. A confirmation message is displayed indicating that the job is created and subsequently that the job was successful.

You can verify the changes that you made on the Tenant Settings page.

RELATED DOCUMENTATION

| [About the Sites Page](#) | 40

# Users and Roles

IN THIS CHAPTER

- [Role-Based Access Control Overview | 16](#)
- [About the Users Page in Customer Portal | 17](#)
- [Adding Tenant and OpCo Tenant Users | 19](#)
- [Editing and Deleting Tenant and OpCo Tenant Users | 21](#)
- [Resetting the Password for Tenant Users | 22](#)
- [Roles Overview | 23](#)
- [About the Tenant Roles Page | 26](#)
- [Adding User-Defined Roles for Tenant Users | 27](#)
- [Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 28](#)
- [Access Privileges for Role Scopes \(Tenant and Operating Company\) | 31](#)

## Role-Based Access Control Overview

Contrail Service Orchestration supports the authentication and authorization of users. Both service provider and tenant users access the pages within the unified Administration and Customer Portal based on their role and access permissions.

In addition to predefined roles, CSO enables you to add object-based custom roles. You can create custom roles and assign access privileges (read, create, update, delete, and other actions) to each role.

[Table 8 on page 16](#) shows predefined service provider, tenant, and OpCo roles and their access privileges.

Table 8: Roles and Access Privileges

Role	Role Scope	Access Privileges
Tenant Admin	Tenant	Users with the Tenant Admin role have full access to the Customer Portal UI and APIs. They can add one or more users with the Tenant Administrator or Tenant Operator roles.

Table 8: Roles and Access Privileges (*continued*)

Role	Role Scope	Access Privileges
Tenant Operator	Tenant	Users with the Tenant Operator role have read-only access to the Customer Portal UI and APIs.
OpCo Admin	Operating Company	Users with the OpCo Admin role have full access to the OpCo's Administration Portal UI or API capabilities. They can use the UI or APIs to add one or more users with OpCo Admin, OpCo Operator, and custom roles. They can onboard tenants, and add the first tenant user during the OpCo's tenant onboarding process. They can also add tenant administrators or operators by switching the scope to a specific tenant.
OpCo Operator	Operating Company	Users with the OpCo Operator role have read-only access to the OpCo's Customer Portal UI and APIs.

## RELATED DOCUMENTATION

[About the Users Page in Customer Portal](#) | 17

## About the Users Page in Customer Portal

To access the Users page for a tenant or OpCo tenant, click **Administration > Users** in the Customer Portal.

Use this page to manage tenants and OpCo tenant users in the Tenant and OpCo scopes respectively. In the Tenant scope, the SP Admin, SP Operator, Tenant Admin, and Tenant Operator can access the Users page for tenants. The SP Admin and the SP Operator can switch scope from all tenants to a specific tenant.

In the OpCo scope, the SP Admin, SP Operator, OpCo Admin and OpCo Operator can access the OpCo Tenant Users page.

For information about the predefined roles and access permissions of OpCo tenant users and tenant users, see *Role-Based Access Control Overview*.

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

- **Local Authentication** —The **Users** page lists local users that you can add, edit, and delete.
- **Authentication and Authorization with SSO Server**—The **Users** page is not displayed because users are externally managed in the single sign-on (SSO) server.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Add a tenant user or an OpCo tenant user. See [“Adding Tenant and OpCo Tenant Users” on page 19](#).
- Edit or delete a tenant user or an OpCo tenantuser. See [“Editing and Deleting Tenant and OpCo Tenant Users” on page 21](#).
- View details of users in the respective scope. See [Table 9 on page 18](#).
- Show or hide columns about users. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a user. Click the Search icon in the top right corner of the page to search for a user.

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

The search results are displayed on the same page.

### Field Descriptions

[Table 9 on page 18](#) describes the fields on the Users page for the Tenant and OpCo scopes in the Customer Portal.

Table 9: Fields on the Users Page

Field	Description
Username	Username of the user.  Example: <i>abc@example.com</i>
First Name	First name of the user.
Last Name	Last name of the user.
Status	Indicates whether the user is enabled (can log in to CSO) or disabled (cannot log in to CSO).
Role	Depending on the scope selected, indicates the roles assigned to the tenant or OpCo tenant user.  By default, this column lists only one role assigned to the user. When a user is assigned more than one role, a <b>+&lt;integer&gt;</b> icon (for example: +2) appears to the right of the role. The integer indicates the number of additional roles assigned to the user. Click on the integer to view the additional roles.



Table 9: Fields on the Users Page (continued)


Field	Description
Last Login	Date and time of the last login. The format is MM/DD/YYYY HH:MM.  Example: 07/22/2017 20:07  A date and time is not displayed when a user has not logged in to the Customer Portal.

RELATED DOCUMENTATION

| [Switching the Tenant Scope](#) | 6

## Adding Tenant and OpCo Tenant Users

Use the Add Tenant User page and Add OpCo Tenant User page in the Customer Portal to add tenant users and OpCo tenant users respectively to Contrail Service Orchestration (CSO). After you add a user, the user receives an e-mail with the initial login credentials.

**NOTE:** To add users, you should be assigned a role, such as Tenant Admin, that allows you to add users.

To add a tenant user or an OpCo tenant user:

1. Select **Administration > Users**.  
  
The Users page appears.
2. Click the add icon (+) or click **Add User button**. The Add User button appears when there are no users configured in the scope.  
  
In the Tenant scope, the Add Tenant User page appears. In the OpCo scope, the Add OpCo Tenant User page appears.
3. Complete the configuration as described in [Table 10 on page 20](#).
4. Click **OK** to save the changes. If you want to discard the changes, click **Cancel**.

If you click OK, a confirmation message indicating that the user account is created appears and the user account is listed on the Users page.

To enhance the security related to login credentials, an automatically generated password is sent to the e-mail address that you have specified for the user. You are prompted to change the password when you login to the portal with the automatically generated password. For more information about changing the password on first login, see *Changing the Password on First Login*.

**Table 10: Fields on the Add Tenant User and Add OpCo Tenant User Pages**

Field	Description
<b>First Name</b>	Enter the first name as a string of alphanumeric characters, some special characters [underscore ( _ ) and period(.)], and spaces. The maximum length allowed is 32 characters.
<b>Last Name</b>	Enter the last name as a string of alphanumeric characters, some special characters [underscore ( _ ) and period(.)] and spaces. The maximum length allowed is 32 characters.
<b>Username (E-mail)</b>	Enter a valid e-mail address in the <i>user@domain</i> format.
<b>Status</b>	Click the toggle button to enable or disable the user.  By default, the status is enabled. A user can log in to CSO only when the status is enabled.
<b>Role</b>	Select one or more roles (both predefined and custom) that you want to assign to the tenant or OpCo tenant user.  The following predefined roles are available—Tenant Operator, Tenant Admin, and ConfigureSite. To know more about the predefined roles for tenant users and OpCo tenant users, see <i>Role-Based Access Control Overview</i> .  Click the right-arrow icon to move the selected roles from the <b>Available</b> column to the <b>Selected</b> column. Note that you can use the search icon on the top right of each column to search for role names.  Click the role name to preview the access privileges assigned to the tenant user.

## Editing and Deleting Tenant and OpCo Tenant Users

### IN THIS SECTION

- [Editing Tenant and OpCo Tenant Users | 21](#)
- [Deleting Tenant and OpCo Tenant Users | 22](#)

You can edit the information of tenant and OpCo tenant users and delete one or more users.

**NOTE:** To edit and delete users, you should be assigned a role, such as Tenant Admin, that allows you to edit and delete users.

### Editing Tenant and OpCo Tenant Users

To modify a tenant user or an OpCo tenant user:

1. Select **Administration > Users**.

The Users page appears.

2. Select the user that you want to modify, and click the edit icon.

In the Tenant scope, the Edit Tenant User page appears. In the OpCo scope, the Edit OpCo Tenant User page appears.

3. Modify the parameters following the guidelines provided in [Table 10 on page 20](#).

**NOTE:** You cannot modify the **Username (E-mail)** field.

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

If you click OK, a confirmation message indicating that the user information is modified appears on top of the Users page.

## Deleting Tenant and OpCo Tenant Users

To delete one or more tenant users and OpCo tenant users:

1. Select **Administration > Users**.

The Users page appears.

2. Select the users that you want to delete and click the delete icon.

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

3. Click **Yes** to delete the users or click **No** to cancel the deletion.

If you click **Yes**, a confirmation message indicating that the selected users account are deleted from CSO appears on top of the Users page.

## Resetting the Password for Tenant Users

Users with the Tenant Administrator role can reset the password for tenant users. Also, users with the Update capability for Users objects can reset the password for tenant users.

To reset the password:

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

The Users page appears, displaying a list of tenant users.

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

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

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

A confirmation message appears, indicating that the password has been successfully reset, and an e-mail with a new system-generated password is sent to the user.

The user can use the new system-generated password to log in to CSO.

### RELATED DOCUMENTATION

| [About the Users Page in Customer Portal](#) | 17

## Roles Overview

### IN THIS SECTION

- [Types of Roles | 23](#)
- [Role Scopes | 24](#)
- [Access Privileges | 24](#)
- [Relationship Between User, Roles, and Access Privileges | 24](#)
- [Benefits of role-based access control \(RBAC\) | 25](#)

A role is a function assigned to a user that defines the tasks that the user can perform within CSO. Each user can be assigned one or more roles depending on the tasks that the user is expected to perform.

User roles enable you to classify users based on the privileges to perform tasks on CSO objects. Roles assigned to a user determine the tasks and actions that the user can perform.

This topic contains the following sections:

### Types of Roles

There are two types of roles: predefined roles and custom roles.

- **Predefined roles**—System-defined roles with a set of predefined access privileges assigned to a user to perform tasks within the CSO application. Predefined roles are created in the system during CSO installation. For more information about predefined roles, see *Role-Based Access Control Overview*.
- **Custom roles**—Object-based user-defined roles with a set of access privileges assigned to a user to perform tasks within the CSO application. Objects include menu and submenu items (for example, Resources, Devices, Images, and POPs) in the CSO application, from which you can create, edit, clone, and delete objects.

Custom roles can be created by:

- An OpCo Administrator, or a Tenant Administrator.
- A tenant user with the Create Role privilege. This user can create custom roles for tenant users.
- An OpCo user with the Create Role privilege. This user can create custom roles for both OpCo and tenant users.

You can create custom roles and assign access privileges to each role by using the Roles page (**Administration > Roles**).

You can assign one or more roles to a user when you create or edit a user account. Each role can have one or more access privileges.

## Role Scopes

A role scope defines the specific scope, which is assigned to the role, such as service provider, OpCo, or tenant. An OpCo Administrator can assign OpCo, and tenant roles to OpCo users and tenant roles to tenant users. A Tenant Administrator can assign tenant roles only to tenant users. A role can have the following scopes:

- **Tenant**—Represents a customer that can view, configure, and manage its sites through Customer Portal.
- **Operating Company (OpCo)**—Similar to a service provider that can manage its own tenants. Tenants managed by one OpCo are isolated from tenants of another OpCo. An OpCo can manage all activities related to its own tenants.

## Access Privileges

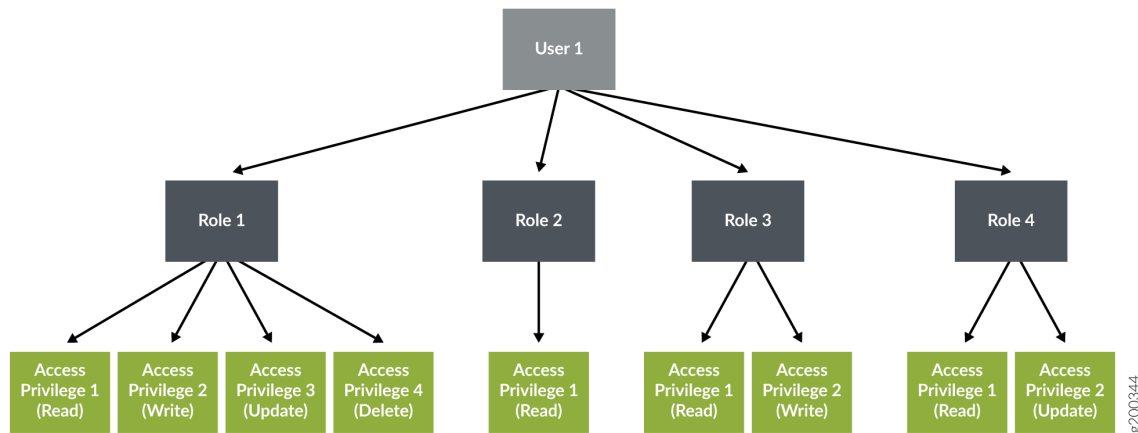
The following access privileges and actions can be assigned to a user role:

- Read
- Create
- Update
- Delete
- Other actions (Example: For device templates object, the following other actions are supported: Clone and Edit Device Template) .

## Relationship Between User, Roles, and Access Privileges

[Figure 1 on page 25](#) shows the relationship between a user, user roles, and access privileges. A user can have one or more roles and each role can have one or more access privileges.

Figure 1: Relationship Between User, Roles, and Access Privileges



### Benefits of role-based access control (RBAC)

- CSO provides pre-defined and user-defined set of roles for day-to-day system operations on the unified Administration and Customer portal.
- Controls which system users can view, read, write, and execute objects based on certain business and operation needs.
- Provides granular level access control on CSO objects within each navigation menu.
- Helps service providers in upselling advanced features to their tenants as a power user.
- CSO supports RBAC and authenticate users using local authentication and the external Single Sign On (SSO) server.

### RELATED DOCUMENTATION

[About the Tenant Roles Page | 26](#)

[Adding User-Defined Roles for Tenant Users | 27](#)

[Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 28](#)

## About the Tenant Roles Page

To access this page, select **Administration > Roles** in the Customer Portal.

You can use the Roles page to view a list of predefined (system-defined) and custom (user-defined) roles that can be assigned to tenant users. You can create, edit, or delete custom roles and clone both custom and predefined roles.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a custom role for the tenant users. See [“Adding User-Defined Roles for Tenant Users” on page 27](#).
- Edit, clone, or delete a custom role. See [“Editing, Cloning, and Deleting User-Defined Roles for Tenant Users” on page 28](#).

### Field Descriptions

[Table 11 on page 26](#) describes the fields on the Roles page.

Table 11: Fields on the Roles Page

Field	Description
Role Name	Displays the name of the role.
Role Scope	Displays the scope of the role.
Role Type	Displays whether the role is a predefined role or a custom role.
Created By	Displays the name of the user that created the role.

### RELATED DOCUMENTATION

[Roles Overview | 23](#)

[Role-Based Access Control Overview | 16](#)

[Adding User-Defined Roles for Tenant Users | 27](#)

[Editing, Cloning, and Deleting User-Defined Roles for Tenant Users | 28](#)



## Adding User-Defined Roles for Tenant Users

Use the Add Role page to create custom (user-defined) roles and assign access privileges (read, create, update, delete, and other actions) to the tenant user roles.

A Tenant Administrator or a user with the Create Role privilege can create custom roles for tenant users.

To create a custom role:

1. Select **Administration > Roles** in Customer Portal.

The Roles page appears.

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

The Add Role page appears.

3. Complete the configuration according to the guidelines provided in [Table 12 on page 27](#).

4. Click **OK**.

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

Table 12: Fields on the Add Role Page

Field	Description
Role Name	Enter a unique role name. The name can contain alphanumeric characters, underscore, period, and space.
Description	Enter a description for the role.
Role scope (Visibility)	Select the scope of the role.  If you select the scope as Tenant, then the Privileges section of the page displays all the objects of Customer Portal.

Table 12: Fields on the Add Role Page (continued)

Field	Description
Privileges	<p><b>All Objects</b>—Displays the objects of the Customer Portal. You must select the check box against each object and then select the type of privileges (read, create, update, delete, and other actions (schedule, deploy, reboot, activate, retry, schedule update, schedule delete, and so on)) that you want to assign the user for the selected object. You can select one or more access privileges to assign to the tenant user role.</p> <p><b>NOTE:</b> You must assign at least one access privilege to a role.</p> <p>If you select the first-level objects, the submenu items that belong to the main object and the corresponding access privileges are selected by default.</p> <p>The following access privileges can be assigned to a user role:</p> <ul style="list-style-type: none"><li>• <b>Read</b>—Enables the user to read existing objects.</li><li>• <b>Create</b>—Enables the user to create new objects.</li><li>• <b>Update</b>—Enables the user to modify existing objects.</li><li>• <b>Delete</b>—Enables the user to delete existing objects.</li></ul> <p>You can also assign other actions to tenant roles. The other actions include retry, schedule update, schedule delete, activate, reboot, push license, RMA, deploy, schedule, start, disable, deploy, move, run, send, preview, renew, configure, and download.</p>

RELATED DOCUMENTATION

<a href="#">Roles Overview   23</a>
<a href="#">Role-Based Access Control Overview   16</a>
<a href="#">About the Tenant Roles Page   26</a>
<a href="#">Editing, Cloning, and Deleting User-Defined Roles for Tenant Users   28</a>

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

IN THIS SECTION

- [Editing Roles | 29](#)
- [Cloning Roles | 29](#)
- [Deleting Roles | 30](#)

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

**NOTE:** You cannot modify or delete the predefined roles.

## Editing Roles

To modify the parameters configured for a role.

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

2. Select the role that you want to edit and click the edit icon (pencil) to modify the parameters.

The Edit Role page appears. The fields on the Edit Role page are available for editing.

**NOTE:** You cannot modify the role name and role scope.

3. Modify the role description and privileges as needed.

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

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

## Cloning Roles

You can clone a role (both custom and predefined) when you want to quickly create a copy of an existing role and modify its access privileges.

**NOTE:** You cannot modify the role name and role scope.

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

2. Select the role that you want to clone and then click the **Clone** button at the top-right corner of the page.

The Clone Role: *Role-Name* page appears.

3. Specify an appropriate name for the new clone role.

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

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

The name of the clone role is displayed on the Roles page.

5. Select the new clone role and click the edit icon (pencil) to modify its parameters.

The Edit Role page appears.

6. Select the objects, and modify the access privileges of the role, as needed.

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

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

## Deleting Roles

To delete a role name:

1. Select **Administration > Roles**.

The Roles page appears, displaying the existing role names.

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

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

3. Click **Yes** to delete the selected role name.

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

## RELATED DOCUMENTATION

*About the Roles Page*

*Adding User-Defined Roles for OpCo, and Tenant Users*

## Access Privileges for Role Scopes (Tenant and Operating Company)

This topic describes the access privileges for the tenant and Operating company (OpCo) role scopes. For more information about roles and role scopes, see [“Roles Overview” on page 23](#).

[Table 13 on page 32](#) shows the access privileges for operating company scope.

[Table 14 on page 34](#) shows the access privileges for tenant scope.

Table 13: Access Privileges for Operating Company Scope

Role Scope	Menu Name	Actions	Other Actions
Operating company (OpCo)	SP Geo Map	Read	-
	Tenants SLA Performance	Read	-
	Alerts	Read and Delete	-
	Alarms	Read	-
	SD-WAN Alerts Definitions	Read	-
	Security Alert Definitions	Read	-
	Device Events	Read	Manage Filter
	Jobs	Read	Retry Schedule Update Schedule Delete
	POPs	Read	-
	provider hub Devices	Read	-
	Tenant Devices	Read	-
	Device Templates	Read, Create, Update, and Delete	Clone Edit Template
	Images	Read	-
	Application SLA Profiles	Read, Create, Update, and Delete	-
	Application Traffic Type Profiles	Read	-
	Tenants	Read, Create, Update, and Delete	-

Table 13: Access Privileges for Operating Company Scope (*continued*)

Role Scope	Menu Name	Actions	Other Actions
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Authentication	Read, Create, Update, and Delete	-
	Licenses	Read, Create, Update, and Delete	Push License
	Signature Database	Read	-
	SMTP	Read, Create, Update, and Delete	-
	Email Templates	Read and Update	-
	Getting Started	Read	-
	What's New	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

Table 14: Access Privileges for Tenant Scope

Role Scope	Menu Name	Actions	Other Actions
Tenant	Tenant GeoMap	Read	-
	Link Switch Events	Read	-
	Jobs	Read	Retry Schedule Update Schedule Delete
	SD-WAN Alert Definitions	Read	-
	Security Alert Definitions	Read, Create, Update, and Delete	-
	Alerts	Read and Delete	Jump to Event Viewer
	Alarms	Read and Delete	
	Security Events	Read	Manage Filter Create Alert Create Report
	Device Events	Read	Manage Filter Create Alert
	Application Visibility	Read	-
	Threats Map (Live)	Read	-
	Application SLA Performance	Read	-
	Devices	Read and Delete	



Table 14: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
			Activate Push License Reboot RMA Traceroute Ping Discover APs Configure Stage-2
	Device Configuration	Read and Update	-
	Images	Read	Upgrade History Deploy Stage
	Deployments	Read	Deploy Schedule
	Network Services	Read, Update, and Delete	Start Disable
	SD-WAN Policy	Read and Update	Deploy
	Tenant SLA Based Steering Profiles	Read, Create, Update, and Delete	-
	Tenant Path Based Steering Profiles	Read, Create, Update, and Delete	-
	Cloud Breakout Policy	Read, Create, Update, and Delete	Assign Sites
	Firewall Policy	Read, Create, Update, and Delete	Deploy
	SSL Policy	Read, Create, Update, and Delete	Deploy

Table 14: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	NAT	Read, Create, Update, and Delete	Deploy
	UTM	Read, Create, Update, and Delete	-
	Schedule	Read, Create, Update, and Delete	-
	Address	Read, Create, Update, and Delete	-
	Department	Read, Create, and Delete	-
	Service	Read, Create, Update, and Delete	-
	Application Signature	Read, Create, Update, and Delete	Clone
	Site Management	Read, Create, and Delete	Configure Upgrade
	Site Groups	Read, Create, Update, and Delete	-
	Site LAN Segment	Read, Create, and Delete	Deploy Deploy History Re-assign
	Report Definitions - Security	Read, Create, Update, and Delete	Run/Preview Send Clone
	Report Definitions - SD-WAN	Read, Create, Update, and Delete	Run/Preview Send Clone
	Generated Reports -Security	Read and Delete	-
	Generated Reports SD-WAN	Read and Delete	-

Table 14: Access Privileges for Tenant Scope (continued)

Role Scope	Menu Name	Actions	Other Actions
	Users	Read, Create, Update, and Delete	-
	Roles	Read, Create, Update, and Delete	-
	Device Licenses	Read, Create, Update, and Delete	Push License
	CSO Licenses	Read	
	Tenant Setting	Read, create, and update	
	Tenant Signature Database	Read	Install
	Certificates	Read, Create, Update, and Delete	-
	VPN Authentication	Read	Renew CRL
	Identity Management	Read and Update	-
	Wi-Fi Settings	Read and Update	-
	Getting Started	Read	-
	What's New	Read	-
	Help Center	Read	-
	FAQ	Read	-
	Release Notes	Read	-
	About	Read	-

## RELATED DOCUMENTATION

---

[About the Tenant Roles Page | 26](#)
[Role-Based Access Control Overview | 16](#)

# 2

PART

## Managing Sites, Site groups, and Site Templates

---

Managing Sites | **39**

Managing Site Groups | **144**

Managing Site Templates | **146**

Managing Mesh Tags | **167**

Managing Dynamic VPN | **170**

---

# Managing Sites

## IN THIS CHAPTER

- About the Sites Page | 40
- Multihoming Overview | 42
- Enterprise Hubs Overview | 42
- Adding and Provisioning Switches to Provide LAN Capability to a Site Overview | 44
- Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities | 48
- Adding Provider Hub Sites for SD-WAN Deployment | 63
- Adding Cloud Spoke Sites for SD-WAN Deployment | 64
- Provisioning a Cloud Spoke Site in AWS VPC | 72
- Manually Adding On-Premise Spoke Sites | 76
- Adding an On-Premise Spoke Site with Hybrid WAN Capability | 76
- Adding an On-Premise Spoke Site with SD-WAN Capability | 81
- Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities | 94
- Adding an On-Premise Spoke Site with LAN Capability | 110
- Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities | 114
- Adding and Provisioning a Next Generation Firewall Overview | 121
- Adding a Switch to an Existing Site | 123
- Enabling Integration with Mist Access Points | 128
- Adding a Standalone Firewall Site | 128
- Managing LAN Segments on a Tenant Site | 133
- Managing a Single Site | 139
- Viewing the Sites History | 140
- Deleting a Site | 142

## About the Sites Page

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

You can use the **Sites** page to view existing sites and to add different types of sites (such as spoke sites and hub sites) manually and by using a site template. You can also use this page to view site configuration and device activation information.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Add a provider hub site. See [“Adding Provider Hub Sites for SD-WAN Deployment” on page 63](#).
- Manually add on-premise spoke sites. See [“Manually Adding On-Premise Spoke Sites” on page 76](#).
- Add multiple on-premise spoke sites by using a site template. See [“Adding On-Premise Spoke Sites by Using a Site Template” on page 147](#).
- Add an enterprise hub site. See [“Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities” on page 48](#).
- Add multiple sites by uploading a JSON file. See [“Adding and Configuring Sites by Importing a JSON File” on page 165](#).
- Add a switch to an existing site. See [“Adding a Switch to an Existing Site” on page 123](#).
- Click on the site name to view the site details and to manage the site. See [“Managing a Single Site” on page 139](#).
- View the jobs executed to add and delete sites for a tenant. see [“Viewing the Sites History” on page 140](#).
- Delete a site. See [“Deleting a Site” on page 142](#).
- View device activation logs. See [“Viewing the History of Tenant Device Activation Logs” on page 198](#).

### Field Descriptions

[Table 15 on page 40](#) describes the fields on the **Sites** page.

Table 15: Fields on the Sites Page

Field	Description
Alert Icon	<p>Alert associated with the site. The alert can be critical (indicated by a red icon), major (indicated by an orange icon), or minor (indicated by a yellow icon).</p> <p><b>NOTE:</b> The alert icon is displayed only if there is an alert associated with the site. If there is no alert, no icon is displayed.</p>

Table 15: Fields on the Sites Page (*continued*)

Field	Description
Site Name	<p>Name of the tenant site.</p> <p>Click the name of the site to go to the <i>Site-Name</i> page where you can view the site details and configure parameters related to the site. See <a href="#">“Managing a Single Site” on page 139</a>.</p>
Location	Location of the tenant site.
Template	Displays whether an on-premise spoke site is associated with a site template (displays site template name) or not (-).
Sites Connected To	<p>Number of sites to which the site is connected or N/A (not applicable) if no sites are connected.</p> <p>Mouse over the number to view the list of sites to which the site is connected.</p>
Operational Status	Operational status (Up or Down) of the site.
Type	Indicates whether a site is an on-premise site or a cloud site.
Site Status	<p>The current status of the site:</p> <ul style="list-style-type: none"> <li>• Created—Indicates that the site was added but not configured.</li> <li>• Configured—Indicates that the site was configured but not activated.</li> <li>• Provisioned—Indicates that the site is provisioned (activated).</li> <li>• Upgrade-Required—Indicates that the site needs to be upgraded.</li> <li>• Maintenance—Indicates that the site upgrade is in progress; any deployments that might occur because of other jobs are skipped when the site status is Maintenance.</li> </ul>
Role	Indicates whether the site is a hub site or a spoke site.
Local Breakout	Indicates whether local breakout is enabled for at least one WAN link of the site. If it is enabled for at least one WAN link, the number of links on which local breakout is enabled is also displayed. Mouse over the number to view the list of links on which local breakout is enabled.
Version	Contrail Service Orchestration (CSO) version in which the site was added.

## RELATED DOCUMENTATION

## Multihoming Overview

Multihoming is the ability of a spoke site to connect to two different hub devices in a hub and spoke topology, thereby providing redundancy. The hub devices function as primary and the secondary hub devices. If there are multiple spokes in the system, the same hub device may act as primary hub device for one spoke and secondary hub device for another spoke. That is, the selection of the primary and the secondary hub devices is only in the context of a spoke site. The spoke is connected to both the hub devices through an underlay network.

The hub devices can be MX series routers with an MS-MIC or SRX4000 series routers. For a specific spoke site, both the hub devices must be either MX series routers or SRX series routers. You cannot have one hub as an MX series router and another hub as an SRX series router. To enable multihoming for a site, you must select the hub and spoke topology when you create the tenant. If you enable multihoming for a site, you must specify a primary and back up site when you configure the site.

Traffic is switched from the primary hub to the secondary hub in the following scenarios:

- The primary hub is down
- The primary hub is up, but all the overlay tunnels between the spoke and the primary hub are down
- The tunnels are up, but the iBGP session between the primary hub and vRR is down. In this case, the failover occurs only after the BGP hold-time expires and the default route is withdrawn.

**NOTE:** In addition to hub-level redundancy, you can provide VRR-level redundancy by creating two VRRs—primary and secondary—in two different redundancy groups.

## Enterprise Hubs Overview

### IN THIS SECTION

- [Benefits of Enterprise Hubs](#) | 44



An *enterprise hub* is an SD-WAN site that is used to carry site-to-site traffic between on-premise spoke sites and to break out backhaul (central breakout) traffic from on-premise spoke sites. An enterprise hub typically has a data center department behind it; however, this is not enforced in Contrail Service Orchestration (CSO). You add a enterprise hub from the **Sites** page.

You can add one or more enterprise hubs to act as central breakout (backhaul) nodes and then associate enterprise hubs with on-premise spoke sites. The enterprise hub that is associated with a spoke site functions like a data hub and performs the following functions:

- Before the creation of site-to-site tunnels, site-to-site traffic to or from a spoke site is sent through the enterprise hub. This traffic triggers the creation of the site-to-site tunnel based on dynamic VPN thresholds and matching mesh tags that you configure for the spoke site.
- If Internet-bound traffic from the spoke site (and all departments associated with the spoke site) is destined for central breakout (backhaul), the traffic first reaches the assigned enterprise hub and then breaks out from the enterprise hub.
- If a provider hub is associated with the spoke site, the provider hub works as a fallback option in case traffic cannot be sent through the enterprise hub.

**NOTE:** You must attach an on-premise spoke site (with SDWAN capability) to a provider hub site or an enterprise hub site, or to both hub sites.

If a tenant has more than one enterprise hub configured, CSO statically meshes these sites with overlay tunnels so that the enterprise hubs can exchange routing information for the on-premise spoke sites with which they are associated. This enables the site-to-site communication between the spoke sites that are associated with different enterprise hubs.

The creation of static tunnels between one enterprise hub and another and between a enterprise hub and a spoke site depends on matching mesh tags. These static tunnels are created during the Zero Touch Provisioning (ZTP) workflow. For more information about mesh tags, see [“Mesh Tags Overview” on page 167](#).

Enterprise hubs can have their own departments similar to other sites. If an enterprise hub does not have directly connected LAN segments in the departments used by the associated spoke sites, then CSO automatically pushes the appropriate department virtual routing and forwarding (VRF) instances to the enterprise hub for connectivity.

## Benefits of Enterprise Hubs

- Because enterprise hubs can be used to carry backhaul (central breakout) traffic and are used as an anchor for site-to-site traffic, the volume of traffic sent to the provider hub (controlled by the service provider) is reduced.

## RELATED DOCUMENTATION

| [Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities](#) | 48

## Adding and Provisioning Switches to Provide LAN Capability to a Site Overview

You can use Contrail Service Orchestration (CSO) to provision, deploy, and monitor EX Series switches in branch deployments of enterprise networks. You can deploy an EX Series switch by connecting to a Customer Premise Equipment (CPE) (SRX Series devices only) functioning as a secure SD-WAN router or next-generation firewall. You can also connect the EX Series switch to a third-party Internet gateway device.

CSO Release 5.0.0 supports only EX2300, EX3400, EX4300, Series switches.

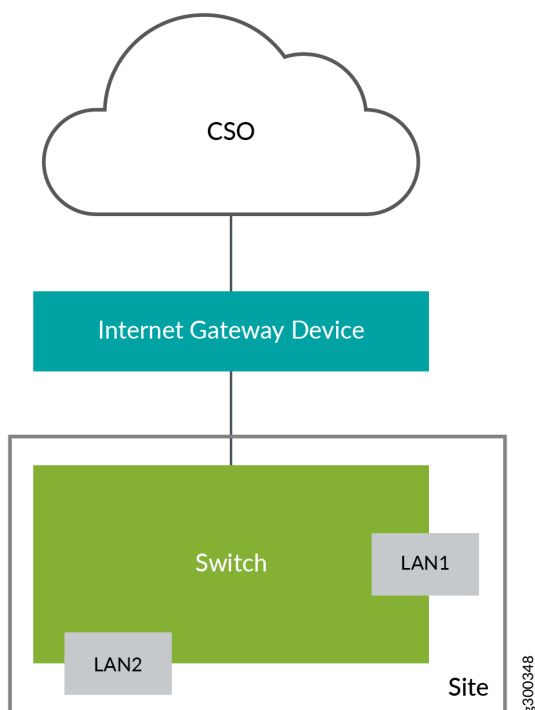
You can provision a switch on a branch network by using CSO in one of the following ways:

- By adding a site with the switch and connecting it to an Internet gateway device.
- By adding a site with an SD-WAN CPE and the switch.
- By adding a site with a next-generation firewall site and the switch.
- By adding a site with an enterprise hub and the switch.
- By adding the switch to an SD-WAN CPE that is already provisioned and managed by CSO.
- By adding the switch to a next-generation firewall site that is already provisioned and managed by CSO.
- By adding the switch to an enterprise hub site that is already provisioned and managed by CSO.

## Standalone Switch Overview

[Figure 2 on page 45](#) shows a site with LAN capability managed by CSO.

Figure 2: Site With LAN Capability (Standalone Switch)



In [Figure 2 on page 45](#), the EX Series switch is connected to CSO through an internet gateway. The gateway can be a device from a manufacturer other than Juniper Networks.

The EX Series switch does not support Phone-Home client in the CSO 5.0.0 release. When provisioning a standalone switch, you must manually copy the stage-1 configuration to the switch during site activation. CSO then deploys the stage-2 configuration on the switch. See [“Adding an On-Premise Spoke Site with LAN Capability” on page 110](#) for details.:

### Switch Behind a CPE or Next Generation Firewall Overview

[Figure 3 on page 46](#) shows a site with SD-WAN and LAN capabilities managed by CSO.

Figure 3: Site with LAN and SD-WAN Capabilities

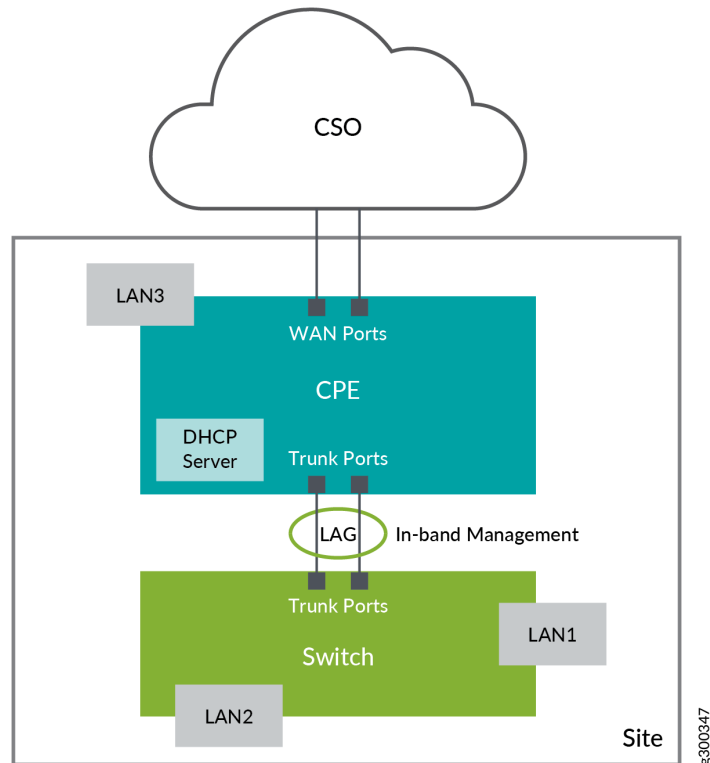
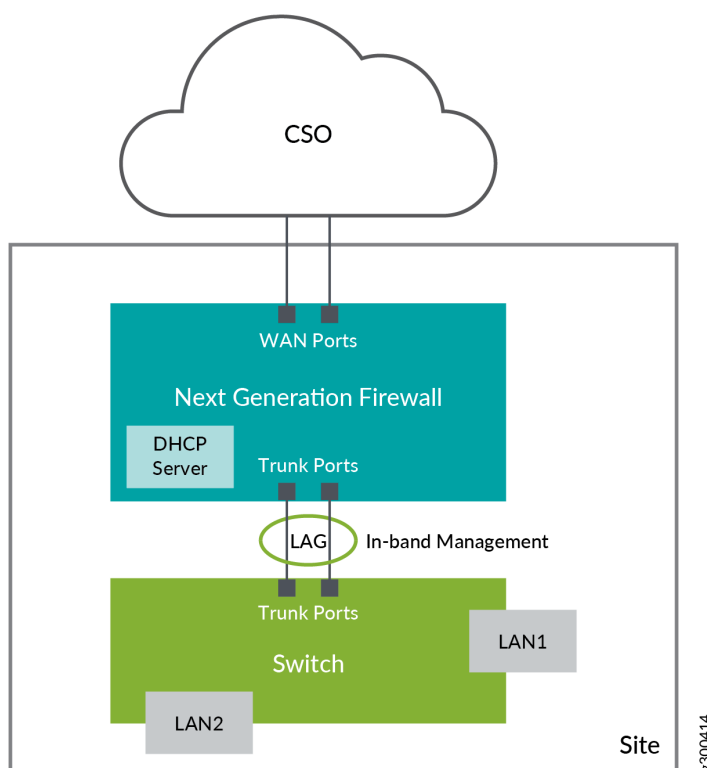


Figure 3 on page 46 shows an example of a switch configured behind a CPE where the switch is connected to two LAN segments (LAN1 and LAN2) and the CPE. The CPE is connected to a LAN segment (LAN3) and to the EX Series switch. The switch can also be connected to a next-generation firewall as shown in Figure 4 on page 47.

Figure 4: Site with LAN and Next-Generation Firewall Capabilities



**NOTE:** You cannot add a LAN segment to the next-generation firewall by using CSO.

The switch and the CPE or firewall can be connected through a trunk port. However, you can use two trunk ports to connect the CPE and the switch and combine them to form a Link Aggregation Group (LAG) for higher throughput and redundancy. Traffic from LAN segments connected to the switch are routed to the CPE or firewall through the trunk ports for further routing into WAN.

You can manage the switch by in-band management, where in, the trunk ports carry the management traffic in addition to data.

**NOTE:** The ae0 port of the SRX Series device is configured as the trunk port for communication with the switch.

The DHCP server, configured on the CPE or firewall, runs on the trunk ports to:

- Allocate unique IP addresses to the access devices connected to the switch.
- Provide management connectivity to the switch.

During ZTP of a site with both WAN and LAN capabilities, the switch is provisioned after the CPE or firewall is provisioned.

When you add a switch to an already provisioned site, CSO redeploys the stage-2 configuration on the CPE or firewall to configure DHCP and LAG. The DHCP configuration enables management connectivity to the switch and allows CSO to discover and provision the switch.

## Monitoring Switches Overview

You can monitor the following for an EX Series switch on the *Device-Name* page (**Resources > Devices**):

- Resource utilization (memory and CPU) on the switch for the past one hour, past eight hours, past one day, past one week, and past one month.
- Status of ports.
- Alerts and alarms generated on the switch for the past one hour, past eight hours, past one day, past one week, and past one month.
- Top Ports consuming the maximum bandwidth.
- Top Ports with the maximum number of errors.
- Top Ports with the maximum packet loss.

## RELATED DOCUMENTATION

[Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities | 94](#)

[Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities | 114](#)

[Adding an On-Premise Spoke Site with LAN Capability | 110](#)

[Adding a Switch to an Existing Site | 123](#)

[Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities | 48](#)

## Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities

An enterprise hub is an SD-WAN site that is used to carry site-to-site traffic between on-premise spoke sites and to break out backhaul (central breakout) traffic from on-premise spoke sites. An enterprise hub *typically* has a data center department behind it; however, this is not enforced in Contrail Service Orchestration (CSO). The following device templates are supported for enterprise hubs:

- SRX as SD-WAN CPE (vSRX only)
- Dual SRX as SD-WAN CPEs
- SRX4x00 as SD-WAN CPE
- Dual SRX4x00 as SD-WAN CPEs

To add an enterprise hub:

**NOTE:** You can add enterprise hubs only for tenants with real-time optimized SD-WAN mode.

1. Click **Resources > Site Management**.

The Sites page appears.

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

The **Add Enterprise Hub for *Tenant-Name*** page appears.

3. Do one of the following: Complete the configuration settings according to the guidelines provided in [Table 16 on page 50](#).

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

- To create an enterprise hub with only SD-WAN capability, complete configuration settings according to guidelines provided in [Table 16 on page 50](#).
  - To create an enterprise hub with both SD-WAN and LAN capabilities, complete configuration settings according to guidelines provided in [Table 16 on page 50](#) for the WAN capability and [Table 17 on page 58](#) for LAN capability.
4. (Optional) You can review the configuration in the **Summary** tab and modify the settings, if required.
  5. Click **OK**.

The site activation job is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the enterprise hub and the switch (when LAN capability is selected). The enterprise hub is activated first and then the process to activate the switch is initiated.

Go to the next step if you have selected LAN capability for the site.

6. To activate the switch, you must manually configure the stage-1 configuration on the switch.
- a. On the Site Activation page, after the Prestage Device step completes successfully for the switch, the **View Stage-1 Configuration** link appears next to the Prestage Device step.

b. Click the **View Stage-1 Configuration** link.
- The Stage-1 Configuration page appears displaying the stage-1 configuration.
- c. Copy the stage-1 configuration and log in to the CLI of the EX Series switch.

d. Enter the configuration mode, paste, and commit the configuration.
- After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.

Table 16: Add Enterprise Hub for <Tenant-Name> Settings (WAN Capability)

Field	Description
General	
Site Information	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
Site Capabilities	
WAN Capabilities	SD-WAN capability is selected by default. You cannot clear the selection.
LAN Capabilities	Select <b>LAN</b> if you want to include LAN capability in the enterprise hub site.
Configuration	



Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Primary Provider Hub	<p>Select the provider hub site (or primary provider hub site in case of multihoming) to which you want to connect the enterprise hub site.</p> <p>If you do not specify a provider hub site, then the enterprise hub site can connect only to the on-premise spoke sites that are associated with the enterprise hub site.</p> <p>If you specify a provider hub site, then the enterprise hub site can also connect to the on-premise spoke sites to which that provider hub site is associated.</p>
Secondary Provider Hub	<p>Select the secondary provider hub site (in case of multihoming) to which you want to connect the enterprise hub site.</p> <p>When the primary provider hub is down, the enterprise hub connects to the secondary provider hub and the on-premise spoke sites to which that provider hub site is associated.</p>
<b>On-Demand VPN Threshold</b>	
Threshold for Tunnel Creation	<p>Specify the threshold for the number of sessions (flows) closed (in a two-minute duration) between the enterprise hub and a destination site. When the number of sessions closed exceeds the specified threshold, a tunnel is created between the enterprise hub and the destination site.</p> <p>The default value is 5.</p> <p>For example, if you specify the Create Threshold as 5, dynamic VPN tunnels are created if the number of sessions closed between the enterprise hub and destination site exceeds 5 in 2 minutes.</p>
Threshold for Tunnel Deletion	<p>Specify the threshold for the number of sessions closed (in a 15-minute duration) between the enterprise hub and a destination site. When the number of sessions closed is lower than the specified threshold, the tunnel between the enterprise hub and destination site is deleted.</p> <p>The default value is 2.</p> <p>For example, if you specify the number of sessions closed as 2, dynamic VPN tunnels between the enterprise hub and destination site are deleted if the number of sessions closed is lesser than or equal to 2.</p>
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	<p>Select the country where the site is located.</p> <p>You can click the <b>Validate</b> button to verify the address that you specified:</p> <ul style="list-style-type: none"> <li>• The <b>site address verification successful</b> message is displayed if the address can be verified. You can click the <b>View location on a map</b> link to see the address location.</li> <li>• If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	<p>Enter the phone number of the contact person for the site.</p> <p>Click <b>Next</b> to continue.</p>
<b>Advanced Configuration</b>	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
<b>WAN</b>	
<b>Device Profile</b>	

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Device Series	Select the device series to which the CPE belongs.
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
<b>Device Information</b>	
Serial Number  <b>NOTE:</b> Primary Serial Number and Secondary Serial Number fields appear when a template for dual CPE is selected.	<p>Enter the serial number of the CPE device.</p>
Auto Activate	<p>Click the toggle button to enable (default) or disable automatic activation of the CPE device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the CPE device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i>.</p>
Firewall Policies	Select a firewall policy to be applied on the site.
<b>WAN Links</b>	
WAN_0	<p>This field is enabled by default.</p> <p>Enter parameters related to WAN_0. Fields marked with an asterisk (*) must be configured to proceed.</p>

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Link Type	Select whether the link would be an MPLS link or Internet link.
Egress Bandwidth	Enter the maximum bandwidth (in Mbps) that the CPE allows towards the WAN link.  Range: 1 through 10,000.
Address Assignment	Select the method of assigning an IP address to the WAN link—DHCP or STATIC.  If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.
Gateway IP Address	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
<b>Advanced Settings</b>	
Provider	Enter the name of the service provider providing the WAN service.
Cost/Month	Enter the cost for using the WAN link per month and select the currency in which the cost is indicated from the adjacent drop-down list.  Range: 1 through 10,000.  In bandwidth-optimized SD-WAN, CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.
Enable Local Breakout	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.  <b>NOTE:</b> <ul style="list-style-type: none"> <li>• If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent.</li> <li>• If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.</li> </ul>

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Breakout Options	When the <b>Enable Local Breakout</b> field is enabled, select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.
Autocreate Source NAT Rule	<p>If the WAN link is enabled for local breakout, you can click the toggle button to automatically create an interface-based source NAT rule on the WAN link. The automatically-created source NAT rule is implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>By default, this field is disabled.</p> <p><b>NOTE:</b> If this option is enabled for a WAN interface W1 during the site addition workflow, a series of NAT source rules are automatically created. Each automatically created NAT rule is from a zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following zone to W1 interface rule-set might be created:</p> <pre>Zone1 --&gt; W1: Translation=Interface Zone2 --&gt; W1: Translation=Interface Zone3 --&gt; W1: Translation=Interface</pre> <p>To manually override any of these rules, you can create a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant zone and WAN interface as the source and destination. For example:</p> <pre>Zone1 --&gt; W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Zone1, Port 56578 --&gt; W1: Translation=Pool-2</pre>
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a full mesh topology.</p> <p>A site can have a maximum of three links enabled for meshing.</p>
Mesh Overlay Link Type	<p>When <b>Use for Fullmesh</b> field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC.</p> <ul style="list-style-type: none"> <li>• If the link type is Internet, the value for mesh overlay link type is GRE_IPSEC.</li> <li>• If the link type is MPLS, select one of the following options: <ul style="list-style-type: none"> <li>• GRE-IPSEC</li> <li>• GRE</li> </ul> </li> </ul>
Mesh Tag	<p>When the <b>Use for Fullmesh</b> field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <ul style="list-style-type: none"> <li>• For an on-premise spoke site, you can select one mesh tag.</li> <li>• For an enterprise hub you can select one or more mesh tags.</li> </ul> <p>For more information about mesh tags, see <a href="#">“Mesh Tags Overview” on page 167</a>.</p>
Connects to Hubs	<p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted.</li> <li>• For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.</li> </ul>
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>Select the mesh overlay tunnel type—GRE and GRE_IPSEC.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	<p>Displays the peer hub device to which the site is connected.</p>

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
Overlay Peer Interface	Select the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, SLA data is not monitored for the backup link.</p>
Default Link	<p>Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site.</p> <p>Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.</p>
Data VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 2 through 4093.</p>
WAN_1	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for <b>WAN_0</b> for an explanation of the fields</p>
WAN_2	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for <b>WAN_0</b> for an explanation of the fields</p>
WAN_3	<p>Click the toggle button to enable or disable (default) the WAN link.</p> <p>When you enable the WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed. Refer to the fields described for <b>WAN_0</b> for an explanation of the fields</p>
Management Connectivity	

Table 16: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (WAN Capability) (continued)

Field	Description
IP Prefix	Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14.

Refer to [Table 18 on page 60](#) for configuring LAN segments.

Table 17: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (LAN Capability)

Field	Description
-------	-------------

## LAN

**NOTE:** This tab is enabled only if you select **LAN** under LAN Capabilities in General Settings.

### Device Profile

Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, and EX4300.
Device Model	Select the model for the switch you specified in the Device Type.  The models vary in the number and type of ports the switch contains. For example, if you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.

### CPE Settings

Trunk Ports	Select at least two trunk ports on the CPE device to connect with the switch.  The trunk ports are used for carrying the following: <ul style="list-style-type: none"> <li>• LAN traffic between the switch and the CPE.</li> <li>• Management traffic for in-band management of the switch.</li> </ul>
-------------	---



Table 17: Add Enterprise Hub for &lt;Tenant-Name&gt; Settings (LAN Capability) (continued)

Field	Description
Switch Management Subnet	<p>Specify the subnet that the DHCP can use to assign IP addresses. The DHCP server runs on the following ports:</p> <ul style="list-style-type: none"> <li>• Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE.</li> <li>• Out-of-band management port on the CPE to provide DHCP information to the management port on the switch.</li> <li>• LAN ports on the CPE to provide information to the devices connected to the CPE LAN ports.</li> </ul>
<b>Switch Details</b>	
Serial Number	Specify the serial number of the switch.
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the switch is automatically triggered when the device communicates with CSO.</p> <p>By default, auto activation for the switch is enabled or disabled if it is enabled or disabled for the CPE.</p> <p><b>NOTE:</b> You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when you enable this option.</p>
Activation code	<p>When the <b>Auto activate</b> field is disabled, enter the activation code to be used for manually activating the switch. .</p> <p>For information about manually activating a switch, see <a href="#">“Manually Activating a Switch” on page 184</a>.</p>
Zero Touch Provisioning	<p>ZTP must be disabled for all EX Series switches for the CSO 5.0.0 release.</p> <p>The Stage-1 configuration must be copied and pasted onto the CLI of the switch during site activation. See <a href="#">“Step-by-Step Procedure” on page 49</a> for details.</p>
LAN Segments	<p>Displays the LAN segment that you configure on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See <a href="#">Table 18 on page 60</a>.</p>

Table 18: Add LAN Segment Settings

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
Type	<p>Select the type of LAN segment:</p> <ul style="list-style-type: none"> <li>• Directly Connected (default)—Indicates that the LAN segment is directly connected to the site.</li> <li>• Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.</li> </ul>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>
Department	<p>Select a department to which the LAN segment is assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.</p>
Protocol	<p>For dynamically routed LAN segments, select the routing protocol (BGP or OSPF) to be used by the data center department to learn routes from the data center.</p>
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment.</p> <p>For example: 192.0.2.8/24.</p>
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP (default).</p> <p>You can enable DHCP if you want to assign IP addresses by using a DHCP sever or disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, additional fields appear on the page.</p>
Additional Fields	

Table 18: Add LAN Segment Settings (*continued*)

Field	Description
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server.</p> <p>Default: 1440</p> <p>Range: 0 through 4,294,967,295 seconds.</p>
Name Server	<p>Specify one or more IPv4 addresses of the DNS server.</p> <p>To enter more than one DNS server address, type the address, press Enter, and then type the next address.</p> <p><b>NOTE:</b> DNS servers are used to resolve hostnames into IP addresses.</p>
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the Switch device and creates the same LAN segment on the Switch.</li> </ul> <p>If you click to exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field.</p> <p>CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is a physical SRX Series device.</p>
Switch Ports  <b>NOTE:</b> This field is displayed only when LAN capability is selected for the enterprise hub.	<p>If you disable the CPE ports field, select ports on the switch to be part of the LAN segment. The Switch ports and CPE ports are mutually exclusive.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>
<b>BGP Configuration</b>	

Table 18: Add LAN Segment Settings (*continued*)

Field	Description
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• None—Indicates that no authentication should be used. This is the default.</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> </ul>
Peer IP Address	Enter the IP address of the BGP neighbor.
Peer AS Number	Enter the autonomous system (AS) number BGP neighbor.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
OSPF Configuration	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default).</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> <li>• None—Indicates that no authentication should be used.</li> </ul>
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.

## RELATED DOCUMENTATION

[About the Sites Page](#) | 40

## Adding Provider Hub Sites for SD-WAN Deployment

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

To add a provider hub site:

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

The Sites page appears.

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

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

3. Complete the configuration settings according to the guidelines provided in [Table 19 on page 63](#).

4. Click **OK**.

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

Table 19: Fields on the Provider Hub for Tenant-Name Page

Field	Description
<b>Configuration</b>	
Service POP	Select the name of the point of presence (POP) for the site. A network POP is a location at which a service provider instantiates a network function, such as a virtualized network function (VNF).
Hub Device Name	Select the provider hub device for the hub site. The provider hub devices with <b>DATA_ONLY</b> capability and <b>DATA_AND_OAM</b> capability are listed.  <b>NOTE:</b> You need not onboard a provider hub with OAM_ONLY capability. By default, the provider hub with OAM_ONLY capability will be imported.

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)

[About the Site Groups Page | 144](#)

## Adding Cloud Spoke Sites for SD-WAN Deployment

A cloud spoke represents an automation endpoint (virtual machine (VM) or an EC2 Instance) running a Juniper Networks vSRX image in the Amazon Web Services(AWS) virtual private cloud (VPC). The cloud spoke sites are connected to the hub sites using the overlay connections. You create a cloud spoke site from the **Sites** page. This topic describes how to add a cloud spoke site for a tenant.

### NOTE:

- You can add a cloud spoke site only in hub-and-spoke topology.
- To ensure that only hub-and-spoke topology is created, we recommend you to disable the DVPN configuration while adding the tenant.
- You cannot add a cloud spoke site in full mesh topology.

To add a cloud spoke site:

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

The Sites page appears.

2. Click **Add** and select **Add Cloud Spoke**.

The **Add On-Premise Spoke Site for Tenant Name** page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 20 on page 65](#).

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

4. Review the configuration and modify the settings, if needed, from the **Summary** tab.

5. Click **OK**.

The newly added cloud spoke site is displayed on the **Sites** page.

Table 20: Fields on the Add Cloud Spoke Site Page

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a unique name for the site. Enter a unique string of alphanumeric characters and special character (-). The maximum length is 15 characters.  Example: aws-cloud-spoke
Site Group	(Optional) Select a site group to which you want to assign the site.  Example: cloud-spoke
<b>Site Capabilities</b>	
WAN Capabilities	Select <b>SD-WAN</b> to include SD-WAN capabilities in the cloud spoke site
<b>Configuration</b>	
Primary Provider Hub	Select the hub site to which the spoke site must connect.
<b>Advanced Configuration</b>	
Name Server IP List	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone for the site.
<b>WAN</b>	
Device Template	Click a device template to select the plan for WAN connectivity.  A device template contains information such as device family, a list of SD-WAN features supported, and the number of links supported.  <b>NOTE:</b> vSRX as SD-WAN spoke in AWS template supports cloud spoke site for AWS VPC.

Table 20: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
<b>Cloud Information</b>	
Region	<p>Select the region to which the site belongs. The regions in CSO are mapped to the regions in the AWS account.</p> <p>Example: Ohio</p>
VPC ID	<p>Enter the VPC ID from the AWS account.</p> <p>To obtain VPC ID:</p> <ol style="list-style-type: none"> <li>1. Log in to your AWS account.</li> <li>2. Search for the VPC service.</li> <li>3. Click the VPC dashboard.</li> <li>4. Select a VPC ID.</li> </ol> <p>Ensure that the VPC is connected to an Internet gateway.</p> <p>To check whether VPC is attached:</p> <ol style="list-style-type: none"> <li>1. Log in to your AWS account.</li> <li>2. Search for the VPC service.</li> <li>3. Click the Internet Gateway dashboard.</li> <li>4. Check whether the VPC state is <b>attached</b>.</li> </ol> <p>Example: vpc-6d810314</p>
Management Subnet	<p>Specify whether CSO must create a new subnet or use an existing subnet from the AWS account. The management subnet of vSRX is used to push the initial stage-1 configuration. The following options are available:</p> <ul style="list-style-type: none"> <li>• Use an existing subnet in AWS account</li> <li>• Create new</li> </ul>



Table 20: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
IP Prefix	<p>Enter the management IP prefix. The first four IP addresses in the subnet are reserved by AWS. For example, IP addresses x.x.x.0/x through x.x.x.3/x are always reserved by AWS. Hence, provide an IP address prefix other than the reserved IP address prefix.</p> <p>Example: 105.0.1.5/24</p>
<b>Device Information</b>	
Activation Code	<p>Enter the activation code of the primary device that your service provider supplied for the device. If you do not want to specify an activation code, on the Template Settings page, disable the ACTIVATION_CODE_ENABLED field and save the changes.</p>
<b>WAN Links</b>	
WAN_0 (ge-0/0/0) WAN_1 (ge-0/0/1)	<p>Select the check boxes to configure the WAN links. You can configure up to two WAN links per site that support SD-WAN.</p>
Link Type	Displays the connection type for WAN underlays. Only Internet link is supported.
Egres Bandwidth	Enter the maximum bandwidth (in Mbps) to be allowed for a specific WAN link.
Address Assignment	<p>Select the method of assigning an IP address to the WAN link—DHCP or STATIC.</p> <ul style="list-style-type: none"> <li>• If you select DHCP, the IP address is provided by using the DHCP server of the service provider of the WAN link.</li> <li>• If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.</li> </ul>
Static IP Prefix	<p>If you configure the address assignment method as STATIC, enter the private IPv4 address of the WAN link from the subnet. For example, if the IPv4 CIDR address is 105.0.2.0/24 for a WAN interface in the AWS account, then enter any IP address within the subnet. The first four IP addresses in the subnet are reserved by AWS. Hence, provide an IP prefix other than the reserved IP prefix.</p> <p>Example: 105.0.2.12/24</p>
Gateway IP	<p>If you configured the address assignment method as STATIC, enter the IPv4 address for the gateway of the WAN service provider. Typically, the first IP address in the subnet is selected for gateway IP address.</p> <p>Example: 105.0.2.1</p>

Table 20: Fields on the Add Cloud Spoke Site Page (continued)

Field	Description
Elastic IP	<p>Elastic IP address is a public, static IPv4 address designed for dynamic cloud computing. The public IP address is mapped to the private subnet IP using one-to-one NAT. You must allocate the IP addresses based on the number of WAN links that are enabled. For example, If two WAN links are enabled, then you must allocate two elastic IP addresses.</p> <p>Example: 34.213.255.184</p>
<b>Advanced Settings</b>	Based on the connectivity requirement, the following fields are populated:
Provider	Enter the name of the service provider (SP).
Cost/Month	Enter the cost per month of the subscribed bandwidth in the specified currency. In bandwidth-optimized SD-WAN, this information is used to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.
Enable Local Breakout	<p>Click the toggle button to enable or disable (default) local breakout on the WAN link.</p> <ul style="list-style-type: none"> <li>• If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent.</li> <li>• If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.</li> </ul>
Breakout Options	Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.

Table 20: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Autocreate Source NAT Rule	<p>If the WAN link is enabled for local breakout, you can click the toggle button to automatically create an interface-based source NAT rule on the WAN link. The automatically-created source NAT rule is implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>By default, this field is disabled.</p> <p><b>NOTE:</b> If this option is enabled for a WAN interface W1 during the site addition workflow, a series of NAT source rules are automatically created. Each automatically created NAT rule is from a zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following zone to W1 interface rule-set might be created:</p> <pre>Zone1 --&gt; W1: Translation=Interface Zone2 --&gt; W1: Translation=Interface Zone3 --&gt; W1: Translation=Interface</pre> <p>To manually override any of these rules, you can create a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant zone and WAN interface as the source and destination. For example:</p> <pre>Zone1 --&gt; W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Zone1, Port 56578 --&gt; W1: Translation=Pool-2</pre>
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>Select the mesh overlay tunnel type—GRE and GRE_IPSEC.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>

Table 20: Fields on the Add Cloud Spoke Site Page (*continued*)

Field	Description
Overlay Peer Device	Displays the peer hub device to which the site is connected.
Overlay Peer Interface	Select the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	<p>Select a backup link through which traffic can be routed when the primary links are unavailable. You cannot select the default link as the backup link. Note that you cannot assign the backup link for exclusive breakout traffic (the <b>Use only for breakout traffic</b> option). If local breakout is enabled for the site, the breakout traffic is also routed through the backup link when the breakout link is not available.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, note that the SLA data is not monitored for the backup link.</p>
Default Links	<p>Select the default links that must be used for routing traffic. The site can have multiple default links to the hub site as well as to the Internet.</p> <p>Default links are used primarily for overlay traffic but can be used for local breakout traffic as well. A default link cannot be used exclusively for local breakout traffic. The default link is optional and in case it is not chosen, all links are used through equal-cost multipath (ECMP).</p>
<b>Management Connectivity</b>	
IP Prefix	<p>Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14</p> <p>Example: 192.0.2.10/32</p>
<b>LAN</b>	Add at least one LAN segment.
LAN Segment	<p>Displays the LAN segment that you configure on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See <a href="#">Table 21 on page 70</a>.</p>

Table 21: Fields on the Add LAN Segment Page

Field	Description
<b>Add LAN Segment</b>	

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

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters. No spaces are allowed and the maximum length is 15 characters.</p>
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.</p>
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the switch device and creates the same LAN segment on the switch.</li> </ul> <p>If you exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field. CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is an SRX Series device.</p>

## RELATED DOCUMENTATION

[Provisioning a Cloud Spoke Site in AWS VPC | 72](#)

[About the Sites Page | 40](#)

[About the Site Groups Page | 144](#)

## Provisioning a Cloud Spoke Site in AWS VPC

### IN THIS SECTION

- Add a Cloud Spoke Site | 72
- Download the Cloud Formation Template | 73
- Provision the Device on AWS Server | 74
- Activate the Device | 75

Use the following high-level steps to provision a vSRX cloud spoke site in Amazon Web Services (AWS) virtual private cloud (VPC).

Before you begin:

- Set up your Amazon Web Services (AWS) account.
- Identify the virtual private cloud (VPC) in which the AWS spoke site must be provisioned.
- Install licenses to use vSRX features. Choose any of the following AWS vSRX Image Licenses.
  - Bring Your Own License (BYOL)— If you plan to use a BYOL, then you must install the license on the device before deploying CSO SD-WAN functionality. See <https://aws.amazon.com/marketplace/pp/B01LYWCGDX>.
  - License included. See <https://aws.amazon.com/marketplace/pp/B01NAUWN0G>.
- Ensure that you have the supported software version for the AWS spoke.
- Reserve two elastic IP (public IP) addresses on AWS.

To set up and monitor your network:

### Add a Cloud Spoke Site

To add a cloud spoke site:

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

The Sites page appears.

2. Click **Add > Add Cloud Spoke**.

The **Add On-Premise Spoke Site for *Tenant-Name*** page appears.

3. Specify the site information such as, site name, AWS region, VPC ID, management subnet, IP prefix and click **Next**.
4. Specify vSRX as SD-WAN spoke in AWS as the device template.

**NOTE:**

- Only hub-and-spoke topology is supported for AWS cloud spoke site.
- Only Internet link is supported for WAN underlay connections.

5. Provide the WAN details and click **Next**.

The WAN traffic page appears, displaying a set of values for the WAN link configuration.

6. Specify additional requirements and click **Next**.
7. Specify LAN segment information and click **Next**.
8. In the **Summary** tab, check the configuration and click **Edit** to modify the settings.
9. Click **OK** to save the changes.

The new cloud spoke site that you created appears in the Sites page.

## Download the Cloud Formation Template

To download the cloud formation template:

1. Click **Resources > Devices**.

The Devices List page appears.

2. Select the device and click **Cloud Info Template**.

The Cloud Info Template page appears.

3. Click **Download** to download the cloud formation template.

The template is downloaded to your local computer in JSON format.

## Provision the Device on AWS Server

CSO creates cloud formation template with stage-1 configuration bundled in JSON format. You must download this template and then upload to AWS to provision the vSRX. The cloud formation template creates the required resources such as subnet, interface, vSRX and so on and applies the stage-1 configuration.

To provision the device on AWS server:

1. Log in to your AWS account.
  - If you have already logged in to your AWS account, the Create Stack page appears.
  - If you are not logged into your AWS account, a new Web page opens in your browser, displaying the AWS login information. Log in to your AWS account.

**TIP:** If you do not see the Create Stack page when you log in to or access your AWS account, then search for CloudFormation service.

The Create Stack page appears.

2. Select **CloudFormation > Stacks > Create Stack > Upload a template to Amazon S3**.
3. Click **Choose File** and select the cloud formation template that you downloaded in JSON format .
4. Click **Next**.
5. Specify the Stack name. For example, Oregonstack.
6. In the Parameters section, specify the KeyName for your EC2 instance.
7. Click **Next**.
8. Select **I acknowledge that AWS CloudFormation might create IAM Resources**.
9. Click **Create**.

The Create Stack pages displays a list of existing stacks and indicates that it is creating the stack that you requested. The create stack process takes up to 30 minutes. if the process does not complete in 30 minutes, a timeout occurs and you need to retry the process.



## Activate the Device

To activate the device:

1. After the create stack process is complete, return to the Customer Portal and click **Next**.

The Activate Device page displays a status indicating that CSO is detecting the provisioning agent. This process takes up to 30 minutes. If the process does not complete in 30 minutes, a timeout occurs and you need to retry the process.

**NOTE:** You need not download the cloud formation template again. You can log in to the Customer Portal, access the Activate Device page, enter the activation code and click **Next**. After the CREATE\_COMPLETE message is displayed on the AWS server, click Next on the Activate Device page to proceed with device activation.

If the spoke on AWS has been spawned successfully on AWS, it will contact CSO through outbound SSH connection. The device is detected and normal ZTP process is triggered. The rest of the workflow is consistent with the normal on-premise workflow.

On Device Activation page, the device is activated through the following steps:

- Detecting the device
- Applying stage-one configuration to the device
- Bootstrapping of device
- Activating the device

After each successful step, you can see a green check mark. If any of these steps fails, a red exclamation mark appears.

2. After the activation process is complete, click **OK**.

The Sites page appears. To see the device activation status, hover over the device icon on the Sites page.

## RELATED DOCUMENTATION

---

[Adding Cloud Spoke Sites for SD-WAN Deployment | 64](#)  
[vSRX Deployment Guide for AWS](#)

## Manually Adding On-Premise Spoke Sites

An on-premise site can be added with one WAN capability (SD-WAN, or Hybrid WAN, or Next Gen Firewall), LAN capability, or both WAN and LAN capabilities.

**NOTE:** The WAN and LAN capabilities that are displayed in the Add On-premise Spoke Site page are filtered based on the service types that are assigned to the tenant.

For more information on adding an on-premise spoke site with the following capabilities:

- WAN capability as SD-WAN, see [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81](#).
- WAN capability as Hybrid WAN, see [“Adding an On-Premise Spoke Site with Hybrid WAN Capability” on page 76](#).
- WAN capability as Next Gen Firewall, see [“Adding a Standalone Firewall Site” on page 128](#).
- WAN capability as SD-WAN and LAN capability, see [“Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities” on page 94](#).
- WAN capability as Next Gen Firewall and LAN capability, see [“Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities” on page 114](#).
- Only LAN capability, see [“Adding an On-Premise Spoke Site with LAN Capability” on page 110](#).

## Adding an On-Premise Spoke Site with Hybrid WAN Capability

You add an on-premise spoke site with Hybrid WAN capability from the **Site** page. The Hybrid WAN sites can have a maximum of two WAN links. You cannot apply intent policies for Hybrid WAN sites.

To add an on-premise spoke site with Hybrid WAN capability:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke (Manual)**.

The Add Site for *Tenant-Name* page appears.

3. Complete the configuration settings in the General and WAN sections according to the guidelines provided in [Table 22 on page 77](#).

4. Review the configuration and modify the settings, if needed, from the **Summary** tab.

5. Click **OK**.

You are returned to the Sites page and a message indicating that the site creation job was triggered is displayed. You can click the job ID link to view the progress of the job. After the job is completed successfully, a confirmation message is displayed and the site that you added is displayed on the Sites page.

**Table 22: Fields on the Add Spoke Site Page**

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
WAN Capabilities	Select <b>Hybrid WAN</b> to include Hybrid WAN capability in the on-premise spoke site.
LAN Capabilities	This option is disabled for Hybrid WAN.
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Enter the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the locality of the site.

Table 22: Fields on the Add Spoke Site Page (continued)

Field	Description
Country	<p>Select the country where the site is located.</p> <p>Click the <b>Validate</b> button to verify the address.</p> <ul style="list-style-type: none"> <li>The <b>site address verification successful</b> message is displayed if the address is verified.</li> </ul> <p>You can click the <b>View location on a map</b> link to see the address location.</p> <ul style="list-style-type: none"> <li>If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of a contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
<b>Advanced Configuration</b>	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server.</p> <p>To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
<b>Device Profile</b>	
Device Series	Select the device series to which the CPE belongs—SRX, NFX150, or NFX250.

Table 22: Fields on the Add Spoke Site Page (continued)

Field	Description
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
<b>Device Information</b>	
Device Model	Select the device model for NFX150 device.
Serial Number	<p>Enter the serial number of the CPE device.</p> <p>The serial number is a 12-digit number present on the rear panel of the device. Serial numbers are case-sensitive.</p>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the CPE device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the CPE device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>
Activation Code	<p>Enter the activation code of the CPE device that your service provider supplied. If you do not want to specify an activation code, then disable the <code>ACTIVATION_CODE_ENABLED</code> field in the device template and save the changes.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i>.</p>
<b>CPE Info</b>	

Table 22: Fields on the Add Spoke Site Page (continued)

Field	Description
CPE AS Number	Specify the autonomous system(AS) number.
<b>Access Info</b>	
Router Name	Specify the router name.
Router AS Number	Specify the AS number for the router.
<b>Management Connectivity</b>	
OAM Traffic Information	Select this option if the management connectivity is initiated by Contrail Service Orchestration (CSO).
VLAN Id	Enter an OAM VLAN ID for in-band management of the site. If you specify an OAM VLAN ID, then an in-band OAM traffic reaches the site through the selected OAM interface. The range is 0 through 65535.
IP Prefix	<p>Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14.</p> <ul style="list-style-type: none"> <li>For NFX150 and NFX250 devices, if the USE_SINGLE_SSH_TO_NFX parameter is disabled in the device template, then enter the IP address prefix as /29 or lower based on the number of VNFs.</li> <li>For all other devices, enter the IP address prefix as /32.</li> </ul>
Gateway IP	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
<b>WAN links</b>	
<b>WAN_0</b>	
Link Type	Select whether the link would be an MPLS link or Internet link.

Table 22: Fields on the Add Spoke Site Page (*continued*)

Field	Description
VLAN ID	Specify the identifier for the Layer 2 VLAN for the CPE device.
Local IP Prefix	Enter the local IP address prefix of the WAN link.
Remote IP Prefix	Enter the remote IP address prefix of the WAN link.
<b>WAN_1</b>	Refer to the fields described for WAN_0 for an explanation of the fields.
VRF Name	Specify the name of the virtual routing and forwarding (VRF) instance.
Ipssec Concentrator Name	Specify the name of the IPsec concentrator device.
Internet Gateway IP	If you specified that the device is an IPsec concentrator, then specify the IPv4 address of the Internet gateway.

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)
[About the Site Groups Page | 144](#)

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

An on-premise spoke represents an endpoint that is part of customer premise equipment (CPE) at some physical location such as branch office or point of sale location. Typically, these points are connected using overlay connections to hub sites. You add an on-premise spoke site from the **Sites** page. The following device templates are supported for on-premise spoke sites:

- NFX150 as SD-WAN CPE
- NFX250 as SD-WAN CPE
- Dual NFX250 as SD-WAN CPEs
- SRX as SD-WAN CPE
- Dual SRX as SD-WAN CPEs

- SRX4x00 as SD-WAN CPE
- Dual SRX4x00 as SD-WAN CPEs

To add an on-premise spoke site with only SD-WAN capability:

1. Click **Add** and select **On-Premise Spoke Site**.

The **Add Site for *Tenant-Name*** page appears.

2. Complete the configuration settings according to the guidelines provided in [Table 23 on page 82](#).
3. (Optional) You can review the configuration in the **Summary** tab and modify the settings, if required.
4. Click **OK**.

You are returned to the Sites page and a message indicating that the site creation job was triggered is displayed. You can click the job ID link to view the progress of the job. After the job is completed successfully, a confirmation message is displayed and the site that you added is displayed on the Sites page.

**Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability**

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
WAN Capabilities	Select <b>SD-WAN</b> to include SD-WAN capability in the on-premise spoke site.
LAN Capabilities	You need not select this option as you are creating the on-premise site with only SD-WAN capability.
<b>Configuration</b>	
Primary Provider Hub	Select the primary hub site to which this spoke site must connect.



Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Secondary Provider Hub	<p>Select the secondary hub site to which this site must connect.</p> <p>This site connects to the secondary data hub site when the primary data hub is not reachable.</p>
Primary Enterprise Hub	<p>Select the enterprise hub with which you want to connect the spoke site. If you specify a enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.</p>
Secondary Enterprise Hub	<p>Select the secondary enterprise hub for this spoke site.</p> <p>The spoke site connects with secondary gateway hub when the primary gateway hub is not reachable.</p>
<b>On-Demand VPN Threshold</b>	
Threshold for Tunnel Creation	<p>Enter the maximum number of sessions closed between the connected sites in a duration of two minutes at which full mesh is created between the two sites.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes exceeds 5.</p>
Threshold for Tunnel Deletion	<p>Enter the number of sessions closed between the connected sites in a duration of 15 minutes below which full mesh is deleted between the two sites.</p> <p>The default value is 8.</p> <p>For example, if you specify the number of sessions closed as 8, dynamic VPN tunnels are deleted if the number of sessions closed is lesser than or equal to 8.</p>
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Country	<p>Select the country where the site is located.</p> <p>Click the <b>Validate</b> button to verify the address.</p> <ul style="list-style-type: none"> <li>• The <b>site address verification successful</b> message is displayed if the address is verified. You can click the <b>View location on a map</b> link to see the address location.</li> <li>• If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
<b>Advanced Configuration</b>	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
<b>WAN</b>	
<b>Device Profile</b>	
Device Series	Select the device series to which the CPE belongs—SRX, NFX150, or NFX250.
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
<b>Device Information</b>	
Device Model	Select the device model number for NFX150 device.

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Serial Number	<p>Enter the serial number of the CPE device.</p> <p>The serial number is a 12-digit number present on the rear panel of the device. Serial numbers are case-sensitive.</p>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the CPE device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the CPE device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>
Activation Code	<p>If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i>.</p>
Firewall Policies	<p>Select the firewall policy that you want to deploy to the standalone firewall site. The firewall policy list is populated from the <b>Configuration &gt; Firewall &gt; Firewall Policy</b> page.</p> <p>Default: Factory_Default_Fw_Policy</p>
NAT Policies	<p>Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the <b>Configuration &gt; NAT &gt; NAT Policies</b> page.</p> <p>Default: Factory_Default_NAT_Policy</p>
<b>Management Connectivity</b>	

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
IP Prefix	<p>Enter an IPv4 address prefix for the loopback interface on the CPE device.</p> <p>The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14.</p> <ul style="list-style-type: none"> <li>For NFX150 and NFX250 devices, if the USE_SINGLE_SSH_TO_NFX parameter is disabled in the device template, then enter the IP address prefix as /29 or lower based on the number of VNFs.</li> <li>For all other devices, enter the IP address prefix as /32.</li> </ul>
<b>WAN Links</b>	
Link Type	Select whether the link would be an MPLS link or Internet link.
Access Type (NFX150 and NFX250)	<p>If you select Internet as the link type, select the access type for the underlay link—Ethernet, LTE, ADSL, or VDSL.</p> <p>You can select the LTE, ADSL, or VDSL access type only for one WAN link.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>You cannot configure an access type (LTE, ADSL, and VDSL) if you are using the Dual SRX and Dual NFX device templates. By default, Ethernet is configured as the access type for the underlay link.</li> <li>Currently, CSO supports only LTE and VDSL access types on SRX 300 line devices.</li> </ul>
Egress Bandwidth	<p>Enter the maximum bandwidth, in Mbps, allowed on the WAN link.</p> <p>Range: 1 through 10,000.</p>
Address Assignment	<p>Select the method of assigning an IP address to the WAN link—DHCP or STATIC.</p> <p>If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.</p>
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.
Gateway IP	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
<b>Advanced Settings</b>	

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Provider	<p>Enter the name of the service provider (SP) providing the WAN service.</p> <p>Only alphanumeric characters and '_', '@', ':', '/', '#', '&amp;', '+' and '-' are allowed. The maximum number of characters allowed is 15.</p>
Cost/Month	<p>Enter the cost for using the WAN link per month and select the currency in which the cost is indicated from the adjacent drop-down list.</p> <p>Range: 1 through 10,000.</p> <p>In bandwidth-optimized SD-WAN, CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.</p>
Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent.</li> <li>• If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.</li> </ul>
Breakout Options	<p>Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.</p>

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Autocreate Source NAT Rule	<p>If the WAN link is enabled for local breakout, you can click the toggle button to automatically create an interface-based source NAT rule on the WAN link. The automatically-created source NAT rule is implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>By default, this field is disabled.</p> <p><b>NOTE:</b> If this option is enabled for a WAN interface W1 during the site addition workflow, a series of NAT source rules are automatically created. Each automatically created NAT rule is from a zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following zone to W1 interface rule-set might be created:</p> <pre>Zone1 --&gt; W1: Translation=Interface Zone2 --&gt; W1: Translation=Interface Zone3 --&gt; W1: Translation=Interface</pre> <p>To manually override any of these rules, you can create a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant zone and WAN interface as the source and destination. For example:</p> <pre>Zone1 --&gt; W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Zone1, Port 56578 --&gt; W1: Translation=Pool-2</pre>
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the most preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a fullmesh topology.</p> <p>A site can have a maximum of three links enabled for meshing.</p>

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (continued)

Field	Description
Mesh Overlay Link Type	<p>When <b>Use for Fullmesh</b> field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC.</p> <p>If the link type is Internet, by default, the value for mesh overlay link type is GRE_IPSEC.</p> <p>If the link type is MPLS, select one of the following options:</p> <ul style="list-style-type: none"> <li>• GRE-IPSEC</li> <li>• GRE</li> </ul>
Mesh Tag	<p>When the <b>Use for Fullmesh</b> field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <ul style="list-style-type: none"> <li>• For an on-premise spoke site, you can select one mesh tag.</li> <li>• For a enterprise hub you can select one or more mesh tags.</li> </ul> <p>For more information about mesh tags, see <a href="#">“Mesh Tags Overview” on page 167</a>.</p>
Connects to Hubs	<p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted.</li> <li>• For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.</li> </ul>
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>When the <b>Connects to Hubs</b> field is enabled, select the mesh overlay tunnel type—GRE and GRE_IPSEC.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	<p>When the <b>Connects to Hubs</b> field is enabled, view the peer hub device to which the site is connected.</p>
Overlay Peer Interface	<p>When the <b>Connects to Hubs</b> field is enabled, select the interface name of the hub device to which the WAN link of the site is connected.</p>

Table 23: Fields on the Add Site for Tenant-Name Page With only SD-WAN Capability (*continued*)

Field	Description
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, SLA data is not monitored for the backup link.</p>
Default Link	<p>Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site.</p> <p>Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.</p>
Data VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 2 through 4093.</p>
WAN_1	Refer to the fields described for WAN_0 for an explanation of the fields.
WAN_2	Refer to the fields described for WAN_0 for an explanation of the fields.
WAN_3	Refer to the fields described for WAN_0 for an explanation of the fields.
<b>LAN</b>	
Add LAN Segment	<p>You must add at least one LAN segment for the on-premise site. To add a LAN segment:</p> <ol style="list-style-type: none"> <li>1. Click the + icon. The Add LAN Segment page appears.</li> <li>2. Complete the configuration settings according to the guidelines provided in <a href="#">Table 24 on page 91</a>.</li> <li>3. Click <b>Save</b>. The LAN segment is added and you are returned to the Add Site for <i>Tenant-Name</i> page.</li> </ol>



Table 24: Fields on the Add LAN Segment page

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
Type	<p>Select the type of LAN segment:</p> <ul style="list-style-type: none"> <li>• Directly Connected (default)—Indicates that the LAN segment is directly connected to the site.</li> <li>• Dynamic Routed—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.</li> </ul>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>
Department	<p>Select a department to which the LAN segment is assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.</p>
Protocol	<p>For dynamically routed LAN segments, select the routing protocol (BGP or OSPF) to be used by the data center department to learn routes from the data center.</p>
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment.</p> <p>For example: 192.0.2.8/24.</p>
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP (default).</p> <p>You can enable DHCP if you want to assign IP addresses by using a DHCP sever or disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, additional fields appear on the page.</p>
Additional Fields	

Table 24: Fields on the Add LAN Segment page (*continued*)

Field	Description
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server.</p> <p>Default: 1440</p> <p>Range: 0 through 4,294,967,295 seconds.</p>
Name Server	<p>Specify one or more IPv4 addresses of the DNS server.</p> <p>To enter more than one DNS server address, type the address, press Enter, and then type the next address.</p> <p><b>NOTE:</b> DNS servers are used to resolve hostnames into IP addresses.</p>
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the Switch device and creates the same LAN segment on the Switch.</li> </ul> <p>If you click to exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field.</p> <p>CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is a physical SRX Series device.</p>
Switch Ports  <b>NOTE:</b> This field is displayed only when LAN capability is selected for the enterprise hub.	<p>If you disable the CPE ports field, select ports on the switch to be part of the LAN segment. The Switch ports and CPE ports are mutually exclusive.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>
<b>BGP Configuration</b>	

Table 24: Fields on the Add LAN Segment page (*continued*)

Field	Description
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• None—Indicates that no authentication should be used. This is the default.</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> </ul>
Peer IP Address	Enter the IP address of the BGP neighbor.
Peer AS Number	Enter the autonomous system (AS) number BGP neighbor.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
OSPF Configuration	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default).</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> <li>• None—Indicates that no authentication should be used.</li> </ul>
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.

## RELATED DOCUMENTATION

| [About the Sites Page](#) | 40

## Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities

You can add an on-premise spoke site in CSO by provisioning a CPE and a switch behind the CPE to provide SD-WAN and LAN capabilities to the site. See [“Switch Behind a CPE or Next Generation Firewall Overview” on page 45](#) for details.

To add a site with SD-WAN and LAN capabilities:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke (Manual)**.

The Add Site for *Tenant-Name* page appears.

3. Complete the configuration according to the guidelines provided in [Table 25 on page 95](#).

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

4. Review the configuration and modify the settings, if needed, from the **Summary** tab.
5. Click **OK** to add the site.

The site activation job is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the CPE and the switch. The CPE is activated first and then the process to activate the switch is initiated.

6. To activate the switch, you must manually configure the stage-1 configuration on the switch.
  - a. On the Site Activation page, after the Prestage Device step completes successfully for the switch, the **View Stage-1 Configuration** link appears next to the Prestage Device step.
  - b. Click the **View Stage-1 Configuration** link.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- c. Copy the stage-1 configuration and log in to the CLI of the EX Series switch.
  - d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.

**Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities)**

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
WAN Capabilities	Select <b>SD-WAN</b> to include SD-WAN capabilities in the spoke site.
LAN Capabilities	Select <b>LAN</b> to include SD-LAN capability in the spoke site.
<b>Configuration</b>	

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Primary Provider Hub	Select the hub site (or primary hub site in case of multihoming) to which the spoke site must connect.
Secondary Provider Hub	<p>Select the secondary hub site to which this site must connect.</p> <p>This site connects to the secondary data hub site when the primary data hub is down.</p>
Primary Enterprise Hub	Select the primary enterprise hub with which you want to connect the spoke site. If you specify a enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.
Secondary Enterprise Hub	<p>Select the secondary enterprise hub for this spoke site.</p> <p>The spoke site connects with secondary gateway hub when the primary gateway hub is down.</p>
<b>On-Demand VPN Threshold</b>	
Threshold for Tunnel Creation	<p>Specify the threshold for the number of sessions (flows) closed (in a two-minute duration) between the on-premise spoke site and a destination site. When the number of sessions closed exceeds the specified threshold, a tunnel is created between the on-premise spoke site and the destination site.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes exceeds 5.</p>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Threshold for Tunnel Deletion	<p>Specify the threshold for the number of sessions closed (in a 15-minute duration) between the on-premise spoke site and a destination site. When the number of sessions closed is lower than the specified threshold, the tunnel between the on-premise spoke site and destination site is deleted.</p> <p>The default value is 2.</p> <p>For example, if you specify the number of sessions closed as 2, dynamic VPN tunnels are deleted if the number of sessions closed is lesser than or equal to 2.</p>
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	<p>Select the country where the site is located.</p> <p>Click the <b>Validate</b> button to verify the address.</p> <ul style="list-style-type: none"> <li>The <b>site address verification successful</b> message is displayed if the address is verified.</li> </ul> <p>You can click the <b>View location on a map</b> link to see the address location.</p> <ul style="list-style-type: none"> <li>If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
<b>Advanced Configuration</b>	

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
<b>WAN</b>	
<b>Device Profile</b>	
Device Series	Select the device series to which the CPE belongs—SRX. NFX250.
Device Template	<p>Select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>
<b>Device Information</b>	
Serial Number	Enter the serial number of the CPE device.
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the CPE device.</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the CPE device is automatically triggered after the site is added to CSO.</p> <p>The device template that you select determines whether this option is enabled or disabled by default.</p>



Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Activation Code	<p>If you disable the Auto Activate field, enter the activation code for the CPE or firewall device.</p> <p>For information about activating a CPE or firewall device, see <a href="#">“Activating a CPE Device” on page 181</a>.</p>
Boot image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image is populated based on the device template that you have selected while creating a site. See <i>Uploading a Device Image</i>.</p>
<b>WAN Links</b>	
WAN_0	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_0 link is enabled.</p> <p>When you enable a WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed.</p>
Link Type	Select the underlay network type (MPLS or Internet) of the WAN link that is connected to the on-premise spoke site.
Access Type (NFX150, NFX250, SRX320, SRX340, and SRX345)	<p>If you select Internet as the link type, select the access type for the underlay link—Ethernet, LTE, ADSL, or VDSL.</p> <p>You can select the LTE, ADSL, or VDSL access type only for one WAN link.</p> <p><b>NOTE:</b> You cannot configure an access type (LTE, ADSL, and VDSL) if you are using the Dual SRX and Dual NFX device templates. By default, Ethernet is configured as the access type for the underlay link.</p>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Egress Bandwidth	<p>Enter the maximum bandwidth (in Mbps) that the CPE or firewall allows over the WAN link.</p> <p>Range: 1 through 10,000.</p>
Address Assignment	<p>Select the method of assigning an IP address to the WAN link—DHCP or STATIC.</p> <ul style="list-style-type: none"> <li>• If you select DHCP, the IP address is provided by using the DHCP server of the service provider of the WAN link.</li> <li>• If you select STATIC, you must provide the IP address prefix and the gateway address for the WAN link.</li> </ul>
Static IP Prefix	If you configured the address assignment method as STATIC, enter the IP address prefix of the WAN link.
Gateway IP Address	If you configured the address assignment method as STATIC, enter the IP address of the gateway of the WAN service provider.
<b>Advanced Settings</b>	
Provider	Enter the name of the service provider who is responsible for providing the WAN link.
Cost/Month	<p>Enter the cost per month (in a specified currency) for the WAN link. Specify the currency from the adjacent drop-down list.</p> <p>Range: 1 through 10,000.</p> <p>In bandwidth-optimized SD-WAN, CSO uses this information to identify the least-expensive link to route traffic when multiple WAN links meet SLA profile parameters.</p>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
Enable Local Breakout	<p>Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• If you enable this option, the WAN link can be used for local breakout. The decision of whether traffic breaks out locally from the site depends on the breakout profile that is referenced in the SD-WAN policy intent.</li> <li>• If you do not enable local breakout on at least one WAN link for a single CPE connection plan and at least two WAN links for a dual CPE connection plan, then local breakout is disabled for the site.</li> </ul>
Breakout Options	<p>Select whether you want to use the WAN link for both breakout and WAN traffic (default) or only for breakout traffic.</p>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
Autocreate Source NAT Rule	<p>If the WAN link is enabled for local breakout, you can click the toggle button to automatically create an interface-based source NAT rule on the WAN link. The automatically-created source NAT rule is implicitly defined and applied to the site and is not visible on the NAT Policies page.</p> <p>By default, this field is disabled.</p> <p><b>NOTE:</b> If this option is enabled for a WAN interface W1 during the site addition workflow, a series of NAT source rules are automatically created. Each automatically created NAT rule is from a zone to the WAN interface, with a translation of type interface. Each pair of [zone - interface] represents a rule-set.</p> <p>For example, the following zone to W1 interface rule-set might be created:</p> <pre>Zone1 --&gt; W1: Translation=Interface Zone2 --&gt; W1: Translation=Interface Zone3 --&gt; W1: Translation=Interface</pre> <p>To manually override any of these rules, you can create a NAT rule within a particular rule-set. For example, to use a source NAT pool instead of an interface for translation, create a NAT rule within this particular rule-set, that includes the relevant zone and WAN interface as the source and destination. For example:</p> <pre>Zone1 --&gt; W1 : Translation=Pool-2</pre> <p>The manually created NAT rule is placed at a higher priority than the corresponding automatically created NAT rule.</p> <p>You can also add other fields (such as addresses, ports, protocols, and so on) as part of the source or destination endpoints. For example:</p> <pre>Zone1, Port 56578 --&gt; W1: Translation=Pool-2</pre>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (continued)

Field	Description
Preferred Breakout Link	<p>Click the toggle button to enable the WAN link as the preferred breakout link.</p> <p>If you disable this option, then the breakout link is chosen using ECMP from the available breakout links.</p>
Use For Fullmesh	<p>Click the toggle button to specify whether the WAN link can be a part of a full mesh topology.</p> <p>A site can have a maximum of three links enabled for meshing.</p>
Mesh Overlay Link Type	<p>When <b>Use for Fullmesh</b> field is enabled, select the type of mesh overlay link—GRE and GRE_IPSEC:</p> <ul style="list-style-type: none"> <li>• If the link type is Internet, the value for mesh overlay link type is GRE_IPSEC.</li> <li>• If the link type is MPLS, select one of the following options: <ul style="list-style-type: none"> <li>• GRE-IPSEC</li> <li>• GRE</li> </ul> </li> </ul>
Mesh Tag	<p>When the <b>Use for Fullmesh</b> field is enabled, enter the tag to be associated with the WAN link for creating tunnels. You can assign only one tag to the link.</p> <p>Matching mesh tags is one of the criteria used to form tunnels between sites that support meshing.</p> <p>For more information about mesh tags, see <a href="#">“Mesh Tags Overview” on page 167</a>.</p>
Connects to Hubs	<p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted.</li> <li>• For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.</li> </ul>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
Use for OAM Traffic	<p>If you have specified that the WAN link is connected to a hub, click the toggle button to enable sending the OAM traffic over the WAN link.</p> <p>This WAN link is then used to establish the OAM tunnel.</p>
Overlay Tunnel Type	<p>Select the mesh overlay tunnel type—GRE and GRE_IPSEC.</p> <p>MPLS links can have both GRE and GRE_IPSEC as the overlay link type where as Internet links can have only GRE_IPSEC as the overlay link type.</p>
Overlay Peer Device	Displays the peer hub device to which the site is connected.
Overlay Peer Interface	Select the interface name of the hub device to which the WAN link of the site is connected.
Backup Link	<p>Select a backup link through which traffic can be routed when the primary (other) links are unavailable. You can select any link other than the default links or links that are configured exclusively for local breakout traffic.</p> <p>When a primary link comes back online, CSO monitors the performance on the primary link and when the primary link meets the SLA requirements, the traffic is switched back to the primary link. However, SLA data is not monitored for the backup link.</p>
Default Link	<p>Select one or more links that will be used for routing traffic in the absence of matching SD-WAN policy intents. A site can have multiple default links to the hub site.</p> <p>Default links are used primarily for overlay traffic but can also be used for local breakout traffic. However, a default link cannot be used exclusively for local breakout traffic. If you do not specify a default link, then equal-cost multipath (ECMP) is used to choose the link on which to route traffic.</p>
Data VLAN ID	<p>Enter a VLAN ID for the WAN link.</p> <p>Range: 2 through 4093.</p>

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
WAN_1	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_1 link is disabled.</p> <p>Refer to the fields described for WAN_0 for an explanation of the fields.</p>
WAN_2	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_2 link is disabled.</p> <p>Refer to the fields described for WAN_0 for an explanation of the fields.</p>
WAN_3	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_3 link is disabled.</p> <p>Refer to the fields described for WAN_0 for an explanation of the fields.</p>
<b>Management Connectivity</b>	
IP Prefix	Enter an IPv4 address prefix for the loopback interface on the CPE device. The IP address prefix must be a /32 IP address prefix and must be unique across the entire management network. If you do not specify an IPv4 address prefix, CSO automatically assigns the IP prefix from the reserved pool 100.124.0.0/14.
<b>LAN</b>	
<b>Device Profile</b>	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, and EX4300.

Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
Device Model	<p>Select the model for the switch you specified in the Device Type.</p> <p>The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.</p>
<b>CPE Settings</b>	
Trunk Ports	<p>Select at least two trunk ports on the CPE device to connect with the switch, which are used for the following:</p> <ul style="list-style-type: none"> <li>• LAN traffic between the switch and the CPE</li> <li>• Management traffic for in-band management of the switch.</li> </ul> <p><b>NOTE:</b> The ae0 LAG interface of the SRX Series devices is used as the trunk port for communication with the switch.</p>
Switch Management Subnet	<p>Specify the subnet that the DHCP server can use to assign IP addresses. The DHCP server runs on the following ports:</p> <ul style="list-style-type: none"> <li>• Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE.</li> <li>• Out-of-band management port on the CPE to provide DHCP information to the management port on the switch.</li> <li>• LAN ports on the CPE to provide information to the devices connected to the CPE LAN ports.</li> </ul>
<b>Switch Details</b>	
Serial Number	Specify the serial number of the switch.



Table 25: Fields on the Add Site for Tenant-Name Page(SD-WAN and LAN Capabilities) (*continued*)

Field	Description
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the switch is automatically triggered when the device communicates with CSO.</p> <p>By default, auto activation for the switch is enabled, if it is enabled for the CPE and vice-versa.</p> <p><b>NOTE:</b> You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when you enable this option.</p>
Activation code	<p>When the <b>Auto activate</b> field is disabled, enter the activation code to be used for manually activating the switch.</p> <p>For information, see <a href="#">“Manually Activating a Switch” on page 184</a>.</p>
Zero Touch Provisioning	<p>ZTP must be disabled for all EX Series switches for the CSO 5.0.0 release.</p> <p>The Stage-1 configuration must be copied and pasted onto the CLI of the switch during site activation. See <a href="#">“Step-by-Step Procedure” on page 94</a> for details.</p>
LAN Segment	<p>Displays the LAN segment that you configure on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See <a href="#">Table 26 on page 107</a>.</p>

Table 26: Fields on the Add LAN Segment Page when Adding a Switch along with CPE

Field	Description
Add LAN Segment	

Table 26: Fields on the Add LAN Segment Page when Adding a Switch along with CPE (*continued*)

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.</p>
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default.</p> <p>You enable DHCP if you want to assign IP addresses by using a DHCP sever. You disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.</p>
<b>[DHCP-Related Fields]</b>	
Address Range Low	<p>Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.</p>
Address Range High	<p>Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.</p>
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server.</p> <p>Range: 0 through 4,294,967,295.</p>

Table 26: Fields on the Add LAN Segment Page when Adding a Switch along with CPE (*continued*)

Field	Description
Name Server	Specify or select one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the switch device and creates the same LAN segment on the switch.</li> </ul> <p>If you exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field. CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is an SRX Series device.</p>
Switch Ports	<p>If you disable the CPE ports field, select ports on the switch that will be part of the LAN segment.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>

## RELATED DOCUMENTATION

[Adding and Provisioning Switches to Provide LAN Capability to a Site Overview | 44](#)
[Adding an On-Premise Spoke Site with LAN Capability | 110](#)
[Adding a Switch to an Existing Site | 123](#)
[Deleting a Site | 142](#)

## Adding an On-Premise Spoke Site with LAN Capability

You can add an on-premise spoke site in CSO by provisioning a switch to provide LAN capability to the site. See [“Standalone Switch Overview” on page 44](#) for details.

You can provision and monitor a switch by adding a site with LAN capability to Contrail Service Orchestration (CSO).

To provision a site with LAN capability:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke (Manual)**.

The Add Site for *Tenant-Name* page appears.

3. Complete the configuration according to the guidelines provided in [Table 27 on page 111](#).

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

4. (Optional) Review the configuration and modify the settings, if needed, from the **Summary** tab.
5. Click **OK** to add the site.

The site activation job is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the switch.

6. To activate the switch, you must manually configure the stage-1 configuration on the switch.
  - a. On the Site Activation page, after the Prestage Device step completes successfully for the switch, the **View Stage-1 Configuration** link appears next to the Prestage Device step.

- b. Click the **View Stage-1 Configuration** link.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- c. Copy the stage-1 configuration and log in to the CLI of the EX Series switch.

- d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.

**Table 27: Fields on the Add Site for Tenant-Name Page ( LAN Capability)**

Field	Description
<b>Site Information</b>	
Site Name	Enter a unique name for the site. You can use alphanumeric characters and hyphen (-). The maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
LAN Capabilities	Select <b>LAN</b> to include LAN capabilities in the site.
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.

Table 27: Fields on the Add Site for Tenant-Name Page ( LAN Capability) (continued)

Field	Description
Country	<p>Select the country where the site is located. Click the <b>Validate</b> button to verify the address.</p> <ul style="list-style-type: none"> <li>• The <b>site address verification successful</b> message is displayed if the address is verified. You can click the <b>View location on a map</b> link to see the address location.</li> <li>• If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed.</li> </ul> <p>If you enter the wrong address and click the <b>Validate</b> button to verify the address, the <b>Site address could not be validated message</b> is displayed.</p>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	Enter the phone number of the contact person for the site.
<b>Advanced Configuration</b>	
Name Server IP List	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on.</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>
Select Timezone	Select the time zone of the site.
<b>Device Profile</b>	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, and EX4300.

Table 27: Fields on the Add Site for Tenant-Name Page ( LAN Capability) (continued)

Field	Description
Device Model	<p>Select the model for the switch you specified in the Device Type field.</p> <p>The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.</p>
<b>Switch Details</b>	
Serial Number	<p>Specify the serial number of the switch.</p> <p>The serial number is a alphanumeric string 12 characters long. It is case-sensitive.</p>
Auto activate	<p>Click the toggle button to enable or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning (ZTP) of the switch is automatically triggered when the device communicates with CSO.</p> <p><b>NOTE:</b> The switch must be powered on for automatic activation when you enable this option.</p>
Activation code	<p>When the <b>Auto activate</b> field is disabled, enter the activation code to be used for manually activating the switch.</p> <p>For information about manually activating a switch, see <a href="#">“Manually Activating a Switch” on page 184</a>.</p>
Zero Touch Provisioning	<p>ZTP must be disabled for all EX Series switches for the CSO 5.0.0 release.</p> <p>The Stage-1 configuration must be copied and pasted onto the CLI of the switch during site activation. See <a href="#">“Step-by-Step Procedure” on page 110</a> for details.</p>
LAN Segment	<p>Displays the LAN segment that you configure on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. See <a href="#">Table 28 on page 113</a>.</p> <p>Adding a LAN segment while creating the site is optional.</p>

Table 28: Fields on the Add LAN Segment Page when Adding a Site With LAN Capability

Field	Description
<b>Add LAN Segment</b>	

Table 28: Fields on the Add LAN Segment Page when Adding a Site With LAN Capability (*continued*)

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
VLAN ID	<p>Enter the VLAN ID associated with the LAN segment.</p> <p>Range: 2 through 4093.</p>
Switch Ports	<p>Select up to two ports on the switch to form the LAN segment.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>

## RELATED DOCUMENTATION

[Adding and Provisioning Switches to Provide LAN Capability to a Site Overview | 44](#)
[Adding and Provisioning Switches to Provide LAN Capability to a Site Overview | 44](#)
[Adding an On-Premise Spoke Site with LAN Capability | 110](#)
[Adding a Switch to an Existing Site | 123](#)
[Deleting a Site | 142](#)

## Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities

You can add an on-premise spoke site with both firewall and LAN capabilities.

To add a site with both next generation firewall and LAN capabilities at the same time:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke (Manual)**.

The Add On-Premise Spoke Site for *Tenant-Name* page appears.



3. Complete the configuration settings according to the guidelines provided in [Table 29 on page 116](#).

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

4. Click **Next**.

A summary page is displayed.

5. Review the configuration and modify the settings, if needed, from the Summary tab.

6. Click **OK** to add the site.

The site activation job is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the firewall device and the switch (when LAN capability is selected). The firewall device is activated first and then the process to activate the switch is initiated.

7. To activate the switch, you must manually configure the stage-1 configuration on the switch.

- a. On the Site Activation page, after the Prestage Device step completes successfully for the switch, the **View Stage-1 Configuration** link appears next to the Prestage Device step.

- b. Click the **View Stage-1 Configuration** link.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- c. Copy the stage-1 configuration and log in to the CLI of the EX Series switch.

- d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.

**NOTE:** You can also add a site with LAN and next generation firewall capabilities using the site templates. For more information, see [“Adding On-Premise Spoke Sites by Using a Site Template” on page 147](#).

Table 29: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN)

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a unique name for the firewall site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
WAN Capabilities	Select the WAN capabilities as <b>Next Gen Firewall</b> for the site.
LAN Capabilities	Select the LAN capability as <b>LAN</b> for the site.
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.
Country	<p>Select the country where the site is located.</p> <p>You can click the <b>Validate</b> button to verify the address that you specified:</p> <ul style="list-style-type: none"> <li>• The <b>site address verification successful</b> message is displayed if the address can be verified. You can click the <b>View location on a map</b> link to see the address location.</li> <li>• If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	<p>Enter the phone number of the contact person for the site.</p> <p>Click <b>Next</b> to continue.</p>

Table 29: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) (continued)

Field	Description
<b>Advanced Configuration</b>	
Name Server IP List	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone for the site.
<b>WAN</b>	
<b>Device Information</b>	
Serial Number	Enter the serial number of the firewall device. Note that the serial numbers are case-sensitive.
Auto Activate	Click the toggle button to enable or disable automatic activation of the device. This option is enabled by default.
Activation Code	If the <b>Auto Activate</b> feature is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If ZTP is disabled, you must manually copy (by using CLI), the Stage-1 configuration on to the firewall device.</p>

Table 29: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) (continued)

Field	Description
Boot Image	<p>When the Zero Touch Provisioning field is enabled, select the boot image from the drop-down list to upgrade the image on the firewall device to a version that supports Phone-Home client.</p> <p>The boot image is the device image that was previously uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site.</p> <p>By default, the <b>Use Image on Device</b> option is selected.</p>
In-band Management Port	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces. This field is applicable only when a switch is behind a CPE (SD-WAN or a next generation firewall device).
Firewall Policies	<p>Select the firewall policy that you want to deploy to the standalone firewall site. The firewall policy list is populated from the <b>Configuration &gt; Firewall &gt; Firewall Policy</b> page.</p> <p>Default: Factory_Default_Fw_Policy</p>
NAT Policies	<p>Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the <b>Configuration &gt; NAT &gt; NAT Policies</b> page.</p> <p>Default: Factory_Default_NAT_Policy</p>
<b>LAN</b>	
<b>Device Profile</b>	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, and EX4300 .
Device Model	<p>Select the device model for the switch that you specified in the Device Type field.</p> <p>The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.</p>
<b>CPE Settings</b>	

Table 29: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) (continued)

Field	Description
Trunk Ports	<p>Select at least two trunk ports on the CPE device to connect with the switch. The trunk ports are used for the following:</p> <ul style="list-style-type: none"> <li>• LAN traffic between the switch and the CPE</li> <li>• Management traffic for in-band management of the switch.</li> </ul>
Switch Management Subnet	<p>Specify the subnet that the DHCP can use to assign IP addresses. The DHCP server runs on the following ports:</p> <ul style="list-style-type: none"> <li>• Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE.</li> <li>• Out-of-band management port on the CPE to provide DHCP information to the management port on the switch.</li> <li>• LAN ports on the CPE to provide information to the devices connected to the CPE LAN ports.</li> </ul> <p>Example: 192.0.2.0/24</p>
<b>Switch Details</b>	
Serial Number	<p>Specify the serial number of the switch</p> <p>The serial number is a 12-digit number present on the rear panel of the switch.</p>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the switch. When you enable this field, zero-touch provisioning of the switch is automatically triggered when the device communicates with CSO.</p> <p><b>NOTE:</b> You must physically connect the switch to the CPE device (firewall) and power it on for the switch to be automatically activated when you enable this option.</p>
Activation code	<p>When the <b>Auto activate</b> field is disabled, enter the activation code to be used for manually activating the switch.</p> <p>For information, see <a href="#">“Manually Activating a Switch” on page 184</a>.</p>
Zero Touch Provisioning	<p>ZTP must be disabled for all EX Series switches for the CSO 5.0.0 release.</p> <p>The Stage-1 configuration must be copied and pasted onto the CLI of the switch during site activation. See <a href="#">“Step-by-Step Procedure” on page 114</a> for details.</p>

Table 29: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Firewall and LAN) (continued)

Field	Description
LAN Segment	<p>Displays the LAN segment configured on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. Specify values for the LAN segment based on guidelines provided in <a href="#">Table 30 on page 120</a>.</p> <p>Fields marked * are mandatory.</p> <p><b>NOTE:</b> The same LAN segment is created on the CPE device (firewall) if the switch is connected to the CPE device (firewall) that is managed by CSO.</p>

Table 30: Fields on the Add LAN Segment Page when Adding a Switch along with CPE

Field	Description
<b>Add LAN Segment</b>	
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093</p>
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default.</p> <p>You enable DHCP if you want to assign IP addresses by using a DHCP server. You disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.</p>
<b>[DHCP-Related Fields]</b>	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.

Table 30: Fields on the Add LAN Segment Page when Adding a Switch along with CPE (*continued*)

Field	Description
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server.  Range: 0 through 4,294,967,295.
Name Server	Specify or select one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
Switch Ports	Select ports on the switch to be part of the LAN segment.  Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.  If you create a LAN segment on a switch when the switch is connected to the CPE device (firewall), CSO automatically assigns LAN ports on the CPE device (firewall) and creates the same LAN segment on the CPE device (firewall).

## RELATED DOCUMENTATION

[Adding and Provisioning a Next Generation Firewall Overview](#) | 121

## Adding and Provisioning a Next Generation Firewall Overview

### Overview

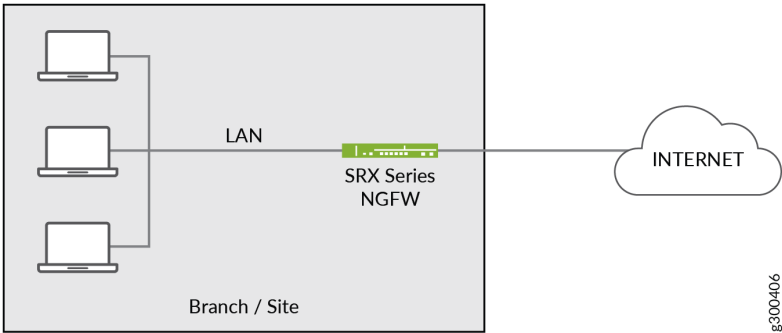
You can use Contrail Service Orchestration (CSO) to

- Add a firewall site for the next generation firewall device.
- Configure a CPE device (SRX Series services gateway) as a next generation firewall device.
- Add firewall policies for the standalone firewall site.
- Deploy the firewall policies for the standalone firewall site.

Topology

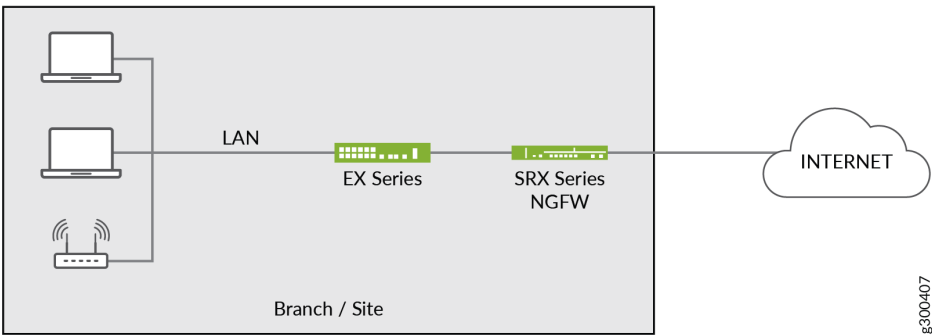
The topology to add an on-premise spoke site with next generation firewall capabilities is shown in [Figure 5 on page 122](#).

Figure 5: On-premise spoke site with next generation firewall



The topology to add an on-premise spoke site with next generation firewall and LAN capabilities is shown in [Figure 6 on page 122](#).

Figure 6: On-premise spoke site with next generation firewall and LAN



Workflow

The following workflow describes the steps that are required to set up a firewall site and provision the firewall device associated with the site.



To set up a next generation firewall site and provision the firewall device:

1. Add a standalone next generation firewall site. See [“Adding a Standalone Firewall Site” on page 128.](#)

To add a site with next generation firewall and switch, see [“Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities” on page 114.](#)

**NOTE:** Before proceeding to the next step ensure that the ZTP process is complete and the firewall device status is set to **Provisioned** state.

2. Configure the firewall device. See [“Configuring the Firewall Device” on page 240.](#)
3. Add firewall policies for the site. See [“Adding a Firewall Policy” on page 288.](#)
4. Add firewall policy intents for the firewall policies that you added. See [“Adding Firewall Policy Intents” on page 291.](#)
5. Deploy firewall policies to the site. See [“Deploying Firewall Policies” on page 351.](#)

## Adding a Switch to an Existing Site

You can add a switch to an existing on-premise spoke site or an enterprise hub site to provide LAN capability to the site. See [“Switch Behind a CPE or Next Generation Firewall Overview” on page 45](#) for details.

You can use the Customer Portal in CSO to add a switch to a spoke site that already has a CPE or firewall device provisioned.

To add a switch to an existing site:

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

The Sites page appears.

2. Select the site to which you want to add the switch.

3. Click **Add > Add Switch**.

The Add Switch page appears.

4. Complete the configuration according to the guidelines provided in [Table 31 on page 124.](#)

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

5. Click **OK** to add the switch to the site.

The site activation process is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the CPE and the switch.

6. To activate the switch, you must manually configure the stage-1 configuration on the switch.
  - a. On the Site Activation page, after the Prestage Device step completes successfully for the switch, the **View Stage-1 Configuration** link appears next to the Prestage Device step.
  - b. Click the **View Stage-1 Configuration** link.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- c. Copy the stage-1 configuration and log in to the CLI of the EX Series switch.
  - d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the switch has the outbound SSH configuration to connect with CSO. CSO then executes the bootstrap and provisioning processes on the switch and completes provisioning the switch.

**Table 31: Fields on the Add Switch Page**

Field	Description
<b>Device Profile</b>	
Device Name	Enter a name for the switch. You can use alphanumeric characters and hyphen (-). The maximum length allowed is 15 characters.
Device Type	Select the type of switch—EX2300, EX3400, and EX4300.
Device Model	Select the model for the switch you specified in the Device Type field.  The models vary in the number and type of ports the switch contains. For example, If you selected EX3400, select a model such as EX3400-24P, EX3400-48P, EX3400-24T among others.
<b>CPE Settings</b>	

Table 31: Fields on the Add Switch Page (*continued*)

Field	Description
Trunk Ports	<p>Select at least two trunk ports on the CPE device to connect with the switch, which are used for the following:</p> <ul style="list-style-type: none"> <li>• LAN traffic between the switch and the CPE or firewall.</li> <li>• Management traffic for in-band management of the switch.</li> </ul> <p><b>NOTE:</b> The ae0 port of the SRX Series devices is used as the trunk port for communication with the switch.</p>
Switch Management Subnet	<p>Specify the subnet that the DHCP can use to assign IP addresses. The DHCP server runs on the following ports:</p> <ul style="list-style-type: none"> <li>• Trunk ports to provide DHCP information to all devices connected to the switch and to the in-band management port, switch management port, and LAN ports on the CPE or firewall.</li> <li>• Out-of-band management port on the CPE or firewall to provide DHCP information to the management port on the switch.</li> <li>• LAN ports on the CPE or firewall to provide information to the devices connected to the CPE or firewall LAN ports.</li> </ul>
<b>Switch Details</b>	
Serial Number	Specify the serial number of the switch.
Auto activate	<p>Click the toggle button to enable or disable automatic activation of the switch. When you enable this field, zero-touch provisioning of the switch is automatically triggered when the device communicates with CSO.</p> <p><b>NOTE:</b> You must physically connect the switch to the CPE and power it on for the switch to be automatically activated when you enable this option.</p>
Activation code	<p>When the <b>Auto activate</b> field is disabled, enter the activation code to be used for manually activating the switch.</p> <p>For information, see <a href="#">“Manually Activating a Switch” on page 184</a>.</p>
Zero Touch Provisioning	<p>ZTP must be disabled for all EX Series switches for the CSO 5.0.0 release.</p> <p>The Stage-1 configuration must be copied and pasted onto the CLI of the switch during site activation. See <a href="#">“Step-by-Step Procedure” on page 123</a> for details.</p>

Table 31: Fields on the Add Switch Page (*continued*)

Field	Description
LAN Segment	<p>Displays the LAN segment configured on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the LAN table. The Add LAN Segment page appears. Specify values for the LAN segment based on guidelines provided in <a href="#">Table 32 on page 126</a>. Fields marked * are mandatory.</p> <p><b>NOTE:</b> The same LAN segment is created on the CPE if the switch is connected to the CPE managed by CSO.</p>

Table 32: Fields on the Add LAN Segment Page when Adding a Switch to an Existing Site

Field	Description
<b>Add LAN Segment</b>	
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to add a new department and assign the LAN segment to it. See <a href="#">"Adding a Department" on page 602</a> for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level. .</p> <p><b>NOTE:</b> This field is not displayed when you add the switch to a site with next-generation firewall capability.</p>
Gateway Address/Mask	Specify a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.

Table 32: Fields on the Add LAN Segment Page when Adding a Switch to an Existing Site *(continued)*

Field	Description
DHCP	<p>For directly connected LAN segments, click the toggle button to enable or disable DHCP on the LAN segment. DHCP is disabled by default.</p> <p>You enable DHCP if you want to assign IP addresses by using a DHCP sever. You disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.</p>
<b>[DHCP-Related Fields]</b>	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server.</p> <p>Range: 0 through 4,294,967,295 seconds.</p>
Name Server	Specify or select one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
Switch Ports	<p>Select ports on the switch to be part of the LAN segment.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p> <p>If you create a LAN segment on a switch when the switch is connected to the CPE device, CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p>

## RELATED DOCUMENTATION

[Adding and Provisioning Switches to Provide LAN Capability to a Site Overview | 44](#)

[Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities | 94](#)

[Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities | 114](#)

## Enabling Integration with Mist Access Points

You can enable integration with the Mist access points to easily access and view Mist access points connected to the branch network. When integration with Mist access point is enabled, the connected access points are listed in the **Devices** tab of the **Resources > Site Management > Site Name** page. You can click the access point name to view the Mist access point details from the Mist portal that is integrated with CSO.

To enable integration with the Mist access point:

1. Select **Administration > WiFi Settings**.

The WiFi Settings page appears.

2. Click the Enable toggle button to enable integration with Mist access points.

The Login E-mail and Login Password fields appear.

3. In the Login E-mail page, enter the e-mail address that is the username for your Mist account.

4. In the Login Password page, enter the password for your Mist account.

5. Click **Save**.

After you enable integration and enter the login credentials, CSO adds the access point to the list of devices associated with a site. To view details about the access point, **Devices** tab of the **Resources > Site Management > Site Name** page and click the access point name. The Mist portal page for the selected device appears.

## Adding a Standalone Firewall Site

You add the standalone firewall site from the **Sites** page.

To add a standalone firewall site:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke (Manual)**.

The Add On-Premise Spoke Site for *Tenant-Name* page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 33 on page 130](#).

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

4. Click **Next**.

A summary page is displayed.

5. Review the configuration and modify the settings, if needed, from the Summary tab.

6. Click **OK** to add the site.

The site activation job is initiated and the Site Activation: *Site-Name* page appears displaying the progress of the steps executed for activating the firewall site.

You can click the view job details link in the pop-up to view the progress of the job.

7. • If you have disabled the Zero Touch Provisioning (ZTP) field for the firewall device, you must manually configure the stage-1 configuration on the firewall device.

To manually configure the stage-1 configuration:

- a. On the Site Activation: *Site-Name* page, after the Prestage Device step completes successfully, the click to copy stage-1 config link appears .

- b. Click the **click to copy stage-1 config** link.

The Stage-1 Configuration page appears displaying the stage-1 configuration.

- c. Copy the stage-1 configuration and log in to the CLI of the firewall device.

- d. Enter the configuration mode, paste, and commit the configuration.

After the stage-1 configuration is committed, the firewall device establishes the outbound SSH connection to connect with CSO. After the firewall device is detected, CSO executes the bootstrap

and provisioning processes and completes provisioning the firewall device. The standalone firewall site status is set to **Provisioned** in the Sites page.

- If you have enabled the Zero Touch Provisioning field, CSO pushes the stage-1 and stage-2 configuration and provisions the firewall device. The standalone firewall site status is set to **Provisioned** in the Sites page.

**NOTE:** The firewall device is activated automatically, as you have already provided the activation code while creating the firewall site.

**NOTE:** You can also add a standalone firewall site using the site templates. For more information, see [“Adding On-Premise Spoke Sites by Using a Site Template” on page 147](#).

**Table 33: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Standalone Firewall)**

Field	Description
<b>General</b>	
<b>Site Information</b>	
Site Name	Enter a unique name for the firewall site. You can use alphanumeric characters and hyphen (-); the maximum length is 10 characters.
Site Group	Select a site group to which you want to assign the site.
<b>Site Capabilities</b>	
WAN Capabilities	Select the WAN capability as <b>Next Gen Firewall</b> as you are adding a next generation firewall site.
<b>Address and Contact Information</b>	
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.
State/Province	Select the state or province where the site is located.
ZIP/Postal Code	Enter the postal code for the site.



Table 33: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Standalone Firewall) (continued)

Field	Description
Country	<p>Select the country where the site is located.</p> <p>You can click the <b>Validate</b> button to verify the address that you specified:</p> <ul style="list-style-type: none"> <li>• The <b>site address verification successful</b> message is displayed if the address can be verified. You can click the <b>View location on a map</b> link to see the address location.</li> <li>• If the address cannot be verified, the <b>Site address could not be validated</b> message is displayed .</li> </ul>
Contact Name	Enter the name of the contact person for the site.
Email	Enter the e-mail address of the contact person for the site.
Phone	<p>Enter the phone number of the contact person for the site.</p> <p>Click <b>Next</b> to continue.</p>
<b>Advanced Configuration</b>	
Name Server IP List	Enter one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.
NTP Server	Enter the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers. Example: ntp.example.net The site must have DNS reachability to resolve the FQDN during site configuration.
Select Timezone	Select the time zone for the site.
<b>WAN</b>	
<b>Device Information</b>	
Serial Number	Enter the serial number of the firewall device. Note that the serial numbers are case-sensitive.
Auto Activate	Click the toggle button to enable or disable automatic activation of the device. This option is enabled by default.
Activation Code	If the automatic activation of the device is disabled, enter the activation code to manually activate the device. The activation code is provided by the administrator who adds the site.

Table 33: Fields on the Add On-Premise Spoke Site for Tenant-Name Page (Standalone Firewall) (continued)

Field	Description
Zero Touch Provisioning	<p>Click the toggle button to enable or disable Zero Touch Provisioning (ZTP). This option is enabled by default.</p> <p>If ZTP is enabled, the Boot Image field is displayed and you must select an image that supports the Phone-Home client. During ZTP, the image on the firewall device is upgraded to the image that you select for the Boot Image.</p> <p>If ZTP is disabled, you must manually copy (by using CLI), the Stage-1 configuration on to the firewall device.</p>
Boot Image	<p>When the Zero Touch Provisioning field is enabled, select the boot image from the drop-down list to upgrade the image on the firewall device to a version that supports Phone-Home client.</p> <p>The boot image is the device image that was previously uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process. If the boot image is not provided, then the device skips the automatic upgrade procedure. The boot image is populated based on the device template that you have selected while creating a site.</p> <p>By default, the <b>Use Image on Device</b> option is selected.</p>
In-band Management Port	<p>Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces. This field is applicable only when a switch is behind a CPE (SD-WAN or next generation firewall device).</p>
Firewall Policies	<p>Select the firewall policy that you want to deploy to the standalone firewall site. The firewall policy list is populated from the <b>Configuration &gt; Firewall &gt; Firewall Policy</b> page.</p> <p>Default: Factory_Default_Fw_Policy</p>
NAT Policies	<p>Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the <b>Configuration &gt; NAT &gt; NAT Policies</b> page.</p> <p>Default: Factory_Default_NAT_Policy</p>

## RELATED DOCUMENTATION

Adding and Provisioning a Next Generation Firewall Overview | 121

## Managing LAN Segments on a Tenant Site

### IN THIS SECTION

- [Adding LAN Segments | 133](#)
- [Deploying LAN Segments | 137](#)
- [Reassigning a Department to a LAN Segment | 138](#)
- [Deleting LAN Segments | 138](#)

A network on a tenant site is divided into multiple LAN segments to improve traffic management and security. A LAN segment is a small portion of a LAN that is used by a work group. A grouping of multiple LAN segments form a department. LAN segments are separated by a bridge, router, or a switch.

You can view and manage LAN segments from the LAN tab of the *Site Name* page. .

These topics describe how to manage LAN segments on a site.

### Adding LAN Segments

You add LAN segments from the *Site Name* page.

To add a LAN segment:

1. Click **Resources > Site Management**.

The Sites page appears.

2. Click the site for which you want to add the LAN segment.

The *Site-Name* page appears.

3. Click the add icon (+) on the **LAN** tab.

The Add LAN Segment page appears.

4. Complete the configuration settings according to the guidelines provided in [Table 34 on page 134](#).

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

5. Click **OK**.

You are returned to the *Site-Name* page, where the LAN segment that you added is displayed.

**Table 34: Add LAN Segment Settings**

Field	Description
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
Type	<p>Select the type of LAN segment:</p> <ul style="list-style-type: none"> <li>• <b>Directly Connected (default)</b>—Indicates that the LAN segment is directly connected to the site.</li> <li>• <b>Dynamic Routed</b>—Indicates that the LAN segment is not directly connected to the site and is reachable by using a dynamic route. If you select this option, you must specify the dynamic routing information.</li> </ul>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>
Department	<p>Select a department to which the LAN segment is assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You can group LAN segments as departments for ease of management and for applying policies at the department-level. For LAN segments that are dynamically routed, you can assign only a data center department.</p>
Protocol	<p>For dynamically routed LAN segments, select the routing protocol (BGP or OSPF) to be used by the data center department to learn routes from the data center.</p>
Gateway Address/Mask	<p>Enter a valid gateway IP address and mask for the LAN segment. This address will be the default gateway for endpoints in this LAN segment.</p> <p>For example: 192.0.2.8/24.</p>

Table 34: Add LAN Segment Settings (*continued*)

Field	Description
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP (default).</p> <p>You can enable DHCP if you want to assign IP addresses by using a DHCP server or disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, additional fields appear on the page.</p>
<b>Additional Fields</b>	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on the DHCP server.</p> <p>Default: 1440</p> <p>Range: 0 through 4,294,967,295 seconds.</p>
Name Server	<p>Specify one or more IPv4 addresses of the DNS server.</p> <p>To enter more than one DNS server address, type the address, press Enter, and then type the next address.</p> <p><b>NOTE:</b> DNS servers are used to resolve hostnames into IP addresses.</p>

Table 34: Add LAN Segment Settings (*continued*)

Field	Description
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the Switch device and creates the same LAN segment on the Switch.</li> </ul> <p>If you click to exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field.</p> <p>CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is a physical SRX Series device.</p>
Switch Ports  <b>NOTE:</b> This field is displayed only when LAN capability is selected for the enterprise hub.	<p>If you disable the CPE ports field, select ports on the switch to be part of the LAN segment. The Switch ports and CPE ports are mutually exclusive.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>
<b>BGP Configuration</b>	
Authentication	<p>Select the BGP route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• None—Indicates that no authentication should be used. This is the default.</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> </ul>
Peer IP Address	Enter the IP address of the BGP neighbor.
Peer AS Number	Enter the autonomous system (AS) number BGP neighbor.
Auth Key	If you specified that MD5 should be used for authentication, specify an MD5 authentication key (password), which is used to verify the authenticity of BGP packets.
<b>OSPF Configuration</b>	
OSPF Area ID	Specify the OSPF area identifier to be used for the dynamic route.

Table 34: Add LAN Segment Settings (*continued*)

Field	Description
Authentication	<p>Select the OSPF route authentication method to be used:</p> <ul style="list-style-type: none"> <li>• Password—Indicates that password-based authentication should be used. If you choose this option, you must specify the password. (This is the default).</li> <li>• Use MD5—Indicates that MD5 is to be used for authentication. If you choose this option, you must specify an authentication key.</li> <li>• None—Indicates that no authentication should be used.</li> </ul>
Password	Enter the password to be used to verify the authenticity of OSPF packets.
Confirm Password	Retype the password for confirmation purposes.
MD5 Auth Key ID	<p>If you specified that MD5 should be used for authentication, enter the OSPF MD5 authentication key ID.</p> <p>Range: 1 through 255.</p>
Auth Key	If you specified that MD5 should be used for authentication, enter an MD5 authentication key, which is used to verify the authenticity of OSPF packets.

## Deploying LAN Segments

After you create a LAN segment and assign it to a department, you must deploy the LAN segment. You can deploy LAN segments from the *Site Name* page.

To deploy one or more LAN segments:

1. Click the **LAN** tab.
2. Select one or more LAN segments that you want to deploy and click **Deploy**.

A Deploy LAN Segment job is created.

**NOTE:** If a Deploy LAN Segment job is in progress for a site, wait for the job to finish before triggering another Deploy LAN Segment job.

If you attempt to trigger a Deploy LAN segment job when another one is running, the job fails with a message indicating that the previous LAN segment deployment job is in progress.

3. Click **More > Deploy History** to view job status and deployment history of the LAN segment.

The **Deploy LAN Segment History** page displayed.

Alternatively, you can verify the status of the job from the **Monitor > Jobs** page.

## Reassigning a Department to a LAN Segment

You can reassign the department assigned to a LAN segment from the *Site Name* page. .

To reassign a department:

1. Click the **LAN** tab.
2. Select a LAN segment and click **Re-assign Department**.

The Re-assign Department page appears.

**NOTE:** You cannot reassign a LAN segment that is already assigned to a department and is deployed.

3. Select the department to which the LAN segment is to be assigned.
4. Click **Deploy**.

The success message **Re-assign department succeeded.** is displayed.

5. Click **OK**.

The LAN segment with the newly assigned department is displayed on the tenant site page.

## Deleting LAN Segments

You can delete a LAN segments from the *Site Name* page.

To delete a LAN segment:

1. Select a LAN segment and click the delete icon (X) icon on the **LAN** tab.

The Delete LAN Segment page appears.

2. Click **OK** to confirm deletion.

The LAN segment is deleted.



## Managing a Single Site

You can use the **Sites** page to view the site details and to manage the site configurations for a single site. To access the page, click **Resources > Site Management** and then click the site that you want to manage.

You can perform the following tasks from this page:

- On the **Overview** tab, view detailed information about the tenant site, such as geographical location, connection details, device details, alarms, and alerts.
- On the **WAN** tab, view detailed information about the WAN links, such as topology of the hub-site WAN links, total number of hub and spoke links, total number of applications, link utilization details, link metrics based on throughput, and the maximum bandwidth capacity of a WAN link in a site. Hover over the WAN link to view bandwidth capacity.

You can add or delete a VPN tunnel between a source site and destination site. For more information about creating and deleting VPN tunnels between a source site and destination site, see [“Adding On-Demand VPN Tunnels” on page 173](#) and [“Deleting On-Demand VPN Tunnels” on page 175](#).

For sites owned by a tenant in a full mesh topology, you can view all the WAN link connections between WAN interfaces in all the sites. Click a site to see all connections between its WAN interfaces.

- On the **Services** tab, view services, deploy network services, start a service, and disable services for a tenant site. You can also view the topology of the site.

To deploy a network service to a site, select the service, and then select an attachment point in the topology graphic. Alternatively, drag and drop the network service to an attachment point in the topology graphic.

- On the **Policies** tab, view the following details:
  - List of all policies applicable to a tenant site. Click the policy name to view the rules that are applicable for the tenant site. Click the edit icon at the end of the row to edit a policy. You are taken to the **Configuration > Policy** page, where you can edit the policies.
  - Details about the tenant user who last updated the policy.
  - Time when the policy was last updated.
  - Deployment status of the policy—deployed or not deployed.
  - Number of rules applicable to the site compared to the total number of rules applicable to the tenant.

- On the **LAN** tab, view, create, deploy, and delete a LAN segment. In addition, you can use this tab to reassign a LAN segment to a different department. See [“Managing LAN Segments on a Tenant Site” on page 133](#).
- On the **Devices** tab, view a list of devices in your network. See [“About the Devices Page” on page 210](#).

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)

[Dynamic VPN Tunnels Overview | 171](#)

## Viewing the Sites History

### IN THIS SECTION

- [Viewing Jobs Initiated to Add and Configure Sites | 140](#)
- [Viewing Jobs Initiated to Delete Sites | 141](#)

### Viewing Jobs Initiated to Add and Configure Sites

You can view the jobs initiated to add and configure all the sites in a tenant from the Sites page.

To view the jobs executed to add and configure sites:

1. Click **Resources > Site Management**.

The Sites page appears.

2. On the Sites page, click **More > View Add Site History**.

The Add/Configure Site History page appears. The Add/Configure Site History pane lists the jobs executed for adding and configuring all the sites in a tenant.

[Table 35 on page 141](#) describes the fields displayed on the Add/Configure Site History page.

Table 35: Fields on the Add/Configure Site History Page

Field	Description
In Progress	Number of jobs in progress.
Success	Number of jobs that were successfully executed.
Failure	Number of jobs that failed during execution.
Name	<p>Name of the job executed to add a site.</p> <p>Click the hyperlinked name to open the Site History Tasks page, where the tasks executed to complete the job are listed. Click the task link to open the Job Status page, where you can view the date and time when various tasks were executed to complete the job.</p>
Start Date	Date and time that the job was initiated.
End Date	<p>Date and time that the job finished executing.</p> <p>If the job is in-progress or failed, no date is displayed.</p>
Status	Indicates whether the job completed successfully (Success) or not (Failed).
Log	<p>Link to the log generated for the job.</p> <p>Click the link to view the logs on the Job Status page. The Job Status page displays the date and time when the job and various tasks associated with the job were executed in chronological order.</p>

## Viewing Jobs Initiated to Delete Sites

To view jobs initiated to delete sites from a tenant:

1. Click **Resources > Site Management**.

The Sites page appears.

2. On the Sites page, click **More > View Delete History**.

The Delete History page appears. The Delete History page lists the all the jobs executed for deleting sites from a tenant.

Table 36 on page 142 details the fields displayed on the Delete Site History page.

Table 36: Fields on the Site Delete History Page

Field	Description
In Progress	Number of jobs in progress.
Success	Number of jobs that were successfully executed.
Failure	Number of jobs that failed during execution.
Name	<p>Name of the job executed to delete a site.</p> <p>Click the hyperlinked name to open the Site History Tasks page, where the tasks executed to complete the job are listed. Click the task link to open the Job Status page, where you can view the date and time when various tasks were executed to complete the job.</p>
Start Date	Date and time that the job was initiated.
End Date	<p>Date and time that the job finished executing.</p> <p>If the job is in-progress or failed, no date is displayed.</p>
Status	Indicates whether the job completed successfully (Success) or not (Failed).
Log	<p>Link to the log generated for the job.</p> <p>Click the link to view the logs on the Job Status page. The Job Status page displays the date and time when the job and various tasks associated with the job were executed in chronological order.</p>

## SEE ALSO

[About the Sites Page | 40](#)
[Deleting a Site | 142](#)

## Deleting a Site

You can delete a site from the Sites page (**Resources > Site Management**) in the Customer Portal.

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

- You can delete only one site at a time.
- You cannot delete a gateway or hub site when spoke sites are connected to it. You must first delete the spoke sites associated with a gateway site or hub site and then delete the gateway or hub site.
- You cannot delete a site that is associated with site-specific policies. You must first delete the intents in the policy that are associated with the site, redeploy the policy, and then delete the site.
- You must delete service instances before attempting to delete the site.

To delete a site:

1. Click **Resources > Site Management**.

The Sites page appears.

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

The Remove Site Options dialog box appears.

3. Select one of the following options:

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

4. Click **OK**.

A job to remove the site is created. After the job completes successfully, a message appears on top of the Sites page indicating that the site is deleted.

If the delete site operation is successful, configurations associated with the site are deleted from the hub, a peer site, and virtual Route Reflectors (VRRs).

#### NOTE:

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

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)

[Contrail Service Orchestration Monitoring and Troubleshooting Guide](#)

# Managing Site Groups

IN THIS CHAPTER

- About the Site Groups Page | 144
- Creating Site Groups | 145

## About the Site Groups Page

To access this page, click **Resources > Site Groups**.

You can use the **Site Groups** page to view, create, and delete site groups for a tenant. Site groups enable you to group sites logically, thereby easing site management. You can use site groups to apply policies at the site group level.

You must be a Tenant Administrator user to access the **Site Groups** page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details of existing site groups. Click the details icon that appears when you hover over the name of a site group or select **More > Detailed View**.
- Create site groups. See [“Creating Site Groups” on page 145](#).
- Edit site groups. Select a site group and click the edit icon.
- Delete site groups. To delete a site group, select it on the Site Groups page and click the delete (X) icon.

### Field Descriptions

[Table 37 on page 145](#) shows the descriptions of the fields on the **Site Groups** page.

Table 37: Fields on the Site Groups Page

Field	Description
Name	Displays the name of the site group.
Sites	Displays the names of the sites that are members of a site group.

RELATED DOCUMENTATION

| [Creating Site Groups](#) | 145

## Creating Site Groups

You can use the **Create Site Group** page to create a new site group for a tenant and add sites to it.

To create a site group:

1. Click **Resources > Site Groups**.  
The Site Groups page appears.
2. Click the add icon (+).  
The **Create Site Group** page appears.
3. Enter a unique name for the site group.
4. From the list of sites in the **Available** column, select the sites that you want to include in the new group and click the greater-than icon (>).  
The selected sites are moved to the **Selected** column.
5. Click **OK**. If you want to discard your changes, click **Cancel** instead.  
The new site group is displayed on the **Site Groups** page.

RELATED DOCUMENTATION

| [About the Site Groups Page](#) | 144

# Managing Site Templates

## IN THIS CHAPTER

- [About the Site Templates Page | 146](#)
- [Adding On-Premise Spoke Sites by Using a Site Template | 147](#)
- [Adding a Site Template | 149](#)
- [Cloning, Editing, and Deleting Site Templates | 162](#)
- [Adding and Configuring Sites by Importing a JSON File | 165](#)

## About the Site Templates Page

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

You can use the Site Templates page to add site templates, edit, clone, delete, and view existing site templates.

A site template enables you to specify values for many of the attributes used to add a site. You can then use the site template to add multiple sites that share the same set of values (for attributes already specified in the site template) and only specify values for site-specific attributes.

Site templates are available only for on-premise spoke sites.

## Tasks You Can Perform

You can perform the following tasks from this page:

- Add a site template. See [“Adding a Site Template” on page 149](#)
- Edit, clone, or delete site templates. See [“Cloning, Editing, and Deleting Site Templates” on page 162](#).
- View site template details. The site templates are displayed in card format. For each site template you can view the following details:
  - Template name
  - Published by
  - Capability type



- Number of devices attached
- Number of WAN links, if applicable
- Number of sites that the device template is attached to
- Date and time that the template was last updated

## Adding On-Premise Spoke Sites by Using a Site Template

Using a site template, you can add on-premise spoke sites in bulk either manually or by importing the JavaScript Object Notation (JSON) file that contains on-premise site attributes.

To add on-premise spoke sites by using a site template:

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

The Sites page appears.

2. Click **Add** and select **Add On-Premise Spoke Site (Using Site Template)**.

The Add Spoke Site page appears listing the existing site templates.

3. Select the site template and click **Continue**.

The Add Spoke Site page appears.

4. The **Site Template** field displays the name of the site template that you have selected. If you want to change the site template, click the **Change** link and select another site template of your preference from the Add Spoke Site page.

5. Do one of the following to add on-premise spoke sites:

- To add on-premise spoke sites in bulk by importing the JSON file:
  - a. Select **Import from file** in the Site Data field.
  - b. (Optional) Click **Download sample JSON file** to download a sample JSON template and use it to specify site data that you can later import.
  - c. Click **Browse** to upload the JSON file.
  - d. Navigate to the folder and select the JSON file.
  - e. Click **Open**.
- To manually add on-premise spoke sites in bulk, select **Add Manually** in the Site Data field.

The Site 0 tab appears listing the fields based on the capabilities that were selected for the site template. For example, if the site template that you selected has only LAN capability, only general information fields and fields related to LAN capability are displayed.

6. Complete the configuration for Site0.

For more information on the fields for adding an on-premise spoke site with the following capabilities:

- WAN capability as SD-WAN, see [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81.](#)
- WAN capability as Hybrid WAN, see [“Adding an On-Premise Spoke Site with Hybrid WAN Capability” on page 76.](#)
- WAN capability as Next Gen Firewall, see [“Adding a Standalone Firewall Site” on page 128.](#)
- WAN capability as SD-WAN and LAN capability, see [“Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities” on page 94.](#)
- WAN capability as Next Gen Firewall and LAN capability, see [“Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities” on page 114.](#)
- Only LAN capability, see [“Adding an On-Premise Spoke Site with LAN Capability” on page 110.](#)

7. Click the plus icon (+) to add more sites and complete the configuration for each site.

8. Review the sites.

If there are validation errors, an error icon appears in the left pane (next to the site name ). You must ensure that all errors are resolved before proceeding.

9. (Optional) You can remove a site by clicking the **X** icon when you hover over the site name in the left pane.

10. Click **Save**.

A confirmation message is displayed indicating that the job is created for adding sites in bulk.

## RELATED DOCUMENTATION

[Adding a Site Template | 149](#)

[About the Site Templates Page | 146](#)

[Cloning, Editing, and Deleting Site Templates | 162](#)

# Adding a Site Template

You can add a site template for an on-premise spoke site. A site template can be added with one WAN capability (SD-WAN, or Hybrid WAN, or Next Gen Firewall), LAN capability, or both WAN and LAN capabilities.

**NOTE:** If you select the WAN capability as Hybrid WAN you cannot select the LAN capability.

To add a site template:

1. Select **Resources > Site Templates**.

The Site Templates page appears.

2. Click the plus icon (+).

The Add Site Template page appears.

3. Complete the configuration according to the guidelines in [Table 38 on page 149](#).

The fields that are displayed in the Add Site Template page are based on the LAN and WAN capabilities that you choose. The last column of [Table 38 on page 149](#) indicates the capabilities for which a field is applicable.

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

4. Click **OK**.

The site template is added and listed in the Site Templates page. You can use the site template to add multiple on-premise spoke sites.

**Table 38: Fields on the Add Site Template Page**

Field	Description	Applicable To
<b>General Tab</b>		
Template Name	Specify a unique name for the site template that can contain alphanumeric characters and hyphens (-); the maximum length is 32 characters.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Description	Enter a description for the site template; the maximum length is 512 characters.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
<b>Site Information</b>		
Site Group	Select a site group to which you want to assign the template. Example: sdwan-spoke	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
<b>Site Capabilities</b>		
WAN Capabilities	<p>Select one of the following WAN capabilities to include LAN capabilities for the site template:</p> <ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• You must select at least one WAN capability or a LAN capability.</li> <li>• The WAN capabilities that are displayed here are filtered based on the service type that are assigned to the tenant.</li> </ul>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul>
LAN Capabilities	<p>Select <b>LAN</b> to include LAN capabilities for the site template.</p> <p>This field is disabled if the WAN capability is Hybrid WAN.</p>	LAN
<b>Configuration</b>		
Primary Provider Hub	Select the provide hub site (or primary provider hub site in case of multihoming) to which the spoke site must connect.	SD-WAN

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Secondary Provider Hub	<p>Select the secondary provider hub site to which this site must connect.</p> <p>This site connects to the secondary provider hub site when the primary provider hub is down.</p>	SD-WAN
Primary Enterprise Hub	<p>Select the primary enterprise hub with which you want to connect the spoke site. If you specify a enterprise hub, then the initial site-to-site traffic as well as the central breakout (backhaul) traffic (if applicable) is sent through the enterprise hub instead of the hub site.</p>	SD-WAN
Secondary Enterprise Hub	<p>Select the secondary enterprise hub for this spoke site.</p> <p>The spoke site connects with secondary enterprise hub when the primary enterprise hub is down.</p>	SD-WAN
Create Threshold	<p>Enter the maximum number of sessions closed between the connected sites in a duration of two minutes at which full mesh is created between the two sites.</p> <p>The default value is 5.</p> <p>For example, if you specify the number of sessions as 5, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes exceeds 5.</p>	SD-WAN

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Delete Threshold	<p>Enter the number of sessions closed between the connected sites in a duration of 15 minutes below which full mesh is deleted between the two sites.</p> <p>The default value is 2.</p> <p>For example, if you specify the number of sessions closed as 2, dynamic VPN tunnels are deleted if the number of sessions closed is lesser than or equal to 2.</p>	SD-WAN
<b>Address and Contact Information</b>		
Street Address	Enter the street address of the site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
City	Enter the city where the site is located.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
State/Province	Select the state or province where the site is located.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
ZIP/Postal Code	Enter the postal code for the site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>

Table 38: Fields on the Add Site Template Page (continued)

Field	Description	Applicable To
Country	<p>Select the country where the site is located. Click the <b>Validate</b> button to verify the address. The <b>site address verification successful</b> message is displayed if the address is correct. You can click the <b>View location on a map</b> link to see the address location.</p> <p>If you enter the wrong address and click the <b>Validate</b> button to verify the address, the <b>Site address could not be validated message</b> is displayed .</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
Contact Name	Enter the name of the contact person at the site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
Email	Enter the e-mail address of the contact person at the site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
Phone	Enter the phone number for the site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
<b>Advanced Configuration</b>		
Domain Name Server  <b>NOTE:</b>  Starting from CSO Release 5.3.0, the Domain Name Server field is referred as <b>Name Server IP List</b>	<p>Specify one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on..</p> <p>DNS servers are used to resolve hostnames into IP addresses.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>

Table 38: Fields on the Add Site Template Page (continued)

Field	Description	Applicable To
NTP Server	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more NTP servers.</p> <p>Example: ntp.example.net</p> <p>The site must have DNS reachability to resolve the FQDN during site configuration.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
Select Timezone	Select the time zone in which the site is located from the drop-down list.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> <li>• LAN</li> </ul>
<b>WAN Tab</b>		
<b>Device Template</b>		
Device Series	<p>Select the device series to which the CPE belongs (SRX, NFX150, or NFX250) and select a device template for the selected device series.</p> <p>The device template contains information for configuring a device.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> </ul>
Device Model	For NFX150 devices, select a device model from the list. Device models are listed based on the connection plan that you select.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> </ul>
Auto Activate	<p>Click the toggle button to enable or disable automatic activation of the CPE when the CPE is detected by CSO ( management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning of the device is automatically triggered after the site with the CPE is added to CSO.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul>



Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Pre Staged	<p>Click the toggle button to use the preconfigured settings for the firewall device. The preconfigured settings are as follows:</p> <ul style="list-style-type: none"> <li>• Device Template—NGSRXZTP</li> <li>• In-band Management Port—ge-0/0/0 port</li> <li>• Firewall Policies—Factory_Default_Fw_Policy</li> <li>• NAT Policies—Factory_Default_NAT_Policy</li> </ul>	Next Gen Firewall
Boot Image	<p>Select the boot image from the drop-down list if you want to upgrade the image for the CPE device.</p> <p>The boot image is the latest build image uploaded to the image management system. The boot image is used to upgrade the device when the CSO starts the ZTP process.</p> <p>If the boot image is not provided, then the device skips the procedure to upgrade the device image. The boot image (NFX or SRX) is populated based on the device template that you have selected while adding a site. See <i>Uploading a Device Image</i>.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul>
In-band Management Port	Select the port that you want to configure as management interface and connect it to the management device. You can configure any of the ge-0/0/x ports, where x ranges from 0 to 14, as in-band management interfaces.	Next Gen Firewall
Firewall Policies	Select the firewall policy that you want to deploy. The firewall policy list is populated from the <b>Configuration &gt; Firewall &gt; Firewall Policy</b> page.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul>
NAT Policies	Select the NAT policy that you want to deploy to the standalone firewall site. The NAT policy list is populated from the <b>Configuration &gt; NAT &gt; NAT Policies</b> page.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> <li>• Next Gen Firewall</li> </ul>
CPE AS Number	Specify the autonomous system (AS) number for the CPE device on the site.	Hybrid-WAN

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Router Name	Specify the router name.	Hybrid-WAN
Router AS Number	Specify the AS number for the router in the point of presence (POP).	Hybrid-WAN
WAN 0	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN_0 link is enabled.</p> <p>When you enable a WAN link, fields related to the WAN link appear. Fields marked with an asterisk (*) must be configured to proceed.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> </ul>
Link Type	Select the underlay network type (MPLS or Internet) of the WAN link that is connected to the on-premise spoke site.	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• Hybrid-WAN</li> </ul>
Egress Bandwidth	Enter the maximum bandwidth (in mega bits per second [Mbps]) to be allowed for the WAN link. Range: 1 through 10,000	SD-WAN
Address Assignment	<p>Select the method for IP address assignment. The options available are:</p> <ul style="list-style-type: none"> <li>• DHCP—Select DHCP to assign IP address by using a DHCP server.</li> <li>• STATIC—Select STATIC to assign a static IP address.</li> </ul>	SD-WAN
<b>Advanced Settings</b>		
Provider	Enter the name of the service provider who is responsible for providing the WAN link.	SD-WAN
Cost/Month	<p>Enter the cost per month (in the specified currency) of the subscribed bandwidth.</p> <p>Range: 1 through 10,000</p>	SD-WAN
Enable Local Breakout	Click the toggle button to enable local breakout on the WAN link. By default, local breakout is disabled.	SD-WAN

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Use For Fullmesh	Click the toggle button to specify that the WAN link is part of a fullmesh topology.	SD-WAN
Connects To Hubs	<p>Click the toggle button to specify that the WAN link of the site connects to a hub.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>For sites with a single CPE, you must enable at least one WAN link to connect to the hub so that OAM traffic can be transmitted.</li> <li>For sites with a dual CPE, you must enable at least one WAN link per device to connect to the hub so that OAM traffic can be transmitted.</li> </ul>	SD-WAN
Backup Link	Select a backup link through which traffic can be routed when the primary (other) links are unavailable.	SD-WAN
Default Link	Select one or more links to be used for routing traffic in the absence of matching SD-WAN policy intents.	SD-WAN
Data VLAN Id	<p>Enter the VLAN ID that is associated with the data link. A data VLAN identifier is an integer.</p> <p>Range: 0 through 65,535</p>	SD-WAN
VLAN ID	Specify the identifier for the Layer 2 VLAN for the CPE device.	Hybrid-WAN
WAN 1	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN 1 link is disabled.</p> <p>Refer to the fields described for WAN 0 for an explanation of the fields.</p>	<ul style="list-style-type: none"> <li>SD-WAN</li> <li>Hybrid-WAN</li> </ul>

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
WAN 2	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN 2 link is disabled.</p> <p>Refer to the fields described for WAN 0 for an explanation of the fields</p>	SD-WAN
WAN 3	<p>Click the toggle button to enable or disable this WAN link. By default, the WAN 3 link is disabled.</p> <p>Refer to the fields described for WAN 0 for an explanation of the fields</p>	SD-WAN

**Additional Configuration**

**NOTE:** Starting from CSO 5.3.0 release, the Additional Configuration section is added to the site templates to add device configuration to the template.

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Configuration Templates List	<p>Select one or more configuration templates from the list. This list is filtered based on the device that you select.</p> <p>Configuration templates are stage-2 templates that are added by your OpCo administrators or SP administrators or Tenant administrators.</p> <p><b>NOTE:</b> You must set the parameters of the configuration templates that you have selected before you move to the LAN section.</p> <p>To set the parameters for the selected configuration templates:</p> <ol style="list-style-type: none"> <li>1. After you select one or more configuration templates, click <b>Set Parameters</b>.</li> </ol> <p>The <b>Device Configurations</b> page appears. This page consists of two tabs—Configure and Summary.</p> <ol style="list-style-type: none"> <li>2. In the Configure tab, enter values for the parameters in each configuration templates.</li> </ol> <p>(Optional) View the CLI commands in the Summary tab.</p> <ol style="list-style-type: none"> <li>3. Click <b>OK</b>.</li> </ol> <p>You have added and set the parameters for the configuration templates that are part of the site template that you are creating.</p>	<ul style="list-style-type: none"> <li>• SD-WAN</li> <li>• LAN</li> <li>• Next Gen Firewall</li> </ul>
<b>LAN Tab</b>		
Device Type	<p>Select the type of switch—EX2300, EX3400, EX4300, EX4600, and EX4650</p> <p><b>NOTE:</b> Starting from CSO Release 5.1.0, you can select EX4600 and EX4650 device types.</p>	LAN

Table 38: Fields on the Add Site Template Page (*continued*)

Field	Description	Applicable To
Device Model	<p>Select the model for the switch that you chose in the Device Type.</p> <p><b>NOTE:</b> Starting from CSO Release 5.1.0, you can select models for EX4600 and EX4650 device types.</p>	LAN
LAN Segments	<p>Displays the LAN segment on the switch.</p> <p>To add a LAN segment, click the + icon on the top, right corner of the grid. The Add LAN Segment page appears. See <a href="#">Table 39 on page 160</a>.</p>	LAN
Auto Activate Switch	<p>Click the toggle button to enable or disable automatic activation of the switch when the switch is detected by CSO (that is, management status of the device is Device_Detected).</p> <p>When you enable this field, zero-touch provisioning of the switch is automatically triggered after the site with the switch is added to CSO.</p> <p><b>NOTE:</b> The device template that you select determines whether this option is enabled or disabled by default.</p>	LAN

Table 39: Fields on the Add LAN Segment Page

Field	Description
<b>Add LAN Segment</b>	
Name	<p>Enter a name for the LAN segment.</p> <p>The name for a LAN segment should be a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
VLAN ID	<p>Enter the VLAN ID for the LAN segment.</p> <p>Range: 2 through 4093.</p>

Table 39: Fields on the Add LAN Segment Page (*continued*)

Field	Description
Department	<p>Select a department to which the LAN segment is to be assigned.</p> <p>Alternatively, click the <b>Create Department</b> link to create a new department and assign the LAN segment to it. See <a href="#">“Adding a Department” on page 602</a> for details.</p> <p>You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>
Gateway Address/Mask	Enter a valid gateway IP address and mask for the LAN segment; for example, 192.0.2.8/24.
DHCP	<p>For directly connected LAN segments, click the toggle button to enable DHCP. DHCP is disabled by default.</p> <p>You enable DHCP if you want to assign IP addresses by using a DHCP sever. You disable DHCP if you want to assign a static IP address to the LAN segment.</p> <p><b>NOTE:</b> If you enable DHCP, fields related to DHCP-related parameters appear and must be configured.</p>
<b>[DHCP-Related Fields]</b>	
Address Range Low	Enter the starting IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Address Range High	Enter the ending IP address in the range of IP addresses that can be allocated by the DHCP server to the LAN segment.
Maximum Lease Time	<p>Specify the maximum duration (in seconds) for which a client can request for and hold a lease on a DHCP server.</p> <p>Range: 0 through 4,294,967,295.</p>
Name Server	Specify or select one or more IPv4 addresses of the DNS server. To enter more than one DNS server address, type the address, press Enter, and then type the next address, and so on. DNS servers are used to resolve hostnames into IP addresses.

Table 39: Fields on the Add LAN Segment Page (*continued*)

Field	Description
CPE Ports	<p>Click the toggle button to include or exclude the CPE in the LAN segment. When you include the CPE in the LAN segment:</p> <ul style="list-style-type: none"> <li>• CPE ports that you can include in the LAN segment are listed. Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</li> <li>• The <b>Switch Ports</b> field is disabled. CSO automatically assigns LAN ports on the switch device and creates the same LAN segment on the switch.</li> </ul> <p>If you exclude the CPE from the LAN segment, you must specify the switch ports that connect with the LAN in the <b>Switch Ports</b> field. CSO automatically assigns LAN ports on the CPE device and creates the same LAN segment on the CPE device.</p> <p><b>NOTE:</b> You can select only one port if the CPE is an SRX Series device.</p>
Switch Ports	<p>If you disable the CPE ports field, select ports on the switch that will be part of the LAN segment.</p> <p>Select the ports from the <b>Available</b> column and click the right-arrow to move the ports to the <b>Selected</b> column.</p>

## RELATED DOCUMENTATION

[About the Site Templates Page | 146](#)
[Cloning, Editing, and Deleting Site Templates | 162](#)
[Adding On-Premise Spoke Sites by Using a Site Template | 147](#)

## Cloning, Editing, and Deleting Site Templates

### IN THIS SECTION

- [Cloning Site Templates | 163](#)
- [Editing Site Templates | 163](#)
- [Deleting Site Templates | 164](#)



You can clone, edit, or delete a site template.

## Cloning Site Templates

You can clone a site template when you want to quickly create a copy of an existing site template.

To clone a site template:

1. Select **Resources > Site Templates**.

The Site Template page appears.

2. Select the site template that you want to clone.

3. Click **Clone**.

The Clone Site Template page appears.

4. Specify a unique name for the site template that can contain alphanumeric characters and hyphens (-); the maximum length is 32 characters.

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

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

The site template that you have cloned is displayed on the Site Templates page. You can modify the cloned site template as needed by clicking the edit icon.

## Editing Site Templates



**WARNING:** You cannot edit a site template if you have associated the site template with a site.

To edit a site template:

1. Select **Resources > Site Templates**.

The Site Template page appears.

2. Select the site template that you want to edit.

3. Click the edit icon (pencil) to modify the parameters.

The Edit Site Template page appears.

4. Edit the fields, as needed. Modify the fields according to the guidelines provided in [“Adding a Site Template” on page 149](#).

**NOTE:** You cannot edit the site template name.

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

A confirmation message appears, indicating the status of the edit operation. You can use the modified site template for creating multiple on-premise spoke sites.

## Deleting Site Templates



**WARNING:** You cannot delete a site template if you have associated the site template with a site.

To delete a site template:

1. Select **Resources > Site Templates**.

The Site Template page appears.

2. Click the site template that you want to delete and click the delete icon.

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

3. Click **Yes** to delete the site template.

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

## RELATED DOCUMENTATION

---

[About the Site Templates Page | 146](#)

---

[Adding a Site Template | 149](#)

---

[Adding On-Premise Spoke Sites by Using a Site Template | 147](#)

## Adding and Configuring Sites by Importing a JSON File

You can add and configure one or more sites in CSO by uploading a JavaScript Object Notation (JSON) file that contains the parameters for adding and configuring the sites.

Before you begin, ensure that the JSON file contains all the parameters required for each site that you want to add or configure.

**NOTE:** We recommend that you create the JSON file by referring to the sample JSON file provided by CSO. Refer to Step 3 of the procedure for downloading and modifying the sample JSON file..

To add and configure multiple sites by uploading a JSON file:

1. Click **Resources > Site Managemnet**.

The Sites page appears.

2. Click **Add** and select **Import Sites**.

The **Import Sites** page appears.

3. (Optional) Download a sample JSON file by clicking the **Download Sample JSON** link. Edit the parameters based on your requirements and save the file.

4. Click **Browse** and navigate to the directory that contains the JSON file.

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

6. Click **Import**.

A message is displayed indicating that the file is imported to CSO. After the file is imported to CSO successfully, you are returned to the Sites page, where you can view the newly added sites:

- If you enabled automatic activation for the sites, CSO activates and provisions the sites and sets the status of the sites to PROVISIONED.
- If you did not enable automatic activation, CSO sets the status of the sites to CONFIGURED. You must manually activate the sites after which CSO provisions the sites. See [“Activating a CPE Device” on page 181](#) or [“Activating Dual CPE Devices \(Device Redundancy\)” on page 195](#).

After the sites are activated and provisioned, you can install certificates and create policies for the sites. See the *Managing Policies, Profiles, and Proxies* section in this guide for details.

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)

[Manually Adding On-Premise Spoke Sites | 76](#)

# Managing Mesh Tags

## IN THIS CHAPTER

- [Mesh Tags Overview | 167](#)
- [About the Mesh Tags Page | 168](#)
- [Creating User-defined Mesh Tags | 169](#)

## Mesh Tags Overview

A mesh tag is a label that you associate with a WAN link of a spoke site. Mesh tags provide you the flexibility to establish overlay tunnels between WAN links of two different spoke sites. If WAN links are associated with same mesh tags, CSO creates a VPN tunnel between WAN links of spoke sites (enterprise hub to enterprise hub, on-premise spoke site to enterprise hub, on-premise spoke site to on-premise spoke site).

**NOTE:** Mesh tags are applicable only for SD-WAN sites in the Real-time optimized mode (Full mesh).

Mesh tags can be predefined (MPLS and Internet) or user-defined. You can create user-defined mesh tags on the **Administration > Mesh Tags** page.

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

For example, consider that a tenant has two sites—Site A and Site B. Site A has four WAN links (WAN\_A0 through WAN\_A3) and Site B has three WAN links (WAN\_B0 through WAN\_B2). WAN\_A0 and WAN\_B0 are associated with MPLS (predefined mesh tag), and WAN\_A1 and WAN\_B1 are associated with Internet (predefined mesh tag).

A tunnel is established between WAN-A0 and WAN-B0 because they are associated with the same predefined mesh tags.

**NOTE:** You can associate mesh tags for up to three WAN links.

RELATED DOCUMENTATION

[About the Mesh Tags Page | 168](#)

[Creating User-defined Mesh Tags | 169](#)

About the Mesh Tags Page

To access this page, select **Resources > Mesh Tags** in Customer Portal.

Use this page to view predefined mesh tags and create user-defined mesh tags. Mesh tags connect WAN links of different sites. CSO creates a tunnel between WAN links if they are associated with the same mesh tag (user-defined or predefined).

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a mesh tag—See [“Creating User-defined Mesh Tags” on page 169](#).
- Delete a mesh tag. Select a mesh tag and click the delete icon.

Field Descriptions

[Table 40 on page 168](#) describes the fields on the Mesh Tags page.

Table 40: Fields on the Mesh Tag Page

Field	Description
Name	Displays the name of the mesh tag.
Tenant	Displays the tenant name to which the site is associated.
Type	Displays whether the mesh tag is a predefined or a user-defined.

RELATED DOCUMENTATION

| [Mesh Tags Overview](#) | 167

## Creating User-defined Mesh Tags

CSO creates a tunnel between WAN links of two different sites if they are associated with the same mesh tag (user-defined or predefined).

To create a user-defined mesh tag:

1. Select **Resources > Mesh Tags**.

The Mesh Tags page appears.

2. Click the add icon (+) to create a mesh tag.

The Create New Mesh Tag page appears.

3. Complete the configuration according to the guidelines provided in [Table 41 on page 169](#).

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

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

The user-defined mesh tag is created.

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

Table 41: Fields on the Create New Mesh Tag Page

Field	Description
Name	Enter a unique name for the mesh tag.
Description	Enter a description for the mesh tag.

RELATED DOCUMENTATION

| [About the Mesh Tags Page](#) | 168

# Managing Dynamic VPN

## IN THIS CHAPTER

- [Dynamic VPN Tunnels Overview | 171](#)
- [Configuring Dynamic VPN Tunnels Thresholds for all Sites in a Tenant | 172](#)
- [Adding On-Demand VPN Tunnels | 173](#)
- [Deleting On-Demand VPN Tunnels | 175](#)



## Dynamic VPN Tunnels Overview

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

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

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

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

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

- The number of sessions closed between two spoke sites crosses the configured threshold value, and
- The WAN links of spoke sites have matching mesh tags. For more information, see [“Mesh Tags Overview” on page 167](#).

**NOTE:** The dynamic VPN feature is applicable only for SD-WAN sites in Real Time-Optimized mode (Full mesh).

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

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

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

That is, the threshold value that you specify on the Add Site page (On-premise or gateway) overrides the threshold value that you specified on the Dynamic VPN page of Customer Portal.

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

## RELATED DOCUMENTATION

| [Configuring Dynamic VPN Tunnels Thresholds for all Sites in a Tenant](#) | 172

## Configuring Dynamic VPN Tunnels Thresholds for all Sites in a Tenant

CSO dynamically creates or deletes a VPN tunnel (without passing through a enterprise hub or hub) between two spoke sites, if the following conditions are met:

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

For more information on dynamic VPN tunnels, see [“Dynamic VPN Tunnels Overview” on page 171](#).

**NOTE:** The Dynamic VPN page appears only for tenants with real-time optimized SD-WAN mode.

To modify threshold values at the tenant-level:

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

The Dynamic VPN page appears.

2. Complete the configuration according to the guidelines [Table 42 on page 173](#).

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

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

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

The threshold values that you specify are immediately applicable for all sites in the tenant.

**NOTE:** You can also modify the threshold values while adding a spoke site or a enterprise hub site. The threshold value that you specify on the Add Site page (On-premise or enterprise hub site) overrides the threshold value that you specified on the Dynamic VPN page of the Customer Portal.

Table 42: Fields on the Dynamic VPN page

Field	Description
Threshold	Select this check box to customize the dynamic VPN threshold value that will override threshold value specified at the global level (for all tenants).
Threshold for Creating a Tunnel	
Sessions Closed	<p>Specify the number of sessions closed (for a duration of 2 minutes) between two spoke sites.</p> <p>If the number of sessions closed (for a duration of 2 minutes) is greater than or equal to the value that you specified, a dynamic VPN tunnel is created between two spoke sites.</p> <p>The default threshold value (the number of sessions closed for 2 minutes) is 5.</p> <p>For example, if you specify the number of sessions closed as 10, dynamic VPN tunnels are created if the number of sessions closed between two spoke sites in 2 minutes is greater than or equal to 10.</p>
Threshold for Deleting a Tunnel	
Sessions Closed	<p>Specify the number of sessions closed (for a duration of 15 minutes) between two spoke sites.</p> <p>If the number of sessions closed (for a duration of 15 minutes) is lesser than or equal to the value that you specified, a dynamic VPN tunnel is deleted between two spoke sites.</p> <p>The default threshold value (the number of sessions for 15 minutes) is 2.</p> <p>For example, if you specify the number of sessions closed as 10, dynamic VPN tunnels are deleted if the number of sessions closed between two spoke sites in 15 minutes is less than or equal to 10.</p>

## RELATED DOCUMENTATION

[Dynamic VPN Tunnels Overview](#) | 171

## Adding On-Demand VPN Tunnels

An OpCo administrator or the Tenant administrator can create a VPN tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

To create a VPN tunnel between the source site and a destination site:

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

The Sites page appears.

2. Click the site to which you want to add VPN tunnels.

The *Site Name* page appears.

3. On the WAN tab, click +.

The Add On-Demand VPN Tunnel page appears.

4. Complete the configuration according to the guidelines [Table 43 on page 174](#).

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

A tunnel is created between the source site and a destination site.

**Table 43: Fields on On-demand VPN Tunnel page**

Field	Description
Add Tunnel Threshold	
Source Site	Displays the name of the source site.
Destination Site	Select the destination site from the list.
Delete Tunnel	
Displays the threshold value (sessions closed) below which a tunnel is deleted between two sites.	
Enable Threshold	By default, this toggle button is disabled. That is, even if the threshold value (sessions closed) is met, CSO does not delete VPN tunnels. You have to manually delete the VPN tunnel that you created.
Sessions Closed	Displays the number of sessions closed for 15 minutes.

## RELATED DOCUMENTATION

[Dynamic VPN Tunnels Overview](#) | 171

# Deleting On-Demand VPN Tunnels

A user with both OpCo administrator and Tenant administrator roles can delete a VPN tunnel between a source site and destination site by using the CSO GUI in Customer Portal.

To delete a VPN tunnel between a source site and a specific destination site:

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

The Sites page appears.

2. Click the site from which you want to delete VPN tunnels.

The *Site Name* page appears.

3. On the WAN tab, click +.

The Delete On-Demand VPN Tunnel page appears.

4. Complete the configuration according to the guidelines [Table 44 on page 175](#).

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

A VPN tunnel is deleted between the source site and a specific destination site.

**Table 44: Fields on the Delete On-Demand VPN Tunnel page**

Field	Description
Delete Tunnel Threshold	
Source Site	Displays the name of the source site.
Destination Site	Select the destination site from the list.
Delete Tunnel	
Displays the threshold value (sessions closed) below which a tunnel is deleted between two spokes.	
Enable Threshold	By default, this toggle button is disabled. That is, even if the threshold value (sessions closed) is met, CSO does not create VPN tunnels. You have to manually create the VPN tunnel that you deleted.
Sessions Closed	Displays the number of sessions closed for 2 minutes. .

## RELATED DOCUMENTATION

| [Dynamic VPN Tunnels Overview](#) | **171**

# 3

PART

## Managing Devices and Resources

---

Managing Devices | **178**

Managing Device Images | **205**

Managing Resources | **208**

Managing Licenses | **258**

Managing Signature Database and Certificates | **262**

Managing Juniper Identity Management Service | **274**

---

# Managing Devices

## IN THIS CHAPTER

- [Device Redundancy Support Overview | 179](#)
- [Activating a CPE Device | 181](#)
- [Manually Activating a Switch | 184](#)
- [Managing an EX Series Switch | 186](#)
- [Activating Dual CPE Devices \(Device Redundancy\) | 195](#)
- [Viewing the History of Tenant Device Activation Logs | 198](#)
- [Zero Touch Provisioning Overview | 200](#)
- [Workflow for Onboarding a Device Using ZTP | 201](#)



## 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:

- LTE WAN backup link
- Service chain support

**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:

- Dual NFX250 as SD-WAN CPEs—Supports dual CPE NFX Series devices on an SD-WAN site.
- Dual SRX as SD-WAN CPEs—Supports dual CPE SRX Series devices on an SD-WAN site.
- Dual SRX4x00 as SD-WAN CPEs—Supports SRX 4100 and SRX4200 devices as dual CPE devices in an SD-WAN site.

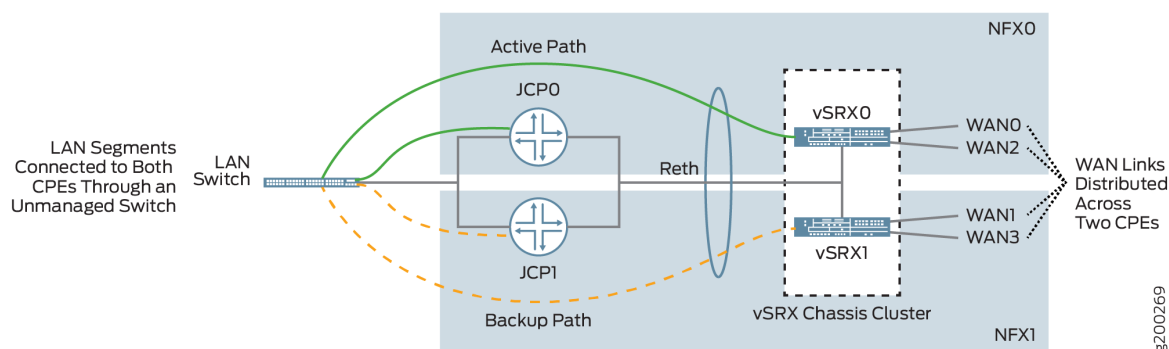
## Create and Configure an SD-WAN Site

You can create and configure an SD-WAN site with dual CPE devices and the two devices back up each other, with one node acting as the primary device and the other as the secondary device. The workflow to add and configure a site with dual CPE devices is similar to the single CPE device. For more information about creating and configuring a site with dual CPE devices, see [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81](#).

### Dual CPE Devices Logical Topology for NFX Network Services Platform

[Figure 7 on page 180](#) shows the logical topology of the NFX Series dual CPE devices.

Figure 7: Dual CPE Device Topology - NFX Network Services Platform



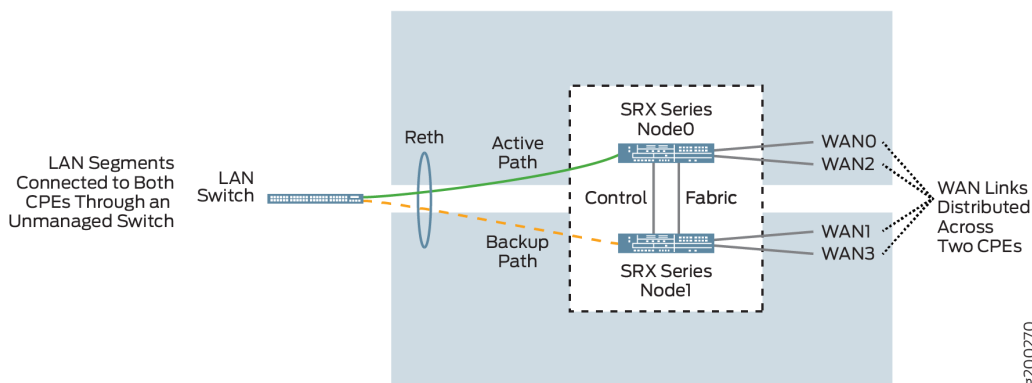
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

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 8 on page 181](#) shows the logical topology of the SRX Series dual CPE devices.

Figure 8: 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.

**NOTE:** On SRX 4100 and SRX4200 devices, out of the eight 1-Gigabit Ethernet/10-Gigabit Ethernet, a maximum of two ports are used for WAN links, and the remaining ports are used for LAN connectivity. The HA ports are used only for forming the cluster.

## RELATED DOCUMENTATION

[Adding an On-Premise Spoke Site with SD-WAN Capability | 81](#)

[Activating Dual CPE Devices \(Device Redundancy\) | 195](#)

## Activating a CPE Device

You can activate SRX300 Services Gateway and NFX250 Network Services Platform devices in the following ways:

- By connecting a computer to the LAN port of the device and entering the activation code through your browser
- By specifying the activation code in Customer Portal

You can activate a vSRX Services Gateway device by copying the configuration available in Customer Portal and pasting the configuration into the SRX Series device console. To copy the configuration in

Customer Portal, select the device and click **More > View Stage-1 Config** on the Devices page (**Resources > Devices**).

To activate a device through your web browser:

1. Connect a computer to the LAN port of the CPE device and power on the device.

Refer to the documentation for the CPE device for more information.

2. Open a Web browser in your computer.

Because the CPE device is preconfigured with a management address, the browser displays the login page.

3. Enter the activation code that you have received during the shipping process.

4. Click **OK**.

On successful authentication, the Phone-Home server pushes the initial configuration to the CPE device.

To activate a device through Customer Portal:

**NOTE:** If you activate the CPE device through Customer Portal, you do not need to activate it through a browser.

1. Log in to Customer Portal.

2. Click the Sites page in Customer Portal.

After you use Customer Portal to add a site that uses a CPE device, the CPE device icon on the Sites page is gray if the device is inactive. When you hover over the CPE device icon on the Monitor page, you should see the message **Device Status: Expected**, which indicates that the device is ready to be activated. If you see the message **Device Status: Undefined**, contact your service provider for assistance.

3. On the Device Status column, click **Activate Device**.

The Activate Device page appears. The Activate Device page consists of Device Information and Device Activation.

4. On Device Information page, view the site details, device details, and recipient details, and specify the activation code. For more information see, [Table 45 on page 184](#).

5. Click **Next**.

On Device Activation page, the device is activated through the following steps:

- Detecting the device
- Applying stage-one configuration to the device
- Bootstrapping of device
- Activating the device

After each successful step, you can see a green check mark. If any of these steps fail, a red exclamation mark appears.

6. After the activation process is complete, click **OK**.

The Sites page appears. To see the device activation status, hover over the device icon on the Sites page. You see one of the following statuses:

- **EXPECTED**—Device is ready for activation.
- **ACTIVE**—Device is authenticated but not yet operational.
- **ACTIVATION\_FAILED**—Device is not authenticated.
- **GWR\_SPAWNED**—Device gateway component spawning is successful.
- **GWR\_SPAWN\_FAILED**—Device gateway component spawning fails.
- **PROVISIONED**—Device is operational.
- **PROVISION\_FAILED**—Device failed to become operational. Contact your service provider for assistance.

**NOTE:** When a device is provisioned successfully, a job to install the default trusted certificates, which are packaged with Junos OS, on the device is triggered. You can view the details of the job (of type **default trustedcertificate**) on the Jobs page (**Monitor > Jobs**).

We recommend that you check the job status to verify that the default trusted certificates were successfully installed. If, however, the job failed and if you want to use the SSL proxy feature, manually install the trusted certificates on the device by using the following procedure:

- Log in to the device and access the Junos OS CLI (operational mode).
- Execute the **request security pki ca-certificate ca-profile-group load ca-group-name DEFAULT\_CSO filename default** command.

The installation takes between 2–5 minutes to complete, so wait until it is done.

- Exit the Junos OS CLI and log out of the device.

Table 45: Fields on the Activate Device Page

Field	Description
Site Name & Type	Name of the site on which the CPE device is activated.
Connected Hub	Name of the hub to which the CPE device is connected.
Device Model	Device model of the CPE device.
Serial Number	Serial number of the CPE device.
Activation Code	Specify the activation code that your service provider supplied for the CPE device.
Expiry Duration	Specify how long you must wait to activate the device after it boots up. You can set a duration in the range 1 through 600 seconds. The default is 120 seconds.
Recipient	Recipient details.

## RELATED DOCUMENTATION

[About the Sites Page | 40](#)

[Adding an On-Premise Spoke Site with SD-WAN Capability | 81](#)

[About the Certificates Page | 266](#)

## Manually Activating a Switch

You can manually activate a switch if you have disabled automatic activation while onboarding the switch to CSO.

**NOTE:** Before activating, ensure that the switch is powered on and connected to the CPE or firewall (if the switch is behind a CPE or firewall).

To manually activate the switch:

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

The Sites page appears.

2. On the Sites page, click on the site that you want to activate.

The detailed view of the site appears.

**NOTE:** You can activate a site that is in the CONFIGURED state.

3. Click the **Devices** tab.

4. Select the switch that you added to the site and click **Activate Device** to activate the switch.

The Activate Device page appears.

5. On the Activate Device page, enter the activation code for the switch. The activation code must match the activation code that you provided during the site addition workflow.

6. Click **Next**.

The progress of switch activation is displayed.

7. After the switch is activated, click **OK**.

The Sites page appears. The status of the switch is set to PROVISIONED if the switch is successfully activated. After the switch is activated, you can manage the switch by using CSO.

## RELATED DOCUMENTATION

[Activating a CPE Device | 181](#)

[Zero Touch Provisioning Overview | 200](#)

## Managing an EX Series Switch

### IN THIS SECTION

- [Viewing the Chassis Information of an EX Series Switch | 187](#)
- [Viewing Information about an EX Series Switch | 190](#)
- [Viewing Information about Ports on an EX Series Switch | 192](#)

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

To access this page, do one of the following:

- To access the *Device-Name* page from the Resources > Site Management menu:

1. Click **Resources > Site Management**.

The Sites page appears with a list of sites displayed under the Site Name column.

2. Click a site from this list.

The Site Management page appears with a list of devices displayed under the Device Name column of the Devices tab.

3. Select an EX Series switch from the list.

The *Device-Name* page appears.

- To access the *Device-Name* page from the Resources > Devices menu:

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

The Devices page appears.

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

The *Device-Name* page appears.



You can perform the following actions from this page:

### Viewing the Chassis Information of an EX Series Switch

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

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

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

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

See [Table 46 on page 187](#) for more details.

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

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

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

The Port Overview tab appears. [Table 51 on page 194](#) describes the fields on the Port Overview tab.

- View details of system meters—Hover over a system meter to view more information from the trays that appear. See [Table 47 on page 189](#) for more details.
- Perform various actions on an EX Series switch—Click **Actions** on the chassis view dashlet.

A list of all actions that you can perform on the switch is displayed. See [Table 48 on page 189](#) for more details.

[Table 46 on page 187](#) describes the fields on the port view pane.

**Table 46: Fields on the Port View Pane**

Field	Description
Admin Status	Administrative status of the port: <ul style="list-style-type: none"> <li>• Green—Indicates that the admin status is up (enabled).</li> <li>• Gray—Indicates that the admin status is down (disabled).</li> </ul>

Table 46: Fields on the Port View Pane (*continued*)

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

Table 47 on page 189 describes the system meters available on the chassis view dashlet. The system meters display current data.

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

**Table 47: System Meters on the Chassis View Dashlet**

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

[Table 48 on page 189](#) describes the actions that you can perform on an EX Series switch.

**Table 48: Options on the Actions List**

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

Table 48: Options on the Actions List (*continued*)

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

## Viewing Information about an EX Series Switch

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

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

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

[Table 49 on page 190](#) describes the dashlets on the Overview tab. The graphical representations on this tab display trends based on historical data.

Table 49: Dashlets on the Overview Tab

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

Table 49: Dashlets on the Overview Tab (*continued*)

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

Table 49: Dashlets on the Overview Tab (*continued*)

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

## Viewing Information about Ports on an EX Series Switch

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

[Table 50 on page 193](#) describes the fields on the Ports tab.

You can perform the following tasks on this tab:

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

[Table 51 on page 194](#) describes the fields on the Port Overview tab.

Table 50: Fields on the Ports Tab

Field	Description
Interface List	
Port	<p>Name of the port.</p> <p>Click each port to view additional information about the port, on the Port Overview page.</p> <p>See <a href="#">Table 51 on page 194</a> for details of dashlets that appear on the Port Overview page.</p>
Admin Status	<p>Indicates the administrative status of the port:</p> <ul style="list-style-type: none"> <li>• Up—if the port is enabled.</li> <li>• Down—If the port is disabled.</li> </ul>
Link Status	<p>Indicates the status of the link or connection to the port:</p> <ul style="list-style-type: none"> <li>• Up—If the connection to the port is up.</li> <li>• Down—If the connection to the port is down.</li> </ul>
MTU	<p>Maximum transmission unit (MTU) size (in bytes) on the ports.</p> <p>Default: 1500 bytes.</p>
Negotiated Speed	Current negotiated speed (in Kbps, Mbps, and Gbps) of the port.
Link Mode	Mode in which the port operates—Half-duplex or Full-duplex.
Media Type	Type of transmission medium—Copper or Fiber.
Power Consumption	Power consumed by the port, in Watts (W).
VLAN ID	<p>ID of the VLAN configured on the port.</p> <p>Range: 1 through 4094.</p>
Input Bandwidth Utilization	Bandwidth (in %) consumed by the incoming packets on the port.
Output Bandwidth Utilization	Bandwidth (in %) consumed by the outgoing packets on the port.
Input Drops	Number of incoming packets dropped by the port due to congestion.
Output Drops	Number of outgoing packets dropped by the port due to congestion.

**Table 50: Fields on the Ports Tab (*continued*)**

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

[Table 51 on page 194](#) describes the dashlets available on the Port Overview tab.

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

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

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

**Table 51: Dashlets on the Port Overview Tab**

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



Table 51: Dashlets on the Port Overview Tab (*continued*)

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

## RELATED DOCUMENTATION

[Managing a Single CPE Device](#) | 226

## Activating Dual CPE Devices (Device Redundancy)

You can activate a device after the device status is changed to **EXPECTED** in the Sites page. When you see the device status is **EXPECTED**, it indicates that the device is ready to be activated. If you see the device status as **Undefined**, contact your service provider for assistance.

**NOTE:** You must activate both the primary and the secondary devices simultaneously.

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.

To activate dual CPE devices used as a cluster:

1. Log in to Customer Portal.

2. Select **Sites**.

The Sites page appears.

3. Click on the *Site Name*.

The *Site Name* page appears.

4. On **Devices** tab, select the cluster device and click **Activate Device**.

The Activate Device page appears. The Activate Device page consists of Device Information and Device Activation tabs.

**NOTE:** You can also activate the device through **Resource > Devices** page.

5. On **Device Information** page, complete the configuration according to the guidelines provided in [Table 52 on page 196](#).

**Table 52: Fields on the Activate Device Page**

Field	Description
Site Name & Type	View the name of the site on which the CPE device is activated.
Connected Region	View the name of the region to which the CPE device is connected.
Primary Device Serial Number	View the serial number of the primary CPE device.
Primary Device Activation Code	<p>Enter the activation code of the primary device that your service provider supplied for the device.</p> <p><b>NOTE:</b> If you do not want to specify an activation code, on the <b>Resources &gt; Edit Template &gt; Template Settings</b> page, disable the ACTIVATION_CODE_ENABLED field and save the changes.</p>

Table 52: Fields on the Activate Device Page (*continued*)

Field	Description
Secondary Device Serial Number	View the serial number of the secondary CPE device.
Secondary Device Activation Code	<p>Enter the activation code of the secondary device that your service provider supplied for the device.</p> <p><b>NOTE:</b> If you do not want to specify an activation code, on the <b>Resources &gt; Edit Template &gt; Template Settings</b> page, disable the <code>ACTIVATION_CODE_ENABLED</code> field and save the changes.</p>

6. Click **Next**.

The Activate Device page appears.

7. On **Activate Device** page, the cluster device (both primary and secondary) is activated through the following steps:

- Device is detected
- Stage-one configuration apply on device is successful
- Bootstrap of device success
- Activation of device is successful
- Device is modelled and is expected to be activated
- Device is active
- Device gateway component is spawned
- Device gateway router is put into cluster mode.
- Device is successful provisioned

After each successful step, you can see a green check mark. If any of these steps fail, a red exclamation mark appears.

8. After the activation process is complete, click **OK**.

The *Site Name* page appears. If the device activation is successful, the management status of the cluster device is changed to **PROVISIONED**. You can also see the following device states:

- **EXPECTED**—Device is ready for activation.
- **ACTIVE**—Device is authenticated but not yet operational.
- **ACTIVATION\_FAILED**—Device is not authenticated.

- **GWR SPAWNED**—Device gateway component spawning is successful.
- **GWR SPAWN\_FAILED** —Device gateway component spawning fails.
- **PROVISIONED**—Device is operational.
- **PROVISION\_FAILED**—Device failed to become operational. Contact your service provider for assistance.

**NOTE:** The **GWR SPAWNED** and **GWR SPAWN\_FAILED** statuses are not applicable for dual CPE SRX Series Services Gateway devices.

## RELATED DOCUMENTATION

[Device Redundancy Support Overview | 179](#)

[Activating a CPE Device | 181](#)

[About the Sites Page | 40](#)

[Adding an On-Premise Spoke Site with SD-WAN Capability | 81](#)

[About the Certificates Page | 266](#)

## Viewing the History of Tenant Device Activation Logs

You can use the Activation Logs page to view the history of device activation logs. You can also view the details of the activation logs and their status.

To view the tenant device activation logs:

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

The Tenant Devices page appears, which list all devices.

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

The Activation Logs page is displayed. [Table 53 on page 199](#) describes the fields on the Activation Logs page.

3. Click a task name.

The ZTP Logs page appears. [Table 54 on page 199](#) describes the fields on the ZTP Logs page.

4. Click the Task Name.

The Job Status page appears. [Table 55 on page 200](#) describes the fields on the Job Status page.

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

**Table 53: 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 54: 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 55: 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](#)

## Zero Touch Provisioning Overview

Zero Touch Provisioning (ZTP) enables you to configure and provision devices automatically, and thus reduces the manual intervention required for adding devices to a network.

In Contrail Service Orchestration (CSO), the ZTP of a device involves the following high-level steps:

1. Activate the device that is associated with the site.
2. The device contacts CSO through the Redirect Server or Phone Home Client (PHC) and the stage-1 (initial) configuration is automatically applied to the device, allowing CSO to establish a secure management connection with the device. The process of applying the stage-1 configuration to the device is called as bootstrapping.
3. CSO automatically applies the provisioning configuration on the device after the completion of the bootstrapping process.

The provisioning configuration is generated by CSO and is applied on a device to make it functional and ready for the intended functionality. For example, provisioning configuration can include IPsec or GRE tunnel configurations, virtual route reflector (vRR) configuration, routing configuration, and so on.

For additional functionality, you can create the stage-2 configuration and apply the configuration to the device by using the CSO GUI. For example, the stage-2 configuration can include LAN configuration, firewall policies, and so on.

After the ZTP process is complete, the device is provisioned.

## Devices Supported

In CSO, you can provision the following devices (including dual CPE devices, if applicable), by using ZTP:

- NFX150 and NFX250 Series
- SRX300, SRX320, SRX340, SRX345, SRX550 High Memory (SRX550M), and SRX1500
- vSRX on an x86 server
- EX2300, EX3400, and EX4300 Series switches

## Benefits

Using ZTP offers the following benefits:

- Simplified, faster, and automated deployment of configurations.
- Auto-generated configurations that are more accurate.
- Faster scaling of the network because you need not manually apply configuration on each device in the network.

## RELATED DOCUMENTATION

| [Workflow for Onboarding a Device Using ZTP | 201](#)

## Workflow for Onboarding a Device Using ZTP

Zero Touch Provisioning (ZTP) enables you to configure and provision devices automatically, minimizing the manual intervention required for adding devices to a network.

This topic provides a sequential list of tasks that you need to perform for successfully onboarding a device to the network by using ZTP:

1. From Customer Portal, add an on-premise spoke site or an enterprise site, and associate a device.

For more information on adding an on-premise spoke site with the following capabilities:

- WAN capability as SD-WAN, see [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81.](#)
- WAN capability as Hybrid WAN, see [“Adding an On-Premise Spoke Site with Hybrid WAN Capability” on page 76.](#)
- WAN capability as Next Gen Firewall, see [“Adding a Standalone Firewall Site” on page 128.](#)
- WAN capability as SD-WAN and LAN capability, see [“Adding an On-Premise Spoke Site with SD-WAN and LAN Capabilities” on page 94.](#)
- WAN capability as Next Gen Firewall and LAN capability, see [“Adding an On-Premise Spoke Site with Next Generation Firewall and LAN Capabilities” on page 114.](#)
- Only LAN capability, see [“Adding an On-Premise Spoke Site with LAN Capability” on page 110.](#)

For more information on adding an enterprise hub, see [“Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities” on page 48.](#)

## 2. Activate the device:

- If you have enabled the **Auto Activate** field while adding an on-premise site or an enterprise hub, ZTP of the device is automatically triggered after the site is added to CSO.
- If you have disabled the **Auto Activate** field while adding an on-premise site or an enterprise hub, you must manually activate the device.

To manually activate the device:

- a. Select **Resources > Site Management**.

The **Sites-Name** page appears.

- b. On the Sites page, click the site that you want to activate.

The detailed view of the site appears.

**NOTE:** You can activate a site that is in the CONFIGURED state.

- c. Click the **Devices** tab.
- d. Select the device that you added to the site and click **Activate Device** to activate the device.  
The Activate Device page appears.
- e. On the Activate Device page, enter the activation code for the device. The activation code must match the activation code that you provided during the site addition workflow.



- f. Click **Next**.

The progress of device activation is displayed.

- g. After the device is activated, click **OK**.

The Sites page appears.

- If you have to activate a vSRX or SRX4X00 Services Gateway devices:

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

The Sites page appears.

2. Click on the site that you want to activate.

The *Site-Name* page appears.

3. On the Devices tab, select the device that you want to activate and click **Stage1 Config**.

A new page appears displaying the stage-1 configuration of the device.

4. Click **Copy to Clipboard** to copy the stage-1 configuration of the device.

5. Log in to the CLI of the device and enter the configuration mode.

6. Paste the stage-1 configuration and commit.

The Phone-Home client or the Redirect Server authenticates the device and establishes a communication between the device and CSO.

After the device activation is complete, CSO applies the stage-1 configuration. The status of the device is changed from Expected to Active, which indicates the device is authenticated but not yet operational.

3. After authenticating the device, CSO automatically triggers a job to push the provisioning and stage-2 (optional) configurations.

You can use the Activation Logs page (**Resources > Tenant Devices > More > Activation Logs**) to view bootstrap logs (stage-1 configuration and device activation) and ZTP logs (provisioning and stage-2 configurations) and their status.

After the job is completed successfully:

- The provisioning configuration and stage-2 configuration (optional) are applied.
- The device state changes from Active to Provisioned, which indicates that the device is fully functional.

The newly-added device is provisioned and is onboarded to the network. You can apply SD-WAN and security policies, if applicable.

## RELATED DOCUMENTATION



# Managing Device Images

## IN THIS CHAPTER

- [Device Images Overview | 205](#)
- [About the Device Images Page | 205](#)
- [Deleting Device Images | 206](#)

## 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.

## RELATED DOCUMENTATION

| [About the Device Images Page | 205](#)

## About the Device Images Page

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

You can use the Images page to view the list of device images that are available in tenant's network.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a device image. Click the details icon that appears when you hover over the name of an image or click **More > Details**.

- Show or hide columns about the device image. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a device image. Click the Search icon in the top right corner of the page to search for a device image.

Field Descriptions

Table 56 on page 206 shows the fields on the Images page.

Table 56: Fields on the Device 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
Size	View the size of the device image.  Example: 14 KB

RELATED DOCUMENTATION

| [Device Images Overview](#) | 205

Deleting Device Images

You can delete one or more device images from the Device 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 delete icon (X).

The Confirm Delete page appears.

3. Click **Yes** to confirm.

**The Delete Success messages is displayed.**

The device image is deleted.

#### RELATED DOCUMENTATION

| [About the Device Images Page](#) | 205

# Managing Resources

## IN THIS CHAPTER

- Multidepartment CPE Device Support | 209
- About the Devices Page | 210
- Perform Return Material Authorization (RMA) for a Single-CPE Device | 213
- Performing Return Material Authorization (RMA) for Dual-CPE Devices | 215
- Granting RMA for a Device | 220
- Managing a Single CPE Device | 226
- Rebooting a CPE Device | 229
- Configuring APN Settings on CPE Devices | 230
- Identifying Connectivity Issues by Using Ping | 233
- Identifying Connectivity Issues by Using Traceroute | 237
- Remotely Accessing a Device CLI | 239
- Configuring the Firewall Device | 240
- About the Physical Interfaces Page | 242
- About the Logical Interfaces Page | 243
- Adding a Logical Interface | 244
- Editing, Deleting, and Deploying Logical Interfaces | 247
- Adding a Security Zone | 248
- Adding a Routing Instance | 251
- About the Static Routes Page | 252
- Adding a Static Route | 253
- Editing, Deleting, and Deploying Static Routes | 256

## 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 | 670](#)

[Viewing the SLA Performance of a Site | 673](#)

## About the Devices Page

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

You can use the Devices page to view the list of available CPE devices at the customer premises. 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 57 on page 211](#).
- Manage a single CPE. See [“Managing a Single CPE Device” on page 226](#).
- Reboot a CPE device. See [“Rebooting a CPE Device” on page 229](#).
- Push licenses to devices. Select the devices and click **Push License**.

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

For information on pushing licenses to devices, see *Pushing a License to Devices*.

- Perform Return Material Authorization (RMA) to replace a device that is faulty or not reachable. You can perform RMA for a single-CPE or a dual-CPE device.
  - For information on performing RMA on devices, see [“Perform Return Material Authorization \(RMA\) for a Single-CPE Device” on page 213](#)
  - For information on performing RMA on dual-CPE devices, see [“Performing Return Material Authorization \(RMA\) for Dual-CPE Devices” on page 215](#)
- View details about a CPE . Click the details icon that appears when you hover over the row for a device or click **More > Details**.
- Show or hide columns about the CPE. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Filter and sort CPE devices. Click a column name to sort the CPE devices based on the column name. Click the filter icon and select whether you want to show or hide column filters or apply a quick filter.

**NOTE:** Sorting and filtering is applicable only to some fields.

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



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

The search results are displayed on the same page.

## Field Descriptions

- [Table 57 on page 211](#) describes widgets on the Devices page.
- [Table 58 on page 211](#) describes the fields on the Devices page.

**Table 57: Widgets on the Devices Page**

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

**Table 58: Fields on the Devices Page**

Field	Description
Device Name	<p>Displays the name of the device.</p> <p>Example: sunny-NFX-250</p>
Tenant	<p>Displays the name of the tenant.</p> <p>Example: tenant-blue</p>
Site Name	<p>Displays the name of the tenant site.</p> <p>Example: site-blue-white</p>

Table 58: Fields on the Devices Page *(continued)*

Field	Description
Management Status	<p>Displays the management status of the CPE devices deployed in the cloud.</p> <ul style="list-style-type: none"> <li>• EXPECTED—Regional server has the activation details for the CPE device, but CPE device has not yet established a connection with the server.</li> <li>• DEVICE DETECTED—Device is configured and is reachable by CSO. After the user enters the activation code for the device, the activation code is validated and device is authenticated.</li> <li>• RMA—CPE device has been tagged for RMA as a result of the user applying the <b>Initiate RMA</b> action on the device.</li> <li>• ACTIVE—ZTP is initiated, CPE device has downloaded images, but not yet configured, and stage-1 configuration is pushed to the device.</li> <li>• PROVISIONED—ZTP is complete, and IPsec tunnel is established and operational on the device.</li> <li>• PROVISION_FAILED—Multiple factors lead to failure in provisioning a device. If any of the steps in ZTP fails or if any process fails as a part of device activation, then provision fails. For example, CPE device provisioning fails when the vSRX is not instantiated properly.</li> </ul>
Model	<p>Displays the name of the device model.</p> <p>Example: NFX</p>
Active Services	<p>Displays the number of services that are activated for the device.</p> <p>Example: 3</p>
Operational Status	<p>Displays whether the device is up or down.</p>
Location	<p>Displays the name of the location.</p> <p>Example: San Jose, CA</p>
Status Message	<p>Displays the latest status message.</p> <p>Example: IPsec provision success</p>
WAN Links	<p>Displays the number of WAN links.</p> <p>Example: 2</p>

Table 58: Fields on the Devices Page *(continued)*

Field	Description
POP Name	Displays the name of the POP.  Example: pop_blue
Image Name	Displays the name of the device image file.  Example: install_nfx_fmfm_agent_1_0.sh
OS Version	Displays the Junos OS Release version.  Example: 15.1X49-D40
Serial Number	Displays the serial number of the device.  Example: XXXXXXXXXXXXX
UUID	Displays the universally unique identifier (UUID) of the device.  Example: xxxxxxxx-xxxx-xxxx-xxx-xxxxxxxxxxxx

## RELATED DOCUMENTATION

| [Managing a Single CPE Device](#) | 226

## Perform Return Material Authorization (RMA) for a Single-CPE Device

Sometimes, due to hardware failure, a device managed by Contrail Service Orchestration (CSO) needs to be returned to the vendor for repair or replacement. In such situations, you perform Return Material Authorization (RMA) to back up the configuration of the faulty device, recall the faulty device and replace it with a new or restored device, push the required configuration to the replacement device, and activate it in order for CSO to recognize and manage the replacement device.

When you request RMA on a site that is associated with a single-CPE device and that has a version earlier than the CSO version, the site version is upgraded to the CSO version. The site version is upgraded as part of the device activation and zero touch provisioning (ZTP) process of the replacement device that is performed after RMA.

RMA can be initiated by an administrator with the RMA privilege.

To return a faulty device and replace it with a new or restored device using RMA:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

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

A confirmation page appears requesting for confirmation to go ahead with the initiate RMA process for the device. Click **Yes** to confirm RMA for the device.

Click **No** to cancel the process.

**NOTE:**

- The **Initiate RMA** option is enabled for a device only if the management status is **PROVISIONED**.
- On the Sites page (**Resources > Site Management**), the **Site Status** for the device for which you performed **Initiate RMA**, will remain **PROVISIONED**, however, you will see a red colored **RMA** tag beside the current status to indicate that RMA has been initiated for this device.

If you click **Yes**, the RMA process is initiated for the selected device. The management status of the device changes to **RMA**. Once you put a device in the RMA state, you have to start the process for getting the new replacement device (referred to as the new device). This process must be performed outside of CSO.

3. After you receive the new device, provide the details of the new device by clicking **More > Grant RMA**. See [“Granting RMA for a Device” on page 220](#).

**NOTE:** The **Grant RMA** option is enabled only if the management status is **RMA**.

4. Activate the new device by selecting the device and clicking **Activate Device**. Enter the **Activation Code** of the device to activate the device for usage.

When the device is activated, its **Management Status** changes to **PROVISIONED**. For a CPE device, an **RMA** tag is also displayed beside the management status indicating that the RMA process is not yet complete. Hover over the RMA tag to see the additional steps that you need to perform to complete the RMA process.

5. Manually push the following configuration to the newly provisioned device:

**NOTE:**

- In SD-WAN deployments, once the new device is in the **PROVISIONED** state, you can proceed to configure the device by manually pushing application signatures, certificates, and policies.
  - In hybrid WAN deployments, service chains are restored automatically.
- Licenses—If the new device is a physical SRX device, you must generate a new license and upload it to CSO.
  - Application Signatures—Push the application signatures to the new device. See [“About the Application Signatures Page” on page 589](#).
  - Certificates—Import and install the required certificates on the new device. See [“Importing a Certificate” on page 268](#) and [“Installing and Uninstalling Certificates” on page 270](#).
  - Policies—Push the defined firewall and NAT policies to the new device. See [“About the Firewall Policy Page” on page 287](#) and [“About the NAT Policies Page” on page 460](#).

For a CPE device, to complete the RMA process, you have to remove the RMA tag manually. To remove the RMA tag, hover over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

## RELATED DOCUMENTATION

[About the Devices Page | 210](#)

[Granting RMA for a Device | 220](#)

## Performing Return Material Authorization (RMA) for Dual-CPE Devices

## IN THIS SECTION

- [Performing RMA for an NFX Cluster | 216](#)
- [Performing RMA for an SRX Cluster | 218](#)

You can perform RMA of devices in an NFX or SRX cluster when the devices fail or need to be replaced with new devices. During the RMA process, the configuration of a faulty device is backed up and the faulty

device is shipped back to Juniper Networks. Juniper Networks ships a new device to the customer for replacing the faulty device. At the customer site, the new device is installed, the configuration backed up from the faulty device is pushed to the new device, and the new device is activated. CSO then manages the new device.

**NOTE:** On a site associated with an NFX dual-CPE device, if the site version is lower than that of the CSO version, you can perform RMA only at the cluster level. After RMA of the cluster, the version of the site is upgraded to that of CSO as part of the device activation and ZTP process of the replacement devices in the cluster.

The following sections discuss how you can perform RMA for an NFX or SRX cluster:

### Performing RMA for an NFX Cluster

Starting from CSO Release 4.1.0 onward, when an NFX250 device in a dual CPE cluster fails, you can perform RMA for only the failed device. Previously, RMA had to be done for both the devices in the cluster.

To perform RMA for an NFX cluster:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

a. Select **Resources > Site Management**.

The **Sites** page appears.

b. Click a site that contains the NFX cluster for which you want to perform RMA.

The *site* page appears

c. On the *site* page, click the **Devices** tab to view the devices and clusters installed at the site.

2. Do one of the following:

- To perform RMA at the cluster level, select the cluster.
- To perform RMA for a single device in the cluster, select the device.

A confirmation dialog box appears. Click **Yes** to confirm RMA for the selected NFX cluster or device.

Click **No** to cancel the process.

If you click **Yes**, the RMA process is initiated for the selected NFX cluster or device. The **Management Status** of the device changes to **RMA**.

**NOTE:**

- The **Initiate RMA** option is enabled for an NFX cluster only if the management status is **PROVISIONED**.
- On the Sites page (**Resources > Site Management**), the status of the site, where the NFX cluster or the device for which you initiated RMA is installed, remains as **PROVISIONED**. However, a red-colored **RMA** tag appears beside the **Site Status** to indicate that RMA is initiated for a cluster or device at the site.

After the NFX cluster or device is in the **RMA** state, you can raise a device replacement request for one or more faulty devices in the NFX cluster. This action is performed outside of CSO.

3. After you receive the new devices or device, click **More > Grant RMA** to enter the details of the new devices or device. See [“Granting RMA for a Device” on page 220](#).

**NOTE:** The **Grant RMA** option is enabled only when the management status of the device is RMA.

4. To activate the devices in the NFX cluster, do one of the following:
  - To activate both the devices in the cluster, select the cluster (in case of whole cluster is RMAed).
  - To activate a single device in the cluster, select the device (in case of a single device is RMAed).

5. Click **Activate Device**.

The Activate Device page appears.

6. Enter the **Activation Code** for the new device or devices.

When the device is activated, its **Management Status** changes to **PROVISIONED**. An **RMA** tag is displayed beside the management status indicating that the RMA process is not yet complete. Mouse over the RMA tag to see the additional steps that you need to perform to complete the RMA process.

7. Manually push the following configuration to the newly provisioned devices:

**NOTE:**

- In SD-WAN deployments, once the new devices are in the **PROVISIONED** state, you can proceed to configure the devices by manually pushing application signatures, certificates, and policies.
- In hybrid WAN deployments, service chains are restored automatically.
- When you perform RMA on a single device, CSO restores certificates on the new device. However, application signatures and policies need to be pushed manually.

- **Application Signatures**—Push the application signatures to the replaced device. See [“About the Application Signatures Page” on page 589](#).
- **Certificates**—Import and install the required certificates on the replaced devices. See [“Importing a Certificate” on page 268](#) and [“Installing and Uninstalling Certificates” on page 270](#).
- **Policies**—Push the defined firewall and NAT policies to the replaced devices. See [“About the Firewall Policy Page” on page 287](#) and [“About the NAT Policies Page” on page 460](#).

To complete the RMA process, you have to remove the RMA tag manually. To remove the RMA tag, mouse over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

### Performing RMA for an SRX Cluster

For an SRX cluster, you can perform RMA on a member device of the cluster. That is, you can select the faulty device from the SRX cluster and perform RMA on it individually.

**NOTE:** You cannot perform RMA for an SRX cluster at the cluster level.

To return a faulty device in an SRX cluster and replace it with a new or restored device by using RMA:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The **Sites** page appears.

- b. Click a site that contains the SRX cluster for which you want to perform RMA.

The *site* page appears



c. On the *site* page, click the **Devices** tab to view the devices and clusters installed at the site.

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

A confirmation page appears. Click **Yes** to confirm RMA for device.

Click **No** to cancel the process.

**NOTE:**

- The **Initiate RMA** option is enabled for a device only if the management status is **PROVISIONED**.
- On the Sites page (**Resources > Site Management**), the status of the site, where the device for which you performed **Initiate RMA** is installed, remains as **PROVISIONED**. However, a red-colored **RMA** tag appears beside the current site status to indicate that RMA is initiated for a cluster or device at the site.

If you click **Yes**, the RMA process is initiated for the selected device. The management status of the device changes to **RMA**. Once you put a device in the RMA state, you can raise a device replacement request for the faulty device in the SRX cluster. This action is performed outside of CSO.

3. After you receive the replacement of the faulty device, provide the details of the replacement device by clicking **More > Grant RMA**. See [“Granting RMA for a Device” on page 220](#).

**NOTE:** The **Grant RMA** option is enabled for a device only if the management status is **RMA**.

To complete the RMA process, you have to remove the RMA tag manually. To remove the RMA tag, mouse over the **PROVISIONED (RMA)** tag, select the check box indicating that you have completed all the steps for RMA, and click **OK**.

## RELATED DOCUMENTATION

[About the Devices Page | 210](#)

[Perform Return Material Authorization \(RMA\) for a Single-CPE Device | 213](#)

[Granting RMA for a Device | 220](#)

## Granting RMA for a Device

### IN THIS SECTION

- [Grant RMA for a Single-CPE Device | 220](#)
- [Grant RMA for a Dual-CPE Device | 222](#)
- [Grant RMA for an SRX Device within an SRX Cluster | 224](#)

To grant RMA for a device, you must specify the information such as serial number, about the new device that is received as a replacement for a faulty device. Grant RMA can be performed by an administrator with the RMA privilege.

### Grant RMA for a Single-CPE Device

Before you grant RMA for a device, ensure that:

- You have received a new device for replacing the faulty device.
- You have the serial number and the activation code for the new replacement device (referred to as new device).

To grant RMA for a device:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The **Sites** page appears.

- b. Click a site that contains the single-CPE device for which you want to perform RMA.

The *site* page appears

- c. On the *site* page, click the **Devices** tab to view the devices and clusters installed at the site.

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

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

**NOTE:** The **Grant RMA** option is enabled only when the **Management Status** of the device is **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 59 on page 221](#).
4. Click **OK** to perform the grant RMA process.

When you perform **Grant RMA** for a device, a job is created to perform the following tasks:

- The device-related configuration is backed up to the CSO database, and the existing device is recalled and the new device is added to the network.
- The management status of the device changes to **EXPECTED** on the **Devices** page. An **RMA** tag is also displayed beside the management status to indicate that the RMA process is not yet complete. Mouse over the RMA tag to see additional steps that you need to perform for completing the RMA process.

On the Sites page (**Resources > Site Management**), the status of the site, where the device for which you performed **Grant RMA** is installed, changes to **Expected**.

**NOTE:** You can see the progress of this job on the **Monitor > Jobs** page. This job might take around 15 minutes to complete.

To complete the RMA process and start using the new device, you must activate the device using the **Activate Device** option. See step 5 in [“Perform Return Material Authorization \(RMA\) for a Single-CPE Device” on page 213](#).

[Table 59 on page 221](#) provides guidelines on using the fields on the **Grant RMA for Device** panel.

**Table 59: Fields on the Grant RMA for Single-CPE Device Page**

Field	Description
Customer Name	Displays the name of the tenant who is performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with a new one through the <b>Grant RMA</b> process.
Serial Number	Enter the serial number of the new device. The serial number is case sensitive. Example: DD2316AF0177

Table 59: Fields on the Grant RMA for Single-CPE Device Page (*continued*)

Field	Description
Activation Code	Enter the activation code for the new device. You receive the activation code (Example: 545454) from the service provider, outside of CSO.

## Grant RMA for a Dual-CPE Device

Before you perform **Grant RMA for a Device**, ensure that:

- You have received the replacement for the faulty devices.
- You have the serial numbers and the activation codes of the new devices.

To perform **Grant RMA** for a dual-CPE device(cluster):

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click a site that contains the dual-CPE device for which you want to perform RMA.

The *site* page appears

- c. On the *site* page, click the **Devices** tab to view the devices and clusters installed at the site.

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

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

**NOTE:** The **Grant RMA** option is only enabled if the **Management Status** of the device is **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 60 on page 223](#).
4. Click **OK** to complete the grant RMA process.

When you grant RMA, the following actions are performed:

- The cluster-related configuration is backed-up to the CSO database, and the devices in the cluster are recalled and the new or restored devices are added to the network.
- The management status of the cluster changes to **EXPECTED** on the **Devices** page. An **RMA** tag is also displayed beside the management status indicating that the RMA process is not yet complete. Mouse over the RMA tag to see the additional steps that you must perform to complete the RMA process.

On the Sites page (**Resources > Site Management**), the status of the site, where the cluster or device for which you performed **Grant RMA** is installed, changes to **Expected**.

**NOTE:** You can see the progress of this job on the **Monitor > Jobs** page. This job might take around 15 minutes to complete.

Table 60 on page 223 provides guidelines on using the fields on the **Grant RMA for Device** panel.

**Table 60: Fields on the Grant RMA for Dual-CPE Device Page**

Field	Description
Customer Name	Displays the name of the tenant performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with new or restored devices through the <b>Grant RMA</b> process.
Primary Serial Number	Enter the serial number of the new primary device. The serial number is case sensitive. Example: DD2316AF0177
Primary Activation Code	Enter the activation code for the new primary device. You will receive the activation code from the service provider, outside of CSO. Example: 545454
Secondary Serial Number	Enter the serial number of the new secondary device. The serial number is case sensitive. Example: DD2316AF0145
Secondary Activation Code	Enter the activation code for the new secondary device. You receive the activation code from your service provider, outside of CSO. Example: 545476

## Grant RMA for an SRX Device within an SRX Cluster

Before you perform **Grant RMA for a Device**, ensure that:

- You have received the replacement for the faulty device.
- You have the serial number and the activation code of the new device.

To perform **Grant RMA** for a device:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

Alternatively,

- a. Select **Resources > Site Management**.

The Sites page appears.

- b. Click a site that contains the SRX device for which you want to perform RMA.

The *site* page appears

- c. On the *site* page, click the **Devices** tab to view the devices and clusters installed at the site.

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

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

**NOTE:** The **Grant RMA** option is enabled only when the **Management Status** of the device is **RMA**.

3. Complete the configuration according to the guidelines provided in [Table 61 on page 225](#).

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

When you perform **Grant RMA** for a device, a job is created to update the device object in CSO with the serial number and activation code of the new device.

On the Sites page (**Resources > Site Management**), the status of the site, where the device for which you performed **Grant RMA** is installed, changes to **PROVISIONED**.

**NOTE:** You can see the progress of this job on the **Monitor > Jobs** page.

[Table 61 on page 225](#) provides guidelines on using the fields on the **Grant RMA for Device** page.

**Table 61: Fields on the Grant RMA for Device Page (for SRX Device in an SRX Cluster)**

Field	Description
Customer Name	Displays the name of the tenant who is performing RMA.
Site Name	Displays the name of site in which the faulty device is present.
Device Name	Displays the name of the faulty device that will be replaced with a new one through the <b>Grant RMA</b> process.
Serial Number	Enter the serial number of the new device. The serial number is case sensitive. Example: DD2316AF0177
Activation Code	Enter the activation code for the new device. You receive the activation code (Example: 545454) from the service provider, outside of CSO.

## RELATED DOCUMENTATION

[About the Devices Page | 210](#)

[Perform Return Material Authorization \(RMA\) for a Single-CPE Device | 213](#)

[Performing Return Material Authorization \(RMA\) for Dual-CPE Devices | 215](#)

## Managing a Single CPE Device

You can use the 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**.

To manage a single CPE device at the tenant site:

1. Click **Overview** tab.

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.
- Recent Alarms for the device.
- License details of the device.
- Details of the device, such as serial number, management IP address, OS version, device template, tenant name, site name, and site location.

2. Click **Policies** tab.

View the following information on the Policies tab:

- List of all policies applicable to a CPE device.
  - Click a policy name to view the rules that are applicable for the CPE device.
  - Click the edit icon at the end of the row to edit a policy. You are taken to the **Configuration > Policy** page, where you can edit the policies.
- Details about the tenant user who last updated the policy.
- Time when the policy was last updated.
- Deployment status of the policy.
- Number of rules applicable to the device compared to the total number of rules applicable to the tenant.

3. Click **Configuration Template** tab.

**NOTE:** The **Configuration** tab that was available in earlier releases for stage-2 template-based configuration is renamed as **Configuration Template**.

Complete the configuration according to the guidelines provided in [Table 62 on page 227](#), [Table 63 on page 227](#), and [Table 64 on page 228](#).



You can also perform the following operations from this page.

- Click **Deploy** to deploy the configuration.
- Click **Rollback** to rollback to previous working configuration.
- Click **Deployment History** to view the deployment history.
- Click **View Changes** to view the changes between current and previous configuration.
- Click **Render Template** to render the configuration in CLI format.
- Click **Save** to save the changes.

4. Click **Configuration** tab (applicable for firewall devices).

You can perform the following operations from this page.

- Click **Physical Interfaces** tab to view and manage the physical interfaces for the device.
- Click **Security Zone** tab to view and manage the security zones for the device.
- Click **Routing Instance** tab to view and manage the routing instances for the device.

For information about managing an EX Series switch, see [“Managing an EX Series Switch” on page 186](#).

**Table 62: Fields on the SRX Root Password Tab**

Field	Description
<b>Edit Settings for SRX root password</b>	
Password	Enter your new password.  The 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.
Confirm Password	Reenter the password for confirmation.

**Table 63: Fields on the NFX Root Password Tab**

Field	Description
<b>Edit Settings for NFX root password</b>	
Password	Enter your new password.  The 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.
Confirm Password	Reenter the password for confirmation.

Table 64: Fields on the APN Configuration Tab

Field	Description
<b>Edit Settings for APN Configuration</b>	
Use default APN settings	<p>Click the toggle button to change the default APN settings.</p> <ul style="list-style-type: none"> <li>• Enabled(Default)—Select this option to use the default APN setting that is shipped along with the CPE device.</li> <li>• Disabled—Select this option to configure the APN settings.</li> </ul>
<b>APN Settings</b>	
APN Name	Enter the access point name (APN) of the gateway router. The name can contain alphanumeric characters and special characters.
SIM Change Required	<p>Click the toggle button to change the SIM card.</p> <ul style="list-style-type: none"> <li>• Enabled(Default)—Select this option to change the APN settings and to use a new SIM card.</li> <li>• Disabled—Select this option to change the APN settings without changing the SIM card.</li> </ul>
Authentication Method	<p>Select the authentication method for the APN configuration.</p> <ul style="list-style-type: none"> <li>• PAP— Select to use Password Authentication Protocol (PAP) authentication. This is the default option.</li> <li>• CHAP— Select to use Challenge Handshake Authentication Protocol (CHAP) authentication.</li> <li>• None—Select to indicate that there is no authentication method.</li> </ul>
<b>Authentication Info</b>	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication if you have selected the APN authentication method as either <b>PAP</b> or <b>CHAP</b> .
SIP Password	Enter the SIP password for authentication if you have selected the APN authentication method as either <b>PAP</b> or <b>CHAP</b> .

## RELATED DOCUMENTATION

[About the Devices Page](#) | 210

## Rebooting a CPE Device

You need to reboot a CPE device if the device is down, or if all troubleshooting options fail.

To reboot a CPE device:

1. Select **Resources > Devices**.
2. Select the CPE 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.

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 Devices Page](#) | 210

## Configuring APN Settings on CPE Devices

### IN THIS SECTION

- [Configuring APN Settings with SIM Change on CPE Devices | 230](#)
- [Configuring APN Settings without SIM Change on CPE Devices | 232](#)

You can configure Access Point Name (APN) settings on the following devices, with or without SIM change. You can change the APN settings either to use a private APN with the current LTE service provider or to use a different LTE service provider.

**NOTE:** You can only insert a SIM card in the SIM1 slot of the LTE Mini-Physical Interface Module (Mini-PIM).

Following is the list of devices on which you can configure APN settings:

- NFX Series—NFX150 and NFX250 CPE devices
- SRX Series—SRX320, SRX340, and SRX345 CPE devices

### Configuring APN Settings with SIM Change on CPE Devices

To configure APN settings with SIM change:

1. Select **Resources > Devices**.

The *Devices* page appears.

2. Click the device that you want to configure.

The *Device-Name* page appears.

3. Click the **Configuration Template** tab and change the APN settings according to the guidelines provided in [Table 65 on page 231](#).

4. Click **Save**.

The new settings are applied after one minute.

5. Remove the USB dongle from the CPE device, change the SIM card, and re-insert the USB dongle.

The system checks for the new APN settings every minute.

- If the applied APN settings are compatible with the new SIM card—The LTE WAN link and its tunnels go down after one minute and remain down till the new SIM card is inserted. The LTE dongle LED indicates that the connection is down during this period. Maximum one minute after the new SIM is inserted, the LTE dongle LED indicates that the connection is up. The LTE WAN link and its tunnels come up automatically.
- If the applied APN settings are not compatible with the new SIM card—The LTE WAN link and its tunnels go down after one minute and remain down even after the new SIM card is inserted. The LTE dongle LED indicates that the connection is down even after the new SIM is inserted.

6. To revert to the old SIM, remove the USB dongle, replace the current SIM with the previous SIM, and re-insert the dongle.

The system checks for the new APN settings every minute. Maximum one minute after the old SIM is inserted, the LTE dongle LED indicates that the connection is up (using the old SIM and old APN). The LTE WAN link and its tunnels come up automatically

**Table 65: Fields for the APN Configuration Settings on the Configuration Template Tab**

Field	Description
<b>Edit Settings for APN Configuration</b>	
Use default APN settings	<p>Click the toggle button to enable (default) or disable the default APN settings.</p> <ul style="list-style-type: none"> <li>• If you enable this option, the default APN settings that are shipped along with the CPE device are used for configuring the APN.</li> <li>• If you disable this option, you must configure the APN settings manually.</li> </ul>
<b>APN Settings</b>	
APN Name	Enter the access point name (APN) of the gateway router.
SIM Change Required	<p>Click the toggle button to enable or disable changing the SIM card:</p> <p><b>NOTE:</b> You can change the SIM card either to use a different LTE service provider or to use a private APN with the current LTE service provider.</p> <ul style="list-style-type: none"> <li>• (Default) Enable this option to change the APN settings and to use a new SIM card.</li> <li>• Disable this option to change the APN settings without changing the SIM card.</li> </ul>

Table 65: Fields for the APN Configuration Settings on the Configuration Template Tab (*continued*)

Field	Description
Authentication Method	<p>From the list, select one of the following authentication methods for the APN configuration as configured by the service provider:</p> <ul style="list-style-type: none"> <li>• (Default) PAP—Select this option to use Password Authentication Protocol (PAP) as the authentication method.</li> <li>• CHAP—Select this option to use Challenge Handshake Authentication Protocol (CHAP) authentication as the authentication method.</li> <li>• None—Select this option if you do not want to use any authentication method.</li> </ul>
<b>Authentication Information</b>	
SIP User ID	Enter the Session Initiation Protocol (SIP) user ID for authentication.
SIP Password	Enter the SIP password for authentication.

## Configuring APN Settings without SIM Change on CPE Devices

To configure APN settings without SIM change:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device that you want to configure.

The *Device-Name* page appears.

3. Click the **Configuration Template** tab and change the APN settings according to the guidelines provided in [Table 65 on page 231](#).

4. Click **Save**.

The new settings will be applied after one minute.

- If the applied APN settings are valid—In CSO, the LTE WAN link and its associated tunnels go down momentarily and then, get re-established automatically.
- If the applied APN settings are invalid—After one minute, the LTE dongle LED indicates that the connection is down. In CSO, the LTE WAN link and its associated tunnels go down.

After two minutes, the LTE dongle LED indicates that the connection is up (using old APN). In CSO, the LTE WAN link and its tunnels come up automatically.

## RELATED DOCUMENTATION

[About the Devices Page](#) | 210

## Identifying Connectivity Issues by Using Ping

You can use Contrail Service Orchestration (CSO) to perform a ping operation from a device (provider hub, tenant device, CPE device, EX switch, enterprise hubs, or next-generation firewall device) to a remote host for identifying issues in connectivity with the remote host.

When you ping a remote host from a device, an Internet Control Message Protocol (ICMP) packet is sent to the remote host. By analyzing the results of the ping operation, you can identify the possible device connectivity issues between the remote host and the device.

**NOTE:** In Contrail Service Orchestration (CSO) Release 5.0, the following devices support ping:

- EX Series: EX2300, EX3400, and EX4300
- MX Series
- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform the ping operation:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list of devices displayed and click **More > Ping**.

The Ping page appears.

**NOTE:** You can ping from a device only when its operational status is Up in CSO.

3. Complete the configuration according to the guidelines provided in [Table 66 on page 234](#).

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

4. Click **Ping** to initiate the ping request.

A job is created and the Ping Progress page appears. After the device sends the ping packets, the Ping Result page appears. . If the ping operation is successful, the Ping Result page displays the parameters specified in [Table 67 on page 236](#).

If the ping operation fails, the Ping Result page displays an appropriate error message (such as **No response** or **No route to host**), indicating that there is an issue in the connectivity to the remote host.

Table 66: Fields on the Ping page

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.
Ping Request Packets	Enter the number of ping request packets to be sent to the remote host.  Default: 5.  Range: 1 through 300.
<b>Advanced</b>	
Source Interface	Select the source interface on the device through which you want to send the ping request to the remote host. If you do not select a source interface, ping requests are sent on all interfaces.  To clear the selected interface, click <b>Clear All</b> and select another interface.
Hostname Resolution	Click the toggle button to enable or disable (default) the display of hostname of the hops along the path to the remote host.



Table 66: Fields on the Ping page (*continued*)

Field	Description
Rapid Ping	<p>Click the toggle button to enable or disable (default) sending ping requests rapidly.</p> <p>If you enable this option, the source device sends a minimum of 100 ping request packets per second or sends a packet as soon as a response to the previous packet is received, whichever is greater.</p> <ul style="list-style-type: none"> <li>• If the source device does not receive a response for 500 ms, timeout is considered.</li> <li>• If the source device receives a response within 500 ms, the next ping request packet is sent immediately.</li> </ul> <p><b>NOTE:</b> The ping results are displayed in a single consolidated message instead of individual messages for each ping request packet sent.</p>
Packet Fragmentation	<p>Click the toggle button to enable or disable (default) the fragmenting of ping request packets.</p> <p>If packet fragmentation is disabled, ping packets with the maximum transmission unit (MTU) greater than 1500 bytes are dropped.</p>
Packet Size (bytes)	<p>Enter the size (in bytes) of the ping request packet.</p> <p>Default: 56 bytes.</p> <p>Range:</p> <ul style="list-style-type: none"> <li>• 1 through 1,472 bytes, if packet fragmentation is disabled.</li> <li>• 1 through 65,468 bytes, if packet fragmentation is enabled.</li> </ul>
Wait Time (seconds)	<p>Enter the time (in seconds) for which the source device waits for a response to the ping request packet. The source device considers the remote host as not reachable after the wait time elapses.</p> <p>Default: 10 seconds.</p> <p>Range: 0 through 600 seconds.</p>
Incoming Interface	<p>Click the toggle button to include or exclude (default) information (on the Ping Result page) about the interface on the source device that receives the ping responses..</p>

Table 66: Fields on the Ping page (*continued*)

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

Table 67: Fields on the Ping Result page

Field	Description
Packet Loss	Displays the percentage of ping packets sent for which the source device did not receive a response.
Round Trip Time Taken (in $\mu$ s)	<p>Displays the following information about the duration (in microseconds) between the time when the source device sends the ping request and the time when the source device receives a response from the remote host.</p> <p>Displays the following:</p> <ul style="list-style-type: none"> <li>• Minimum: The minimum time taken to receive a response for a ping request packet.</li> <li>• Maximum: The maximum time taken to receive a response for a ping request packet.</li> <li>• Average: The average time taken to receive a response for all the ping request packets sent in a ping operation.</li> <li>• Standard Deviation: The variation of the round trip time from the mean round trip time.</li> </ul>

**Details**

Sequence	Sequence number of all the ping request packets.
Result	Result of the ping request packets—Success or Failure.
Incoming Interface	<p>Interface on the source device on which the responses are received for the ping requests.</p> <p>This data appears if you have enabled the Incoming Interface option on the Ping page.</p>
Time Taken	Time taken (in microseconds) to receive response to a ping request packet.

# Identifying Connectivity Issues by Using Traceroute

You can use Contrail Service Orchestration (CSO) to perform a traceroute operation from a device (provider hub, tenant device, CPE device, EX switch, enterprise hubs, or next-generation firewall device) to the remote host. Traceroute helps you view the path that a packet travels to reach the remote host. The result is useful in identifying the point of network failure in the path between the source device and remote host.

**NOTE:** In Contrail Service Orchestration (CSO) Release 5.0, the following devices support traceroute:

- EX Series: EX2300, EX3400, and EX4300
- MX Series
- NFX Series: NFX150, NFX250
- SRX Series: SRX300, SRX320, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600
- vSRX

To perform traceroute operation:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the list of devices displayed and Click **More > Traceroute**.

The Traceroute page appears.

3. Complete the configuration according to the guidelines provided in [Table 68 on page 237](#).

Fields marked with an asterisk (\*) are mandatory.

4. Click **Traceroute** to initiate the traceroute operation.

A job is created and a Traceroute Progress page appears. If the traceroute operation is successful, the Traceroute Result page displays the traceroute parameters specified in [Table 69 on page 238](#).

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

**Table 68: Fields on the Traceroute page**

Field	Description
Remote Host	Enter the IPv4 address or hostname of the remote host.

Table 68: Fields on the Traceroute page (*continued*)

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

Table 69 on page 238 lists the parameters on the Traceroute Result page when the traceroute operation is successful.

Table 69: Fields on the Traceroute Result page

Field	Description
Hop	<p>Hostname or IPv4 address of the network devices that the packet passed through to reach the remote host.</p>

Table 69: Fields on the Traceroute Result page (*continued*)

Field	Description
Time Taken by Packet 1	Duration (in microseconds) between the time from when the source device sends a packet, and the time it received a response from the hops and the remote host.
Time Taken by Packet 2	
Time Taken by Packet 3	

## Remotely Accessing a Device CLI

You can use the Devices page to remotely access the CLI of CPE devices and EX Series switches, and run **show** operational commands.

You can use the **Show** operational commands to monitor a device, verify system operation, view details of specific components on a device, and so on.

To access the Devices page:

1. Select **Resources > Devices**.

The Devices page appears.

2. Select a device from the Devices List.

**NOTE:** You can only select a device whose operational status is marked **Up**.

3. Click **More**.

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

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

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

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

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

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

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

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

The Devices page appears.

**NOTE:** The session times out if the session remains idle for more than two minutes (default) and you are automatically logged out of the device. The **Remote console connection was closed. Please close this window and open the remote console again** message appears on the browser window.

## Configuring the Firewall Device

Zones, physical interfaces, and routing instances are the basic building blocks of firewall policy and NAT policy. You can configure them from the **Resources > Devices > Device-Name > Configuration** page.

**NOTE:** The **Configuration** tab that was available in earlier releases for stage-2 template-based configuration is renamed as **Configuration Template**.

To configure the firewall device:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The physical interfaces, routing instances, and zones tabs appear.

4. Complete the configuration settings according to the guidelines provided in [Table 70 on page 241](#).

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

The newly created physical interfaces, routing instances, and zones are displayed in the relevant tabs in the Configurations page.

**Table 70: Fields on the Device Configuration Page**

Field	Description
<b>Physical Interfaces</b>	
Interface Name	Name of the physical interface on the device.
Logical Interfaces	Click <b>View/Configure</b> to view or configure the logical interfaces associated with the physical interface on the device.  To view and add logical interfaces for a physical interface, see <a href="#">“About the Logical Interfaces Page” on page 243</a> and <a href="#">“Adding a Logical Interface” on page 244</a> .
<b>Zones</b>	
Name	Name of the zone that you use for firewall policies and NAT policies.  To add a new security zone, see <a href="#">“Adding a Security Zone” on page 248</a> .
Interfaces	Interfaces associated with the zone.
Screen	Screen name for the security zone.
Description	Description for the zone.

Table 70: Fields on the Device Configuration Page (*continued*)

Field	Description
<b>Routing Instances</b>	
Name	Name of the routing instances for security configuration. A routing instance is a collection of routing tables, interfaces, and routing protocol parameters.
Static Route	Click <b>View/Configure</b> to view or configure the static routes associated with a routing instance on the device.
Interfaces	Name of the interface over which the traffic flows.
Instance Type	Type of routing instance.
Description	Description of the routing instance.

## About the Physical Interfaces Page

To access this page, click **Resources > Devices > Device-Name > Configuration**.

Use this page to view or edit the physical interfaces on the device. You can also view and configure the logical interfaces associated with the physical interfaces.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the physical interfaces. Click the **View/Configure** button to view or configure the logical interfaces for the physical interface. See [“About the Logical Interfaces Page” on page 243](#).
- Show or hide columns about the physical interface. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a physical interface. Click the Search icon in the top right corner of the page to search for an interface.

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

The search results are displayed on the same page.



## Field Descriptions

Table 71 on page 243 shows the fields on the Physical Interface page.

Table 71: Fields on the Physical Interface Page

Field	Description
Interface Name	Name of the physical interface on the device.
Logical Interfaces	Click View/Configure to view or configure the logical interfaces associated with the physical interface on the device.  To view and add logical interface for a physical interface, see <a href="#">“About the Logical Interfaces Page” on page 243</a> and <a href="#">“Adding a Logical Interface” on page 244</a> .
MTU	Maximum transmission unit (MTU) size (in bytes) on the physical interface.
Speed	Speed in gigabytes per second (Gbps), at which data is transferred for the physical interface.
Description	Description of the physical interface.

## About the Logical Interfaces Page

To access this page, click **Resources > Devices > *Device-Name* > Configuration > Physical Interfaces > View/Configure**.

Use this page to view, create, edit, or delete logical interfaces associated with a physical interface on the device.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the logical interfaces. See [Table 72 on page 244](#) for descriptions of the fields on the logical interfaces page.
- Add a logical Interface. See [“Adding a Logical Interface” on page 244](#).
- Edit, delete, or deploy logical interfaces. See [“Editing, Deleting, and Deploying Logical Interfaces” on page 247](#).

- Clear all selected logical interfaces. Select the logical interface and then right-click or click **More > Clear All Selections**.
- Show or hide columns that contain information about the logical interface. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for logical interfaces 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 72 on page 244 shows the fields on the Logical Interfaces page.

Table 72: Fields on the Logical Interfaces Page

Field	Description
Interface Name	Displays the name of the logical interface associated with a physical interface on the device.
IPv4 Address	Displays the IPv4 address for the logical interface..
IPv6 Address	Displays the IPv6 address for the logical interface.
VLAN ID	Displays the VLAN ID for the 802.1q VLAN tags.
Description	Displays the description of the logical interface.

## Adding a Logical Interface

For a physical interface to function, you must configure at least one logical interface on that device. . You can also configure other logical interface properties.

The logical properties of an interface are the characteristics that do not apply to the physical interface. Logical properties include:

- IP address or addresses associated with the interface. A logical interface can be configured with an IPv6 address, IPv4 address, or both. The IP specification requires a unique address on every interface of each system attached to an IP network, so that traffic can be correctly routed. Individual hosts such as home computers must have a single IP address assigned. Devices must have a unique IP address for every interface.
- Virtual LAN (VLAN) tagging

To create logical interface for a physical interface:

1. Select **Resources > Devices** .

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Physical Interfaces** tab.

The Physical Interfaces page appears.

5. Select a physical interface and click **View/Configure**.

The Logical Interfaces page appears.

6. Click the plus icon (+) .

The Create Logical Interface page appears.

7. Complete the configuration settings according to the guidelines provided in [Table 73 on page 245](#).

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

**Table 73: Fields on the Logical Interfaces Page**

Field	Description
<b>Basic Information</b>	
Unit	Enter the number of the logical interface.  Range: 0 through 2,147,483,647.
Description	Enter a description for the logical interface. The maximum number of characters is 255.
VLAN ID	Enter the VLAN ID for the 802.1q VLAN tags.
<b>IPv4 Address</b>	Click the plus icon (+) .  The Add - Address(IPv4) page appears.

Table 73: Fields on the Logical Interfaces Page (*continued*)

Field	Description
IPv4 Address	Enter an IPv4 address for the logical interface.
Subnet	Enter the subnet for the IPv4 address.  Range: 0 through 32
Primary	Select this check box to mark the IPv4 address as the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv4 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.
<b>IPv6 Address</b>	Click the plus icon (+) .  The Add - Address(IPv6) page appears.
IPv6 Address	Enter an IPv6 address for the logical interface.
Subnet	Enter the subnet for the IPv6 address.  Range: 0 through 32
Primary	Select this check box to specify that the IPv6 address is the primary address of the protocol on the logical interface. If the logical unit has more than one IP address, the primary IP address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.
Preferred	Select this check box to specify that the IPv6 address is the preferred address for the logical interface. If you configure more than one IP address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.

## Editing, Deleting, and Deploying Logical Interfaces

### IN THIS SECTION

- [Editing Logical Interfaces | 247](#)
- [Deleting Logical Interfaces | 248](#)
- [Deploying Logical Interfaces | 248](#)

You can edit, delete, and deploy logical interfaces from the **Logical Interfaces** page.

### Editing Logical Interfaces

To modify the parameters configured for a logical interface:

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.

The **Logical Interfaces** page appears.

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

The **Edit Logical Interface** page appears.

3. Modify the parameters according to the guidelines provided in [“Adding a Logical Interface” on page 244](#).

**NOTE:** You can modify only some fields when you are editing a logical interface.

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

If you click **OK**, the modified values appear on the **Logical Interfaces** page.

## Deleting Logical Interfaces

To delete a logical interface:

**NOTE:** You cannot delete a logical interfaces that is associated with a physical interface on the device.

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.  
The **Logical Interfaces** page appears.
2. Select one or more logical interfaces that you want to delete and then click the delete icon.  
A page requesting confirmation for the deletion appears.
3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected logical interface is deleted from the **Logical Interfaces** page.

## Deploying Logical Interfaces

To deploy a logical interface:

1. Select **Resources > Devices > Device-Name > Configuration > Physical Interface > View/Configure**.  
The **Logical Interfaces** page appears.
2. Select one or more logical interfaces that you want to deploy and then click **Deploy**.  
A job is created. Click the job link or go to the Jobs page and view the status of the deployment.

### RELATED DOCUMENTATION

| [Adding a Logical Interface](#) | 244

## Adding a Security Zone

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are

bound. You can define multiple security zones, the exact number of which you determine based on your network needs.

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone. Through the policies you define, you can permit traffic between zones to flow in one direction or in both. With the routes that you define, you specify the interfaces that traffic from one zone to another must use. Because you can bind multiple interfaces to a zone, the routes you chart are important for directing traffic to the interfaces of your choice. An interface can be configured with an IPv4 address, IPv6 address, or both.

Security zones have the following properties:

- **Policies**—Active security policies that enforce rules for the transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on the traffic as it passes through the firewall.
- **Screens**—A Juniper Networks stateful firewall secures a network by inspecting, and then allowing or denying, all connection attempts that require passage from one security zone to another. For every security zone, you can enable a set of predefined screen options that detect and block various kinds of traffic that the device determines as potentially harmful.
- **TCP-RST**—When this feature is enabled, the system sends a TCP segment with the RESET flag set when traffic arrives that does not match an existing session and does not have the SYNchronize flag set.
- **Interfaces**—List of interfaces in the zone.

Use this page to configure zones and assign interfaces to them.

To create a security zone:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Zones** tab.

The Zones page appears.

5. Click the plus icon (+).

The Add New Zone page appears.

6. Complete the configuration settings according to the guidelines provided in [Table 74 on page 250](#).
7. Click **OK** to save the changes.

**Table 74: Fields on the Add New Zone Page**

Field	Description
<b>General Information</b>	
Name	Enter a unique string of alphanumeric characters, and some special characters, such as dashes, and underscores. The maximum length is 31 characters.
Description	Enter a description for the zone; the maximum length is 900 characters.
Application Tracking	Select the checkbox to maintain application usage statistics on a device.
<b>Interfaces</b>	From the list of interfaces in the Available column, select the interfaces that you want to include in the new zone and click the greater-than icon (>). The selected interfaces are moved to the Selected column.
<b>System Services</b>	From the list of system services in the Available column, select the system services that you want to include in the new zone and click the greater-than icon (>). The selected system services are moved to the Selected column.
Is Except	Select the checkbox to disable specific incoming system service traffic, only when <b>all</b> system services option is defined.
<b>Protocols</b>	From the list of protocols in the Available column, select the protocols that you want to include in the new zone and click the greater-than icon (>). The selected protocols are moved to the Selected column.
Is Except	Select this option to disable specific incoming protocol traffic, only when <b>all</b> protocols option is defined.
<b>Traffic Control Options</b>	
TCP RST	Select the checkbox to enable sending TCP packets with the RST (reset) flag set to 1 in response to TCP packets with any flag other than SYN set and that do not belong to an existing session.
Screen	Enter a predefined security screen for a security zone to detect and block various kinds of traffic that the device determines as potentially harmful.



Table 74: Fields on the Add New Zone Page (*continued*)

Field	Description
<b>Interface Services and Protocols</b>	View the summary of interface, services and protocols for your device.

## Adding a Routing Instance

A routing instance is a collection of routing tables, interfaces, and routing protocol parameters. The set of interfaces belongs to the routing tables, and the routing protocol parameters control the information in the routing tables. There can be multiple routing tables for a single routing instance—for example, unicast IPv4, unicast IPv6, and multicast IPv4 routing tables can exist in a single routing instance. Routing protocol parameters and options control the information in the routing tables.

Each routing instance consists of sets of the following:

- Routing tables
- Interfaces that belong to these routing tables (optional, depending upon the routing instance type)
- Routing option configurations

You can configure the following routing instances:

- Forwarding—Use this routing instance type for filter-based forwarding applications. For this instance type, there is no one-to-one mapping between an interface and a routing instance. All interfaces belong to the default instance `inet.0`.
- Virtual router—Use this for non-VPN-related applications. There are no virtual routing and forwarding (VRF) import, VRF export, VRF target, or route distinguisher requirements for this instance type.

To create a routing instance:

1. Select **Resources > Devices**.

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

- Click **Routing Instances** tab.

The Routing Instances page appears.

- Click the plus icon (+).

The Create Routing Instance page appears.

- Complete the configuration settings according to the guidelines provided in [Table 75 on page 252](#).

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

**Table 75: Fields on the Create Routing Instance Page**

Field	Description
<b>General Settings</b>	
Name	Enter a unique string of alphanumeric characters, dashes, and underscores. The maximum length is 31 characters.
Description	Enter a description for the zone; the maximum length is 900 characters.
Instance Type	Select the routing instance type from the list. Select virtual-router for non-VPN-related application. Select forwarding for filter-based forwarding applications where interfaces are not associated with instances.
<b>Interfaces</b>	From the list of interfaces in the Available column, select the interfaces that you want to include in the new routing instance and click the greater-than icon (>). The selected interfaces are moved to the Selected column.

## About the Static Routes Page

To access this page, click **Resources > Devices > Device-Name > Configuration > Routing Instances > View/Configure**.

Use this page to view, create, edit, or delete static routes for the routing instance.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about the static route. See [Table 76 on page 253](#) for descriptions of the fields on the static routes page.
- Add a static route. See [“Adding a Static Route” on page 253](#).
- Edit, delete, or deploy static routes. See [“Editing, Deleting, and Deploying Static Routes” on page 256](#).
- Clear all selected static routes. Select the static route and then right-click or click **More > Clear All Selections**.
- Show or hide columns that contain information about the static route. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for static routes 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 76 on page 253](#) shows the fields on the Static Routes page.

**Table 76: Fields on the Static Routes Page**

Field	Description
IP Address	View the IP address of the static route.
Next Hop	View the Ipv4 or IPv6 address for the next hop.
Next Table	View the name of the next routing table to the destination.
Metric	View the metric value that signifies the cost for an access route, for the next hop
Status	View the status of the static route.

## Adding a Static Route

Routes that are permanent fixtures in the routing and forwarding tables are often configured as static routes. These routes generally do not change, and often include only one or very few paths to the destination.

To create a static route in the routing table, you must, at minimum, define the route as static and associate a next-hop address with it. The static route in the routing table is inserted into the forwarding table when

the next-hop address is reachable. All traffic destined for the static route is transmitted to the next-hop address for transit.

You can specify options that define additional information about static routes that is included with the route when it is installed in the routing table. All static options are optional.

To create a static route for a routing instance:

1. Select **Resources > Devices** .

The Devices page appears.

2. Click the device name that you want to configure.

The *Device-Name* page appears

3. Click the **Configuration** tab.

The Physical Interfaces, Routing Instances, and Zones tab appears.

4. Click **Routing Instances** tab.

The Routing Instances page appears.

5. Select a routing instance and click **View/Configure** link in the **Static Route** column.

The Static Routes page appears.

6. Click the plus icon (+) .

The Create Static Route page appears.

7. Complete the configuration settings according to the guidelines provided in [Table 77 on page 254](#).

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

**Table 77: Fields on the Create Static Route Page**

Field	Description
<b>Basic Information</b>	
IP Address	Enter the IPv4 or IPv6 address depending on the type of IP address specified.
Subnet	Enter the subnet for the IPv4 address or the prefix for the IPv6 address.
<b>Next Hop</b>	

Table 77: Fields on the Create Static Route Page (*continued*)

Field	Description
IP Address	Enter an IPv4 or IPv6 address for the next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the next hop.
<b>Qualified Next Hop</b>	
IP Address	Enter an IPv4 or IPv6 address for the qualified next hop depending on the type of IP address specified for the static route.
Interface	Select the interface name to be used as the qualified next hop.
Preference	Enter the preference for the qualified next hop; the lower the number, the higher the route preference.
Metric	Enter a metric value to signify the cost for an access route for the qualified next hop.
<b>Next Table</b>	
Next Table	Select the name of the next routing table to the destination.
<b>Advanced Options</b>	
Preference	Enter the preference for the next hop; the lower the number, the higher the route preference.  Range: 0 through 2147483647
Metric	Enter a metric value which signifies the cost for an access route, for the next hop  Range: 0 through 2147483647
Discard	Specify whether to drop packets to destination; send no ICMP unreachable
Resolve Choices	Select whether indirectly connected next hops must be resolved (Resolve) or not (Do not resolve). Select None if no action is required.
Retain Choices	Select whether the route must be retained (Retain) or deleted from the forwarding table (Do not retain) when the routing protocol process shuts down normally. Select None if no action is required.

Table 77: Fields on the Create Static Route Page (*continued*)

Field	Description
Install Choices	Select whether the route must be installed in the forwarding table (Install) or not (Do not install). Select None if no action is required.
Re-advertise Choices	Select whether the route must be re-advertised by routing protocols (Re-advertise) or not (Do not re-advertise). Select None if no action is required.

## Editing, Deleting, and Deploying Static Routes

### IN THIS SECTION

- [Editing Static Routes | 256](#)
- [Deleting Static Routes | 257](#)
- [Deploying Static Routes | 257](#)

You can edit, delete, and deploy static routes from the **Static Routes** page.

### Editing Static Routes

To modify the parameters configured for a static route:

1. Select **Resources > Devices > Device-Name > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

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

The **Edit static route** page appears.

3. Modify the parameters according to the guidelines provided in [“Adding a Static Route” on page 253](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified values appear on the **Static Routes** page.

## Deleting Static Routes

To delete a static route:

1. Select **Resources > Devices > *Device-Name* > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

2. Select one or more static routes that you want to delete and then click the delete icon.

A page requesting confirmation for the deletion appears.

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected static route is deleted from the **Static Routes** page.

## Deploying Static Routes

To deploy a static route:

1. Select **Resources > Devices > *Device-Name* > Configuration > Routing Instances > View/Configure**.

The **Static Routes** page appears.

2. Select one or more static routes that you want to deploy and then click **Deploy**.

A job is created. Click the job link or go to the Jobs page and view the status of the deployment.

## RELATED DOCUMENTATION

| [Adding a Static Route](#) | 253

# Managing Licenses

IN THIS CHAPTER

- About the Device Licenses Page | 258
- About the CSO Licenses Page | 259

## About the Device Licenses Page

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

You can use the Licenses page to view information about uploaded device licenses for virtual network services from your local file system. The license key is required to enable application-based routing, application monitoring, and other vSRX security features.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a device license. Click the details icon that appears when you hover over the name of an image or click **More > Details**.
- Show or hide columns about the device license. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a device license. Click the Search icon in the top right corner of the page to search for a device license.

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

The search results are displayed on the same page.

### Field Descriptions

Table 78 on page 259 describes the fields on the Device License Files page.



Table 78: Fields on the Device License Files Page

Field	Description
File Name	View the filename of the license. Example: license_Image_v1
Build	View the build name of the license. Example: 1
Version	View the version number of the license. Example: 1.1
Vendor	View the vendor name of the license. Example: Juniper Networks
Family	Select the device family of the license. Example: SRX
Model	View the model number of the license. Example: 1
Description	View the description of the license. Example: The license is applicable for SRX340 device.
Uploaded By	View the administrator who uploaded the license. Example: test_admin
Last Uploaded	View the date and time when the license was uploaded. Example: 11/18/2016 19:15

## About the CSO Licenses Page

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

You can use the CSO Licenses page to view information about the existing CSO licenses assigned to a tenant.

## Tasks You Can Perform

You can perform the following tasks from this page:

- Search for CSO licenses by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

You can search using license SKU, sales order, type, tier, or device class.

- Sort CSO licenses—Click a column name to sort based on the column name.

**NOTE:** Sorting is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the CSO Licenses page.

## Field Descriptions

Table 79 on page 260 describes the fields on the CSO Licenses page.

Table 79: Fields on the CSO Licenses page

Field	Description
License SKU	Displays the license SKU name; for example, S-CSO-C-S1-A-3.
Sales Order	Sales order number; for example, 15563238.
Type	Type of site—on-premise or cloud.
Tier	Support tier associated with the license; for example, Standard.
Device Class	Class of the Juniper device associated with the license; for example, B-class.
SSRN	Software support reference number, which is necessary to identify your purchase order when you contact Juniper Networks for support
Start Date	Date (in MMM DD , YYYY format) from which the license is valid; for example, Aug 29, 2019.

Table 79: Fields on the CSO Licenses page *(continued)*

Field	Description
End Date	Date (in MMM DD , YYYY format) up to which the license is valid. CSO calculates the end date based on the validity of the license SKU.
Device Quantity	Total number of devices that you can add for a license.
Available	Available number of devices that you can add for the license.

RELATED DOCUMENTATION

| [About the Device Licenses Page](#) | 258

# Managing Signature Database and Certificates

## IN THIS CHAPTER

- [Signature Database Overview | 262](#)
- [About the Signature Database Page | 263](#)
- [Installing Signatures | 264](#)
- [Certificates Overview | 265](#)
- [About the Certificates Page | 266](#)
- [Importing a Certificate | 268](#)
- [Installing and Uninstalling Certificates | 270](#)
- [About the VPN Authentication Page | 271](#)

## Signature Database Overview

The signature database that Juniper provides contains application and intrusion prevention system (IPS) signatures:

- Application signatures are definitions of predefined attacks and applications, and can be used to identify applications for tracking firewall policies and quality-of-service (QoS) prioritization.
- IPS signatures are definitions of predefined attack object and attack object groups that you can use in IDP policies to match traffic against known attacks.

Users with the tenant administrator role can install the active signature database on one or more devices.

## RELATED DOCUMENTATION

[About the Signature Database Page | 263](#)

[Installing Signatures | 264](#)

## About the Signature Database Page

To access this page, select **Administration > Signature Database**.

Use the Signature Database page to install the active signature database, which contains intrusion prevention system (IPS) and application signatures, on one or more devices. The signature database contains definitions of attacks and application, which are used in defining IPS profile rules and application firewall rules. These attack objects and groups are designed to detect known attack patterns and protocol anomalies within the network traffic.

### Tasks You Can Perform

You can perform the following task from this page:

- Install signatures on one or more devices. See [“Installing Signatures” on page 264](#).
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the Signature Database page.

### Field Descriptions

[Table 80 on page 263](#) describes the fields on this page.

**Table 80: Fields on the Signature Database Page**

Field	Description
<b>Active Database</b>	
Database Version	Version of signature database.
Publish Date	Date and time (YYYY-MM-DD HH:MM:SS 24-hour format) when the signature database was published.
Installed Device Count	Number of devices on which the signature database was successfully installed.
Detectors	Version numbers of the detector engines associated with the signature database.  Click the <i>detector-versions</i> link to view the detector details. The Detector Details for <i>Signature-Database-Version</i> page appears displaying (in a table) the platform, OS version, and version of the detectors for the signature database. Click <b>Close</b> to return to the Signature Database page.

Table 80: Fields on the Signature Database Page (*continued*)

Field	Description
Action	<p>Click the <b>Install on device</b> link to install the signatures on one or more devices.</p> <p>The Install Signatures page appears. See <a href="#">“Installing Signatures” on page 264</a>.</p> <p><b>NOTE:</b> This field appears only for users with the Tenant Administrator role.</p>

## RELATED DOCUMENTATION

[Signature Database Overview](#) | 262

## Installing Signatures

Users with the tenant administrator role can install the active signature database on one or more devices. Signatures must be present on the device for application firewall or intrusion prevention system (IPS) features to be used. If you do not install the signature database on a device, the deployment of IPS profiles or application firewall will fail.

**NOTE:**

- Before you install the signature database on the device, ensure that the IPS license is installed on the device. If the IPS license is not installed, only the application signatures will be installed when the signature database installation is triggered.
- You can install the signature database on the following devices: NFX150, SRX Series, and vSRX.

To install the active signature database:

1. Select **Administration > Signature Database**.

The Signature Database page appears.

2. Click **Install Signatures**.

The **Install Signatures** page appears displaying the signature database version and the devices on which you can install the signature database.

3. Select the check boxes corresponding to the devices on which you want to install the signature database.

You can also search for, filter, or sort the devices displayed in the table.

4. From the **Type** field:

- Select **Run now** to immediately trigger the installation of the signature database on the devices that you selected.
- Select **Schedule at a later time** to install the signature database later and specify a date and time at which you want the installation to be triggered.

5. Click **OK**.

- If you specified that the database must be installed immediately, a job is triggered and in the Job Tasks page that appears, the tasks associated with the signature database installation are displayed. Click **OK** to exit and return to the Signature Database page.
- If you specified that the database must be installed later, a job is created and you are returned to the Signature Database page. A confirmation message (with the job ID) is displayed at the top of the page.

After the signature database is installed successfully, you can deploy the firewall policy (that references IPS profiles or application signatures) on the device.

## RELATED DOCUMENTATION

[Signature Database Overview | 262](#)

[About the Signature Database Page | 263](#)

## Certificates Overview

SSL uses public–private key technology that requires a private key paired with an authentication certificate for the SSL service. An SSL certificate includes identifying information such as a public key and a signature issued by a certificate authority (CA).

CAs are entities that validate identities and issue certificates. A CA can issue multiple certificates in the form of a tree structure. A root certificate is the topmost certificate of the tree, the private key of which is used to sign other certificates. All certificates immediately below the root certificate inherit the signature or trustworthiness of the root certificate. This is somewhat like the notarizing of an identity. You can configure a root CA certificate by first obtaining a root CA certificate (by either generating a self-signed one or importing one) and then applying it to an SSL proxy profile.

**NOTE:** SSL certificates are used for the SSL forward proxy feature in CSO.

## RELATED DOCUMENTATION

[SSL Forward Proxy Overview | 514](#)

[About the SSL Proxy Profiles Page | 531](#)

## About the Certificates Page

To access this page, select **Administration > Certificates** in Customer Portal.

Use this page to view and manage SSL certificates. You can import a root certificate or a trusted certificate (directly from a file or by pasting the content) and install a certificate on a site.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View information about the existing certificates; see [Table 81 on page 267](#).
- Import a certificate—Select **More > Import Certificate**. See [“Importing a Certificate” on page 268](#).
- View the sites on which a certificate is installed—Select a certificate and then select **More > View Installed Sites**.

The View Installed Sites page appears, displaying the list of sites on which the selected certificate is installed. Click **OK** to close the page and return to the Certificates page.

- Install a certificate on a site—Select a certificate and then select **More > Install Certificate**. See [“Installing and Uninstalling Certificates” on page 270](#).
- Uninstall a certificate from a site—Select a certificate and then select **More > Uninstall Certificate**. See [“Installing and Uninstalling Certificates” on page 270](#).
- View details about a certificate—Select a certificate and then select **More > Detailed View**. The Detailed View page appears. See [Table 82 on page 267](#) for an explanation of fields on this page.

### Field Descriptions

[Table 81 on page 267](#) displays the fields on the Certificates page.



Table 81: Fields on the Certificates Page

Field	Description
Certificate Name	Name of the certificate.
Type	Type of the certificate: <ul style="list-style-type: none"> <li>• Root certificate</li> <li>• Trusted certificate</li> </ul>
Description	Description of the certificate.

Table 82: Fields on the Detailed View Page

Field	Description
Certificate Name	See <a href="#">Table 81 on page 267</a> .
Type	See <a href="#">Table 81 on page 267</a> .
Valid From	Date and time (UTC) from which the certificate is valid.
Valid Upto	Date and time (UTC) until which the certificate is valid.
Serial Number	Serial number of the certificate.
Signature Algorithm	Algorithm used to sign the certificate.
Issuer Details	Details of the authority that issued the certificate, including details such as name, country, organization, and so on.
Version	X.509 version of the certificate.

## RELATED DOCUMENTATION

[About the SSL Proxy Profiles Page](#) | 531

## Importing a Certificate

You can import an SSL certificate (directly from a file or by pasting the content) from the Import Certificate page.

**NOTE:** If you want to use the SSL proxy feature, you must import at least one root certificate for a tenant; the certificate can be used in one or more sites.

To import a certificate:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears.

2. Select **More > Import Certificate**.

The Import Certificate page appears.

3. Complete the configuration according to the guidelines provided in [Table 83 on page 268](#).

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

4. Click **OK** to import the certificate.

You are taken to the Certificates page. If the certificate content that you imported is validated successfully, a confirmation message is displayed; if not, an error message is displayed.

After importing a certificate, you can use it when you create an SSL proxy profile.

**Table 83: Import Certificate Settings**

Setting	Guideline
<b>Certificate Name</b>	Enter the certificate name, which must be a unique string of alphanumeric characters and some special characters ( _ -). No spaces are allowed and the maximum length is 32 characters.
<b>Certificate Type</b>	Select an option to specify whether the certificate that you are importing is a root certificate ( <b>Root CA</b> ) or a trusted certificate ( <b>Trusted CA</b> ).



```
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
-----END CERTIFICATE-----
```

## RELATED DOCUMENTATION

[Installing and Uninstalling Certificates | 270](#)

[Creating SSL Forward Proxy Profiles | 533](#)

## Installing and Uninstalling Certificates

### IN THIS SECTION

- [Installing a Certificate | 270](#)
- [Uninstalling a Certificate | 271](#)

You can install and uninstall certificates from the Certificates page. This topic has the following sections:

### Installing a Certificate

Use the Install Certificate page to install certificates on one or more sites.

To install a certificate on one or more sites:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears, displaying the existing certificates.

2. Select the certificate that you want to install, and then select **More > Install Certificate**. Alternatively, right-click a certificate and select **Install Certificate**.

The Install Certificate page appears, displaying a list of sites.

3. Select the sites on which you want to install the certificate.
4. Click **Install** to install the certificate on the selected sites.

You are taken to the Certificates page. A job is created and a confirmation message appears with the ID of the job. Click the job ID to go to the Jobs page, where you can view the status of the job.

## Uninstalling a Certificate

If a certificate's validity has expired or if you want to remove a certificate from a site, you can uninstall the certificate from that site.

To uninstall a certificate from one or more sites:

1. Select **Administration > Certificates** in Customer Portal.

The Certificates page appears, displaying the existing certificates.

2. Select the certificate that you want to uninstall, and then select **More > Uninstall Certificate**.  
Alternatively, right-click a certificate and select **Uninstall Certificate**.

The Uninstall Certificate page appears, displaying only those sites on which the certificate was previously installed.

3. Select the sites from which you want to uninstall the certificate.

4. Click **Uninstall** to uninstall the certificate from the site.

You are taken to the Certificates page. A job is created and a confirmation message appears with the ID of the job. Click the job ID to go to the Jobs page, where you can view the status of the job.

## RELATED DOCUMENTATION

| [Importing a Certificate](#) | 268

## About the VPN Authentication Page

To access this page, select **Administration > Certificate Management > VPN Authentication** in Customer Portal.

Use this page to change the method of renewing public key infrastructure (PKI) certificates for a tenant, view PKI certificates for a specific site, update the CRL URL for a PKI certificate, renew a PKI certificate, and change the method of renewing a PKI certificate for a specific site.

### Task You Can Perform

You can perform the following tasks from this page:

- View information about the existing certificates. See [Table 84 on page 272](#).
- Change the method of renewing public key infrastructure (PKI) certificates for a tenant by clicking the **Change** link.

**NOTE:** You can change the default settings of the **Auto Renew** and **Renew before expiry** fields on the VPN Authentication page only if the **Auto Renew** toggle button for a tenant is enabled.

- Update the CRL URL—Select a certificate and then select **Update CRL URL**. The Edit Tenant Certificate CRL page appears. Update the CRL URL and click **OK**.
- Manually renew a certificate on a site—Select a certificate and then select **Renew Certificate**. The Confirm Renew Certificate page appears. Click **Yes** to manually renew the certificate.
- Change the renewal method of a certificate on all sites in a tenant—Select a certificate and then select **Change Renewal Method**. Choose the renewal method (Set Auto Renew or Set Manual Renew). The Edit Certificate Renew Method page appears and click **Yes** to change the renewal method.

**NOTE:** At the tenant-level if you have set the renewal method as Manual Renew, you cannot change the renewal method to Auto Renew at the site-level. That is, the renewal method can be changed at the site-level only if you have set the renewal method as Auto Renew at the tenant-level.

### Field Descriptions

[Table 84 on page 272](#) displays the fields on the VPN Authentication page.

**Table 84: Fields on the VPN Authentication Page**

Field	Description
Certificate ID	ID of the PKI certificate.
Used In	Displays the site name to which the PKI certificate is associated.
Device	Displays the device name to which the PKI certificate is associated.

Table 84: Fields on the VPN Authentication Page (*continued*)

Field	Description
Status	Displays the remaining time duration for the certificate to expire. For example, <b>Less than 2 weeks before expiry</b> .
Expires On	Displays the expiry date of a PKI certificate along with the time.
Renewal Method	Displays the renewal method of a PKI certificate. <ul style="list-style-type: none"><li>• Auto</li><li>• Manual</li></ul>

# Managing Juniper Identity Management Service

## IN THIS CHAPTER

- [Juniper Identity Management Service Overview | 274](#)
- [About the Identity Management Page | 277](#)
- [Configuring CSO and JIMS Connection | 278](#)
- [Configuring JIMS for an SRX Device | 280](#)

## Juniper Identity Management Service Overview

### IN THIS SECTION

- [Access Token Query | 275](#)
- [Batch or Periodic Query | 275](#)
- [IP Address Query | 276](#)
- [User Mapping Query | 276](#)

Juniper Identity Management Service (JIMS) provides a robust and scalable user identification and IP address mapping implementation that includes endpoint context and machine ID. JIMS collects user identity information from different authentication sources, for SRX Series devices.

JIMS collects user identity information from a configured Active Directory and makes it available to SRX Series devices or vSRX instances. You can download and install Juniper Identity Management Service (JIMS), configure the CSO client on JIMS to obtain user identity information from the configured Active Directory, and use CSO and JIMS to manage user-based firewall policy intents on SRX Series devices and vSRX instances.

The SRX Series devices communicate with JIMS through HTTP or HTTPS connection. Use HTTP connection for debugging and HTTPS for deployments. SRX Series devices consist of primary and secondary JIMS configurations. These devices must always query the primary JIMS. The secondary JIMS is available as a



fall back option with limited resources. The secondary JIMS must be used when the HTTP GET query or a number of queries to the primary JIMS fails. SRX Series devices constantly scrutinize the failed primary JIMS and revert to the primary JIMS, once it is up and running.

When you request a JIMS report, the SRX Series device specifies the timestamp. JIMS forms an HTTPS response from the earliest known report since the requested timestamp. SRX Series devices request for the maximum number of reports to include in the response from JIMS. Along with the requested reports, JIMS always returns a cookie. In the subsequent requests to JIMS, SRX Series devices include cookies instead of timestamp to indicate the same context, same beginning timestamp, and to resume the same response from where it has stopped the previous time.

**NOTE:**

- IP and user mapping information might be inaccurate, if the user identities in JIMS are cleared, delayed, or missing.
- SRX firewall authentication can also push the authentication entries to JIMS.

The SRX Series device communicates with JIMS through HTTP or HTTPS messages to obtain the access token and query for user identities. The following different query modes are available and all queries can happen simultaneously.

### Access Token Query

JIMS requires OAuth 2.0 protocol to authenticate or authorize. The SRX Series device user query function requires an access token to query the JIMS server. The SRX Series device uses the client credentials such as client ID and client secret to obtain an access token. These parameters must be consistent with the API client configured on JIMS.

### Batch or Periodic Query

At the beginning, SRX Series device sends the batch queries to JIMS sequentially to obtain all the expected user identities. When there are no more entries in JIMS, SRX Series device periodically queries for the newly generated reports with the configured interval.

The timestamp is mentioned in the query to restart the response. The timestamp is expected in the query under the following circumstances:

- SRX Series device queries the JIMS server for the first time
- SRX Series device switches over to the secondary JIMS
- SRX Series device does the error recovery because of an internal error or upon receiving error response from JIMS

For all the other cases, SRX Series device provides the received cookie information in the query instead of a timestamp.

### IP Address Query

SRX Series device can provide another query to JIMS specifying the IP address, if it has missed the data for the existing IP address flow. If there are many IP address queries in the queue, SRX Series device can keep multiple concurrent HTTP or HTTPS connections with JIMS to increase the throughput. However, the number of concurrent connections are restricted to less than or equal to 20 connections to reduce the load on JIMS.

### User Mapping Query

SRX Series device can engage Captive Portal to obtain the user ID to authenticate the user. Once the user is authenticated, SRX Series device can issue another query to JIMS specifying the user ID and IP address to obtain user information. The firewall authentication uses the `https://<JIMS>/<query-api>/user/ip=<ip>&id=<id>&domain=<domain>` API to push an authentication success entry to JIMS with the user IP, user ID, and the domain. JIMS responds with the user information.

The difference between the IP address query and user query is that the IP address query does not have the user ID. Both these queries insert the user information to the internal cache of JIMS , and all SRX devices are updated with user information.

## RELATED DOCUMENTATION

---

[About the Identity Management Page | 277](#)

---

[Configuring CSO and JIMS Connection | 278](#)

---

[Configuring JIMS for an SRX Device | 280](#)

## About the Identity Management Page

To access this page, select **Administration > Identity Management**.

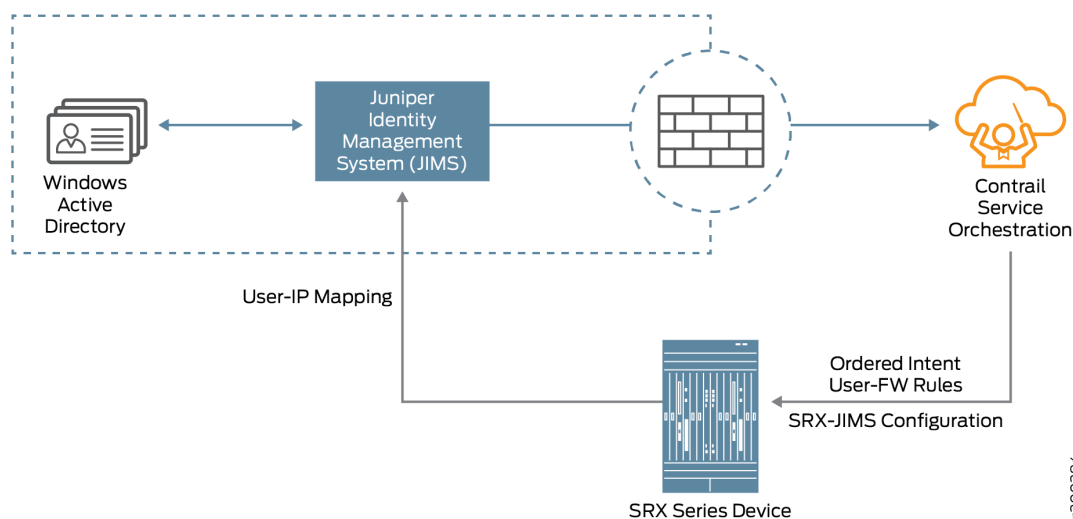
### NOTE:

- For information on system requirements for installing JIMS, see [System Requirements for Installing Juniper Identity Management Service](#)
- For information on installing JIMS on your Windows server, see [Installing Juniper Identity Management Service](#).

Use the **Identity Management** page to download and install JIMS, interface JIMS with CSO to obtain advanced user identity an active directory, and use CSO to push the JIMS configuration to SRX Series devices.

[Figure 9 on page 277](#) illustrates the connectivity between, CSO, JIMS, and an SRX Series device.

**Figure 9: CSO-JIMS-SRX Connectivity Configuration**



## Tasks You Can Perform

You can perform the following tasks from this page:

- Download the JIMS executable to your Windows server using **Download JIMS**. Run the JIMS executable to install JIMS on your Windows server machine. See [System Requirements for Installing Juniper Identity Management Service](#) and [Installing Juniper Identity Management Service](#).

After you have successfully installed JIMS, you can login into JIMS using your Windows user ID and password.

- Configure the connection between CSO and JIMS to import user and group lists from an Active Directory (AD) of your choice, using **JIMS to CSO**. See [“Configuring CSO and JIMS Connection” on page 278](#).
- Configure the connection between JIMS and an SRX Series device. See [“Configuring JIMS for an SRX Device” on page 280](#).

## RELATED DOCUMENTATION

[Juniper Identity Management Service Overview | 274](#)

[Configuring CSO and JIMS Connection | 278](#)

[Configuring JIMS for an SRX Device | 280](#)

[Preparing CSO Identity Management](#)

[JIMS v1.1 Feature Guide](#)

## Configuring CSO and JIMS Connection

Before you begin to configure the connection between CSO and JIMS, ensure that you have downloaded and installed JIMS. See [System Requirements for Installing Juniper Identity Management Service](#) and [Installing Juniper Identity Management Service](#).

To configure a connection between CSO and JIMS:

1. Select **Administration > Identity Management**.

The **Identity Management** page appears.

2. Click **JIMS-to-CSO Configuration** or the greater-than (>) symbol beside it.

The **JIMS-to-CSO Configuration** panel expands. The panel displays a system-generated user name which cannot be changed, the last updated time of the user identity information from Active Directory and the connection status of the JIMS server(s).

**NOTE:** If you have already configured a JIMS user account in CSO, the details of this connection is displayed in the **JIMS-to-CSO Configuration** panel.

3. The **Username** is auto-generated for each tenant. You will not be able to change it. Enter a password of your choice for your JIMS-to-CSO connection in the **Password** field.

**NOTE:** The password must contain a number, an upper-case letter, and a special character.

**NOTE:** The password you entered will appear encrypted. If you want to see the password that you entered as plain text, select **Show Password**.

4. Click **Save** to save your changes. The JIMS user credentials are saved.  
If you do not want to save your changes, click **Cancel**.
5. CSO and JIMS need to be connected in order for JIMS to push data to CSO. To set up this connection, you must configure the CSO client on JIMS, using the username and password that you created in the **JIMS-to-CSO Configuration** panel. For more information on configuring the CSO client on JIMS, see [Configuring the Connection to a CSO Client](#).
6. Configure an Active Directory (AD) as a data source in JIMS, see [Configuring the Connection to an Active Directory](#).

**NOTE:** After your JIMS user credentials are saved, the password field changes to the **Change Password** link.

If you want to change your password, click **Change Password**.

The **Change Password** page appears.

- Enter your new password in the **New Password** field and re-enter the same password in the **Confirm Password** field.
- Click **OK** to save the new password. The updated password is saved.

If you do not want to save your new password, click **Cancel** instead.

## RELATED DOCUMENTATION

## Configuring JIMS for an SRX Device

Configuring the connection between SRX Series devices to JIMS allows the JIMS server to send the IP address, username, and group relationship information to SRX Series devices through CSO. You can also configure a set of optional advanced settings for authentication timeout, domain filters, and choose to include or exclude user identity information in the communication between the JIMS server and the SRX Series device.

For every SRX Series device, you can configure the primary and secondary JIMS servers. The SRX Series device always queries the primary JIMS server. The secondary JIMS server is available as a fallback option with limited resources. The secondary JIMS server is used when a number of queries to the primary JIMS server fails. The SRX Series device constantly scrutinizes the failed primary JIMS server and reverts to the primary JIMS server, once it is up and running.

Before you begin, you need the following information:

- The IP address of the primary and secondary (optional) JIMS server.
- The client ID to obtain an OAuth token from the JIMS server for user queries.
- The client secret to obtain an OAuth token from the JIMS server for user queries.

To configure a connection between an SRX Series device and JIMS:

1. Select **Administration > Identity Management**.

The **Identity Management** page appears.

2. Click **SRX-to-JIMS Configuration** or the greater-than (>) symbol beside it.

The **SRX-to-JIMS Configuration** panel expands.

**NOTE:** If you have already configured JIMS for an SRX Series device, the details of this configuration is displayed in the **SRX-to-JIMS Configuration** panel.

3. Complete the configuration according to the guidelines provided in [Table 85 on page 281](#).

4. Click **Save** to save the changes. JIMS is now configured for an SRX device.

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

Table 85 on page 281 provides guidelines on using the fields on the **SRX-to-JIMS Configuration** panel.

**Table 85: Fields on the SRX-to-JIMS Configuration Panel**

Field	Description
<b>Identity</b>	
IP Address	<p>Enter a valid IPv4 or IPv6 address of the primary JIMS server.</p> <p>SRX Series devices always query the primary JIMS to obtain the user identities.</p>
Secondary Identity	<p>Enable this option to use the secondary JIMS server as a fallback when the primary JIMS server fails. By default, this option is disabled.</p>
Secondary IP Address	<p>Enter a valid IPv4 or IPv6 address of the secondary JIMS server.</p> <p>The secondary JIMS is available as a fall back option with limited resources. Use the secondary JIMS when the HTTP GET query or number of queries to the primary JIMS fails.</p>
<b>Client Credentials</b>	
Client ID	<p>Enter the client ID that the SRX Series device provides to JIMS server as part of its authentication. The SRX Series device must authenticate itself with the JIMS server to obtain an access token that allows the it to query the JIMS server for user identity information. The client ID must be consistent with the CSO client ID or username configured on the JIMS server.</p>
Client Secret	<p>Enter the client secret that the SRX Series device provides to the JIMS server as part of its authentication. The client secret must be consistent with the CSO client secret or password configured on the JIMS server.</p>
<b>Advanced Settings</b>	
Authentication Entry Timeout	<p>Enter the timeout interval (in minutes) after which, the idle entries in the JIMS authentication table expire. The timeout interval begins from when the user authentication entry is added to the authentication table. This value can be between 10 and 1440 minutes, where a value of 0 means no timeout. The default value is 69 minutes.</p>
Include IP Address(es)	<p>The SRX Series device sends a query to JIMS for the user identity information only for the IP addresses present in the selected address group; JIMS responds with the requested user identity information.</p> <p>Click <b>Add New Address</b> to create a new IP address group, see <a href="#">“Creating Addresses or Address Groups” on page 573</a>.</p>

Table 85: Fields on the SRX-to-JIMS Configuration Panel (*continued*)

Field	Description
Exclude IP Address(es)	<p>The SRX Series device does not query JIMS for the user identity information for the excluded IP addresses present in the selected address group.</p> <p>Click <b>Add New Address</b> to create a new IP address group, see <a href="#">“Creating Addresses or Address Groups”</a> on page 573.</p>
Filter Domain(s)	<p>The SRX Series device sends a query to JIMS for the user identity information within the specified domains. Enter a comma-separated list of up to 25 domain names. A domain name can be an alphanumeric string of up to 64 characters that can also contain dashes, underscores, and dots.</p> <p>Example: example.net</p>

## RELATED DOCUMENTATION

---

[Juniper Identity Management Service Overview | 274](#)


---

[About the Identity Management Page | 277](#)


---

[Configuring CSO and JIMS Connection | 278](#)



# 4

PART

## Managing Policies, Profiles, and Proxies

---

Managing Firewall Policies | **284**

Managing UTM Profiles | **357**

Managing SLA Profiles and SD-WAN Policies | **406**

Managing NAT Policies | **456**

Managing IPS Signatures and Profiles | **491**

Managing SSL Proxies | **514**

Deploying Policies | **544**

---

# Managing Firewall Policies

## IN THIS CHAPTER

- Firewall Policy Overview | 285
- About the Firewall Policy Page | 287
- Adding a Firewall Policy | 288
- Editing and Deleting Firewall Policies | 290
- Adding Firewall Policy Intents | 291
- Editing, Cloning, and Deleting Firewall Policy Intents | 297
- Selecting Firewall Source | 299
- Selecting Firewall Destination | 303
- Firewall Policy Examples | 306
- Firewall Policy Schedules Overview | 346
- About the Firewall Policy Schedules Page | 347
- Creating Schedules | 348
- Editing, Cloning, and Deleting Schedules | 350
- Deploying Firewall Policies | 351
- About the Default Profiles for Unified Firewall Policy Page | 352
- Editing Default Settings for the Unified Firewall Policy | 354

## Firewall Policy Overview

Contrail Service Orchestration (CSO) provides the ability to create, modify, and delete firewall policy intents associated with a firewall policy. Firewall policies are presented as *intent-based policies*. A firewall policy intent controls transit traffic within a context that is derived out of the end-points defined in the intent. Intent-based firewall policies can incorporate both transport layer (Layer 4) and application layer (Layer 7) firewall constructs in a single intent. The underlying system, automatically analyzes the intent, translates them into the set of rules the devices understand. The choice of sequence and the assignment happens implicitly based on the endpoints in the intent definition. The intent consist of source and destination endpoints. Endpoints could be applications (L7), sites or site groups, IP address/address-groups, services, or departments.

### NOTE:

- Intent based policies are not applicable for Hybrid WAN deployments.
- Starting from CSO Release 5.0.1, if a device (CPE or next-generation firewall) is running Junos OS Release 18.2R1 or later, a firewall policy acts as a unified firewall policy. In a unified firewall policy, dynamic application can be used as a match condition along with the existing match conditions. Therefore, a separate application firewall is not configured on the device to allow or block traffic to an application.

However, If the device is running a version earlier than Junos OS Release 18.2R1, the firewall policy does not act as a unified firewall policy and application firewalls continue to be configured on the device.

See [Unified Security Policies](#) for information about unified firewall policies.

Firewall policies provide security functionality by enforcing intents on traffic that passes through a device. Traffic is permitted or denied based on the action defined as the firewall policy intent.

A firewall policy provides the following features:

- Permits, rejects, or denies traffic based on the application in use.
- Identifies not only HTTP but also any application running on top of it, enabling you to properly enforce policies. For example, an application firewall intent could block HTTP traffic from Facebook but allow Web access to HTTP traffic from Microsoft Outlook.
- Provides the ability to enable advanced security protection by specifying one or more of the following:
  - Unified threat management (UTM) profile
  - SSL proxy profile
  - Intrusion prevention system (IPS) profile

In CSO, intents are categorized as zone-based intents and enterprise-based intents.

- Zone-based-intents are intents with zones as source and destination endpoints. The policies with zone-based intents can be applied to SD-WAN sites , hybrid WAN sites, and next-generation firewall sites. The parameters that you can define for zone-based intents are listed in [Table 86 on page 286](#).

**Table 86: Zone-based intents**

Source End Points	Destination End points	Advanced Security Options	Supported Options
Zones	Zones	SSL Proxy Profile	Scheduler
Address	Address	UTM Profile	Logging
Users	Service (L4 port/protocol) Applications (Dynamic Applications)	IPS Profile	

**NOTE:** You cannot select a department or site as an endpoint in zone-based intents. The sites assigned to the policy are applicable for zone-based intents and are automatically considered for deployment.

- Enterprise-based intents are intents that contain sites, site-groups, departments, addresses as source and destination endpoints. Firewall policies with enterprise-based intents can be applied only to SD-WAN sites. The parameters that you can define for enterprise-based intents are listed in [Table 87 on page 286](#).

**Table 87: Enterprise-based intents**

Source Endpoints	Destination Endpoints	Advanced Security Options	Supported Options
Sites	Sites	UTM Profile	Scheduler
Site-groups	Site-groups	IPS Profile	Logging
Departments	Departments		
Addresses	Addresses		
Users	Users Service/Applications		

**NOTE:**

- Zones cannot be selected as source or destination endpoints for enterprise-based intents.
- Intents added in CSO Release 4.1 and earlier are now called enterprise-based-intents.

RELATED DOCUMENTATION

About the Firewall Policy Page   287
Firewall Policy Examples   306
Adding Firewall Policy Intents   291
Editing, Cloning, and Deleting Firewall Policy Intents   297

## About the Firewall Policy Page

To access this page, select **Configuration > Firewall > Firewall Policy**.

Use this page to view and manage policy intents associated with your site or site groups. You can filter and sort this information to get a better understanding of what you want to configure.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a firewall policy intent. See [“Adding Firewall Policy Intents” on page 291](#).
- Modify, clone or delete firewall policy intents. See [“Editing, Cloning, and Deleting Firewall Policy Intents” on page 297](#).
- Deploy a firewall policy. See [“Deploying Policies” on page 548](#).

**NOTE:** An orange line is displayed against all undeployed firewall policy intents.

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

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

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.
- View undeployed intents. Click the **Show Hide Columns** icon at the top right corner of the page and select **Undeployed Intent** under **Quick Filters**.

### Field Descriptions

[Table 88 on page 288](#) provides guidelines on using the fields on the **Firewall Policy** page.

Table 88: Fields on the Firewall Policy Page

Field	Description
Source	Source endpoint to which a firewall policy intent applies. A source endpoint can be addresses, sites, site groups, departments, users, or Internet (all in-bound traffic).
Destination	Destination endpoint to which a firewall policy intent applies. A destination endpoint can be addresses, services, sites, application signatures and groups, services and groups, or departments.
Options	Displays whether scheduling, logging, and UTM options are enabled for the firewall policy intent.
Total	Number of intents associated with the firewall policy.
Undeployed	Number of intents associated with the firewall policy that are either created new or updated, but are not yet deployed.

## RELATED DOCUMENTATION

[Firewall Policy Overview | 285](#)
[Adding Firewall Policy Intents | 291](#)
[Firewall Policy Examples | 306](#)
[Editing, Cloning, and Deleting Firewall Policy Intents | 297](#)
[About the Deployments Page | 545](#)
[Deploying Policies | 548](#)

## Adding a Firewall Policy

A firewall policy enforces rules for transit traffic, in terms of what traffic can pass through the firewall, and the actions that need to take place on traffic as it passes through the firewall.

Use this page to add a firewall policy and assign it to one or more sites.

**NOTE:** A single policy can have both enterprise based intents and zone based intents for SD-WAN sites, hybrid WAN sites, and next generation firewall sites.

To add a firewall policy:

- 1. Select **Configuration > Firewall > Firewall Policy**,

The Firewall Policy page appears.

- 2. Click the plus icon (+).

The Add Firewall Policy page appears.

- 3. Complete the configuration settings according to the guidelines provided in [Table 89 on page 289](#).

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

- 4. Click **OK**.

The new firewall policy is created and a confirmation message is displayed.

**Table 89: Fields on the Add Firewall Policy Page**

Field	Description
Name	Enter a unique string of alphanumeric characters that can include spaces and some special characters.  The maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 255 characters.
All Sites	Select the check box to apply the firewall policy to all sites.
Select Sites	Select one or more sites to which the policy must be applied.  Select the sites from the <b>Available</b> column and click the right-arrow to move the sites to the <b>Selected</b> column.

## Editing and Deleting Firewall Policies

### IN THIS SECTION

- [Editing Firewall Policies | 290](#)
- [Deleting Firewall Policies | 290](#)

You can edit and delete firewall policies from the **Firewall Policy** page.

### Editing Firewall Policies

To modify the parameters configured for a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Hover over the firewall policy that you want to edit, and then click on the edit icon (pencil symbol) that appears on the right side of the intent.

The **Firewall Policy** page displays the same options as those that appear when you create a new firewall policy intent.

3. Modify the parameters following the guidelines provided in [“Adding Firewall Policy Intents” on page 291](#).
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **Save**, the modified intent appears on the **Firewall Policy** page.

### Deleting Firewall Policies

To delete a firewall policy:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Select the firewall policy that you want to delete and then click the ... icon that appears on the right side of the policy.



3. Select **Remove**.

A message requesting confirmation for the deletion appears.

4. Click **Yes** to delete the selected firewall policy. If you want to discard your changes, click **Cancel** instead.

If you click **Yes**, the selected policy is deleted from the Firewall Policy page.

## RELATED DOCUMENTATION

## Adding Firewall Policy Intents

Use this page to add a firewall intent that controls transit traffic within a context . The traffic is classified by matching its source and destination zones, the source and destination addresses, and the application that the traffic carries in its protocol headers with the policy database.

You can also enable advanced security protection by specifying one or more of the following:

- Unified threat management (UTM) profile
- SSL proxy profile
- Intrusion prevention system (IPS) profile

To configure a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The Firewall Policy page appears.

2. Click the firewall policy to which you want to add the intent.

The *Firewall-Policy-Name* page appears.

3. Click the add icon (+).

The option to create firewall policy intent appears inline on the *Firewall-Policy-Name* page.

4. Complete the configuration according to the guidelines provided in [Table 90 on page 292](#).

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

If you click **Save**, a new firewall policy intent with the provided configuration is saved and a confirmation message is displayed. Based on the source and destination end points, the intents are categorized as zone-based intents and enterprise-based intents.


**NOTE:** After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications. When a firewall policy intent is created, the Undeployed field is incremented by one indicating that intents are pending deployment.

Table 90: Fields on the <Firewall-Policy-Name> Page

Field	Description
General Information	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters. If you do not enter a name, the intent is saved with a default name assigned by CSO.
Description	Enter a description for the policy intent; maximum length is 1024 characters.

Table 90: Fields on the &lt;Firewall-Policy-Name&gt; Page (continued)

Field	Description
<b>Select Schedule</b>	<p>Policy schedules enable you to define when a policy is active, and thus are an implicit match criterion. You can define the day of the week and the time of the day when the policy is active. For instance, you can define a security policy that opens or closes access based on business hours. Select a pre-saved schedule and the schedule options are populated with the selected schedule's data.</p> <p>You can add a schedule from the <b>End Points</b> panel, by selecting the schedule and clicking on the check mark icon (✓).</p> <p>You can also create new schedules and then associate the schedule to your firewall policy.</p> <p>To create a new schedule and then add it to a firewall policy:</p> <ol style="list-style-type: none"> <li>1. Click <b>Select Schedule</b>.</li> <li>2. Click <b>Add new</b>.  Alternately, click the lesser-than icon (&lt;) to open the <b>End Points</b> panel. Click on the add icon (+) on the top right of the panel and select <b>Schedule</b>.  The <b>Create Schedules</b> page appears.</li> <li>3. Create a new schedule. See <a href="#">“Creating Schedules” on page 348</a>.  The new schedule appears in the <b>End Points</b> tab, under <b>Schedules</b>.</li> <li>4. Select the schedule and click on the add icon (+) to add it to the firewall policy.</li> </ol>
<b>Logging</b>	<p>Click the toggle button to enable logging; by default, logging is disabled. You can see the logged firewall events in the <b>Firewall Events</b> page by using <b>Monitor &gt; Security Events &gt; Firewall Events</b>.</p> <p>For more information, see <a href="#">“About the Firewall Events Page” on page 640</a>.</p>
<i>Identify the traffic that the intent applies to</i>	
<b>Source</b>	<p>Click the add icon (+) to select the source end points on which the firewall policy intent applies, from the displayed list of addresses, departments, sites, site groups, users, zones, or the Internet. You can also select a source end point using the methods described in <a href="#">“Selecting Firewall Source” on page 299</a>.</p>

Table 90: Fields on the &lt;Firewall-Policy-Name&gt; Page (continued)

Field	Description
<b>Destination</b>	Click the add icon (+) to select the destination end points on which the firewall policy intent applies, from the displayed list of addresses, departments, sites, site groups, zones or the Internet. You can also select a destination end point using the methods described in <a href="#">“Selecting Firewall Destination” on page 303</a> .
<b>Select Action</b>	<p>Click the add icon (+) to choose whether you want to permit, deny, or reject traffic between the source and destination.</p> <ul style="list-style-type: none"> <li>• <b>Allow</b>—Device permits traffic using the type of firewall authentication you applied to the policy.</li> <li>• <b>Deny</b>—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable.</li> <li>• <b>Reject</b>—Device sends a TCP reset if the protocol is TCP, and device sends an ICMP reset if the protocols are UDP, ICMP, or any other IP protocol. This option is useful when dealing with trusted resources so that applications do not waste time waiting for timeouts and instead get the active message.</li> </ul>
<b>Advanced Security</b>	<p><b>NOTE:</b> This field is enabled only if you either select <b>Allow</b> for the action or if you select a zone as a source and destination.</p> <ul style="list-style-type: none"> <li>• <b>UTM Profile</b>—When you set the action to <b>Allow</b>, you can specify a UTM profile by selecting a profile from the list (under <b>UTM Profiles [UTM]</b>). You specify a UTM profile for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. You can add a new UTM profile by clicking + in the End Points pane and selecting <b>UTM Profiles</b>. See <a href="#">“Creating UTM Profiles” on page 364</a>.</li> <li>• <b>IPS Profile</b>—When you set the action to <b>Allow</b>, you can specify an IPS profile by selecting a profile from the list (under <b>IPS Profiles [IPS]</b>). You specify an IPS profile to monitor and prevent intrusions.</li> <li>• <b>SSL Proxy Profile</b>—When you configure a zone as part of the source and the destination, you can specify an SSL proxy profile by selecting a profile from the list (under <b>SSL Profiles [SSLP]</b>). You add an SSL proxy profile to ensure the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. You can also add a new SSL proxy profile by clicking + in the End Points pane and selecting <b>SSL Proxy Profile</b>. See <a href="#">“Creating SSL Forward Proxy Profiles” on page 533</a>.</li> </ul>
<i>Add source and destination end points</i>	

Table 90: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
End Points	

Table 90: Fields on the &lt;Firewall-Policy-Name&gt; Page (continued)

Field	Description
	<p>To add an end point to the source or destination:</p> <ol style="list-style-type: none"> <li>Click on <b>Source</b> or <b>Destination</b> and then click the lesser-than icon on the right side of the page to open the <b>End Points</b> panel.</li> </ol> <p>The <b>End Points</b> panel displays the end points relevant to the source or destination based on your selection.</p> <ul style="list-style-type: none"> <li>End points from addresses, departments, users, and sites are displayed for source.</li> </ul> <p><b>NOTE:</b> If JIMS is not configured for CSO, users will not be listed in the <b>End Points</b> panel. Instead you will be provided with an option to import users through the <b>Administration &gt; Identity Management</b> page. To import users, click <b>Set Up</b> and follow the steps provided in <a href="#">"About the Identity Management Page" on page 277</a>.</p> <ul style="list-style-type: none"> <li>End points from addresses, applications, departments, services, and sites are displayed for destination.</li> </ul> <p><b>NOTE:</b> You can also search for a specific end point using the search option.</p> <ol style="list-style-type: none"> <li>(Optional) Click on the edit icon (pencil symbol) to modify an end point.</li> <li>(Optional) Click on the details icon on the right of the end point, to view more information about a source or destination end point.</li> <li>Select the end point you want to add and click on the check mark icon (✓) to add it the source or destination.</li> </ol> <p>The selected end point is added to the source or destination.</p> <p>To add new source and destination end points:</p> <ol style="list-style-type: none"> <li>Click the less-than icon (&lt;) on the right side of the page, to open the <b>End Points</b> panel.</li> <li>Click on the add icon (+) on the top right of the <b>End Points</b> panel.</li> </ol> <p>A list of end points that you can add is displayed.</p> <ol style="list-style-type: none"> <li>Select the end point you want to add.</li> </ol> <p>You can add the following end points:</p> <ul style="list-style-type: none"> <li>Address or address group. See <a href="#">"Creating Addresses or Address Groups" on</a></li> </ul>

Table 90: Fields on the <Firewall-Policy-Name> Page (continued)

Field	Description
	<p><a href="#">page 573</a>.</p> <ul style="list-style-type: none"> <li>• Site group. See <a href="#">“Creating Site Groups” on page 145</a>.</li> <li>• Department. See <a href="#">“Adding a Department” on page 602</a>.</li> <li>• Service or service group. See <a href="#">“Creating Services and Service Groups” on page 579</a>.</li> <li>• Create an application signature group. See <a href="#">“Adding Application Signature Groups” on page 599</a>.</li> <li>• Create a schedule. See <a href="#">“Creating Schedules” on page 348</a>.</li> </ul> <p>4. Click <b>Save</b> to add the new end point.</p> <p>The created end point is listed in the <b>End Points</b> panel.</p> <p>5. Select the end point you want to add to the source or destination, and click on the check mark icon (✓).</p> <p>The end point is added to the source or destination.</p>

## RELATED DOCUMENTATION

[Firewall Policy Overview | 285](#)

[About the Firewall Policy Page | 287](#)

[Firewall Policy Examples | 306](#)

[Editing, Cloning, and Deleting Firewall Policy Intents | 297](#)

## Editing, Cloning, and Deleting Firewall Policy Intents

### IN THIS SECTION

- [Editing Firewall Policy Intents | 298](#)
- [Cloning Firewall Policy Intents | 298](#)
- [Deleting Firewall Policy Intents | 299](#)

You can edit, clone, and delete firewall policy intents from the **Firewall Policy** page.

### Editing Firewall Policy Intents

To modify the parameters configured for a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the list of firewall policies.

2. Click the firewall policy for which you want to edit the firewall policy intents.

The firewall policy intents are displayed in the Firewall Policy page.

3. Hover over the firewall policy intent that you want to edit, and then click the ... icon that appears on the right side of the intent. Click **Edit**.

The **Firewall Policy** page displays the same options as those that appear when you create a new firewall policy intent.

4. Modify the parameters following the guidelines provided in [“Adding Firewall Policy Intents” on page 291](#).

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

If you click **Save**, the modified intent appears on the **Firewall Policy** page.

### Cloning Firewall Policy Intents

To clone a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the intents associated with the policy.

2. Click the firewall policy for which you want to clone the firewall policy intents.

The firewall policy intents are displayed in the Firewall Policy page.

3. Hover over the firewall policy intent that you want to clone, and then click the ... icon that appears on the right side of the intent. Click **Clone**.

The **Firewall Policy** page displays the same options as those that appear when you create a new firewall policy intent. Update the cloned intent as required.

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



If you click **Save**, the cloned intent is added to the firewall policy and appears on the **Firewall Policy** page.

## Deleting Firewall Policy Intents

To delete a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.

The **Firewall Policy** page appears, displaying the intents associated with the policy.

2. Click the firewall policy for which you want to delete the firewall policy intent.

The firewall policy intents are displayed in the Firewall Policy page.

3. Select the firewall policy intent you want to delete, and then click the ... icon that appears on the right side of the intent. Click **Delete**.

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

4. Click **Yes** to delete the selected intent. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected intent is deleted from the policy.

## RELATED DOCUMENTATION

---

[Firewall Policy Overview | 285](#)

---

[About the Firewall Policy Page | 287](#)

---

[Firewall Policy Examples | 306](#)

---

[Adding Firewall Policy Intents | 291](#)

## Selecting Firewall Source

### IN THIS SECTION

- [Adding an End Point as Firewall Source | 300](#)
- [Selecting Firewall Source Using Abbreviations | 301](#)
- [Selecting a Firewall Source from the End Points Panel | 301](#)

- Creating and Selecting a Firewall Source from the End Points Panel | 302
- Creating Addresses from Source | 302

The following procedures provides various methods using which you can choose a firewall source end point:

### Adding an End Point as Firewall Source

View and select the source end point from the complete list of addresses, sites, site groups, zones, or departments. You can also select the **Internet** option which denotes all in-coming traffic from outside your network.

**NOTE:** When you select **Any** address as a source, it implies traffic originating within the network.

**NOTE:**

The following conditions apply when you select **Internet** as a source end point:

- When **Internet** is not chosen as a source end point, it is implied that the traffic is originating within the network.
- If you chose **Internet** as a source, you cannot add other sites, site groups or departments as a source end point along with **Internet**.
- If you chose **Internet** as a source, the destination end point must be a site, site group, or department.

1. Click the **Source** field. A list of relevant endpoints are displayed.
2. Click on **View more results** link provided at the bottom of the source end points. The complete list of addresses, departments, users, sites, site groups, and zones is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, users, department, or site group end point. You cannot edit a site end point.
4. Click check mark icon (✓) to select the end point as a source.

## Selecting Firewall Source Using Abbreviations

Enter an abbreviation in the **Source** field to select the source end point from a filtered list of source endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of departments, enter **DEPT** or **dept**.
- To view a filtered list of sites, enter **SITE** or **site**.
- To view a filtered list of site groups, enter **STGP** or **stgp**.
- To view a filtered list of user ids, enter **USER** or **user**.
- To view a filtered list of zones, enter **ZONE** or **zone**.

Click the endpoints in the filtered list to select them. You can also select the end point from the complete list of addresses, departments, users, sites, and site groups. See [“Adding an End Point as Firewall Source” on page 300](#).

## Selecting a Firewall Source from the End Points Panel

You can select a firewall source end point from the **End Points** panel. Alternately, you can create a new firewall source end point from the **End Points** panel, see [“Creating and Selecting a Firewall Source from the End Points Panel” on page 302](#)

To select an firewall source end point from the from the **End Points** panel:

1. Click on the **Source** field.
2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, departments, users, sites, site groups, and zones.

3. (Optional) To view more information about a source end point, click the details icon on the right of the end point. To edit the source end point, click the edit icon (pencil symbol) on the right of the end point.

**NOTE:** You can only edit or view details of a source end point if these options appear on right side of the end point when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the end point as a source.

## Creating and Selecting a Firewall Source from the End Points Panel

To create an new source end point from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of end point you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new end point.

- To create a new address, see [“Creating Addresses or Address Groups” on page 573](#).
- To create a site or site group, see [“Creating Site Groups” on page 145](#).

After the end point is created, it appears in the **End Points** panel.

2. Click the check mark icon (✓) to add the new end point as a source.

## Creating Addresses from Source

You can use one of the following ways to create a new address from the **Source** field and use the newly created address as a source end point:

- Type the address directly in the **Source** field. If the address is valid, it is created immediately and added as a source end point.
- Create an address from the **Source** field, using the following steps:
  1. In the **Source** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
  2. Click **Add new address** to create a new address.  
The **Create Addresses** page appears.
  3. Configure the new address. See [“Creating Addresses or Address Groups” on page 573](#).
  4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the source. Select the new address to add it to the source.

## RELATED DOCUMENTATION

[Selecting Firewall Destination | 303](#)

[Adding Firewall Policy Intents | 291](#)

---

[Firewall Policy Overview | 285](#)

---

[About the Firewall Policy Page | 287](#)

---

[Editing, Cloning, and Deleting Firewall Policy Intents | 297](#)

---

## Selecting Firewall Destination

### IN THIS SECTION

- [Adding an End Point as Firewall Destination | 303](#)
- [Selecting Firewall Destination Using Abbreviations | 304](#)
- [Selecting a Firewall Destination from the End Points Panel | 304](#)
- [Creating and Selecting a Firewall Destination from the End Points Panel | 305](#)
- [Creating Addresses from Destination | 305](#)

The following procedures provides various methods using which you can choose a firewall destination end point:

### Adding an End Point as Firewall Destination

View and select the end point from the complete list of addresses, applications, departments, services, sites, site groups, or zones.

#### NOTE:

- When you choose **Any** address or service as the destination, it implies that traffic is flowing outside the network unless a site or department is mentioned explicitly.
- Unless you choose a site, site group, or department as a destination end point, it is implied the traffic will flow outside your network.

1. Click on **Destination**. A list of relevant end points are displayed.
2. Click on **View more results** link provided at the bottom of the destination end points. The complete list of addresses, departments, sites, and site groups is displayed in the **End Points** panel on the right.

3. (Optional) Click the edit icon to edit the address, department, or site group end point. You cannot edit a site end point.
4. Click check mark icon (✓) to select the end point as a destination.

### Selecting Firewall Destination Using Abbreviations

Enter an abbreviation in the **Destination** field to select the destination end point from a filtered list of destination endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of addresses, enter **APPS** or **apps**.
- To view a filtered list of departments, enter **DEPT** or **dept**.
- To view a filtered list of services, enter **SVCS** or **svcs**.
- To view a filtered list of sites, enter **SITE** or **site**.
- To view a filtered list of site groups, enter **STGP** or **stgp**.
- To view a filtered list of zones, enter **ZONE** or **zone**.

Click the endpoints in the filtered list to select them. You can also select the end point from the complete list of addresses, departments, sites, and site groups. See [“Adding an End Point as Firewall Destination” on page 303](#).

### Selecting a Firewall Destination from the End Points Panel

You can select a firewall destination end point from the **End Points** panel. Alternately, you can create a new firewall destination end point from the **End Points** panel, see [“Creating and Selecting a Firewall Destination from the End Points Panel” on page 305](#).

To select an firewall destination end point from the from the **End Points** panel:

1. Click on the **Destination** field.
2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, departments, sites, site groups, or zones.

3. (Optional) To view more information about a destination end point, click the details icon on the right of the end point. To edit the destination end point, click the edit icon (pencil symbol) on the right of the end point.

**NOTE:** You can only edit or view details of a destination end point if these options appear on right side of the end point when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the end point as a destination.

## Creating and Selecting a Firewall Destination from the End Points Panel

To create an new destination end point from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of end point you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new end point.

- To create a new address, see [“Creating Addresses or Address Groups” on page 573](#).
- To create a site or site group department, see [“Creating Site Groups” on page 145](#).

After the end point is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new end point as a destination.

## Creating Addresses from Destination

You can use one of the following ways to create a new address from the **Destination** and use the newly created address as a destination end point:

- Type the address directly in the **Destination** field. If the address is valid, it is created immediately and added as a destination end point.
- Create an address from the **Destination** field, using the following steps:
  1. In the **Destination** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
  2. Click **Add new address** to create a new address.

The **Create Addresses** page appears.

3. Configure the new address. See [“Creating Addresses or Address Groups” on page 573](#).
4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the destination. Select the new address to add it to the destination.

## RELATED DOCUMENTATION

[Adding Firewall Policy Intents | 291](#)

[Firewall Policy Overview | 285](#)

[About the Firewall Policy Page | 287](#)

[Editing, Cloning, and Deleting Firewall Policy Intents | 297](#)

## Firewall Policy Examples

### IN THIS SECTION

- [Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B | 308](#)
- [Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B | 310](#)
- [Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B | 313](#)
- [Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A | 314](#)
- [Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments | 316](#)
- [Example 6: Firewall Policy that Denies Access to Social Networking Sites | 324](#)
- [Example 7: Firewall Policy that Controls Access to an Address over the Internet \(HTTP\) | 327](#)
- [Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service | 333](#)
- [Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B | 335](#)
- [Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A | 338](#)
- [Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled | 342](#)
- [Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive. | 345](#)

This topic provides information on how firewall policy intents that you define as part of your firewall policy is handled by Contrail Service Orchestration (CSO), using various examples. Each of the examples provide



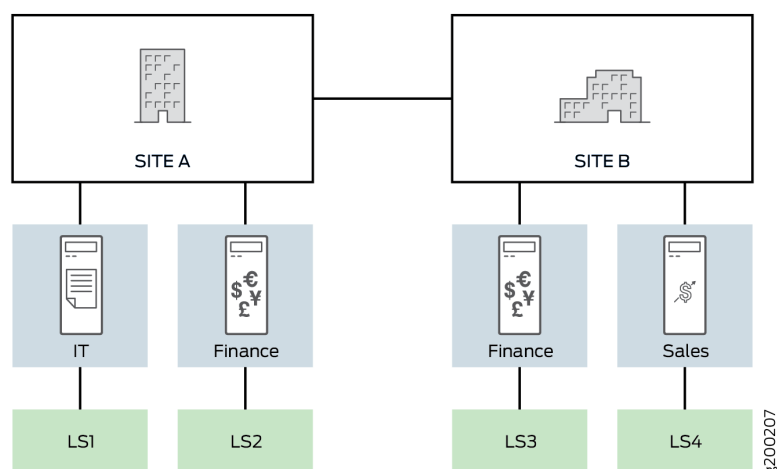
detailed explanation about how a firewall policy intent defined through the CSO GUI resolves into configuration in the system.

**NOTE:** For more information, see [“Firewall Policy Overview” on page 285](#) and [“Adding Firewall Policy Intents” on page 291](#).

For easier understanding, all the examples have been defined to use the topology in illustrated in [Figure 10 on page 307](#). In this topology, there are two sites—site A and site B. Each site has two departments defined as follows:

- Site A - IT (LAN segment LS1) and Finance (LAN segment LS2).
- Site B - Finance (LAN segment LS3) and Sales (LAN segment LS4).

**Figure 10: Topology Diagram**



The following definitions are applicable to all the examples:

- While creating a site, you can designate some of the WAN interfaces to be breakout interfaces. These WAN interfaces can carry both site-to-site traffic (through the trust zone) and breakout traffic (through the untrust zone). The WAN interfaces can also be designated exclusively for carrying breakout traffic.
- A trust zone refers to the overlay interface that contains all the GRE tunnel interfaces, such as gr-0/0/0.1, gr-0/0/0.2, and IPsec interfaces, such as st0.1, st0.2 created between the sites.
- An untrust zone refers to the underlay interfaces (underlying physical interfaces) such as ge-0/0/0, ge-0/0/1.

- If you select an address or a service as a destination endpoint, CSO considers it as an address or service hosted on the Internet, unless the selected address or service is associated with a site.
- [Table 91 on page 308](#) captures the addresses associated with the LAN segments used in the topology illustrated in [Figure 10 on page 307](#).

**Table 91: LAN Segments Definition**

Site	Department	LAN Segment	LAN Segment Address
site A	IT	LS1	192.0.2.0/24
site A	Finance	LS2	192.168.1.0/24
site B	Finance	LS3	198.51.100.0/24
site B	Sales	LS4	203.0.113.0/24

The following examples help you understand the creation of intent-based firewall policies for various traffic scenarios across sources and destinations.

### Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B

Define a firewall policy that permits traffic from the departments in site A to the departments in site B.

[Table 92 on page 308](#) shows the firewall policy intent that is defined:

**Table 92: Firewall Policy Intent Definition for Example - 1**

Source	Destination	Action
site A	site B	Permit

[Table 93 on page 308](#) shows how this firewall policy intent is resolved:

**Table 93: Firewall Policy Intent Resolution for Example - 1**

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Finance	[LS2]	Trust	[LS3, LS4]	Any	Intent 1__0
	IT	[LS1]	Trust	[LS3, LS4]	Any	Intent 1__1

Table 93: Firewall Policy Intent Resolution for Example - 1 (continued)

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site B	Trust	[LS3, LS4]	Sales	[LS2]	Any	Intent 1__0
	Trust	[LS3, LS4]	Finance	[LS1]	Any	Intent 1__1

### Configuration Output Sample

Sample of configuration that permits traffic from departments in site A to the departments in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone FINANCE to-zone trust {
    policy Intent_1__0 {
        match {
            source-address ls-192.168.1.0/24-SP50-L2;
            destination-address [ls-198.51.100.0/24-SP50-L3,
ls-203.0.113.0/24-SP50-L4];
            application any;
        }
        then {
            permit;
        }
    }
}

from-zone IT to-zone trust {
    policy Intent_1__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address [ls-198.51.100.0/24-SP50-L3,
ls-203.0.113.0/24-SP50-L4];
            application any;
        }
        then {
            permit;
        }
    }
}

```

Sample of configuration that permits traffic from departments in site B to the departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone trust to-zone SALES {
  policy Intent_1__0 {
    match {
      source-address [ls-198.51.100.0/24-SP50-L3,
        ls-203.0.113.0/24-SP50-L4];
      destination-address ls-192.0.2.0/24-S42-L1;
      application any;
    }
    then {
      permit;
    }
  }
}

from-zone trust to-zone FINANCE {
  policy Intent_1__1 {
    match {
      source-address [ls-198.51.100.0/24-SP50-L3,
        ls-203.0.113.0/24-SP50-L4];
      destination-address ls-192.168.1.0/24-SP50-L2;
      application any;
    }
    then {
      permit;
    }
  }
}

```

## Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B

Define a firewall policy that permits all the department in site A and site B access to Internet.

[Table 94 on page 310](#) shows the firewall policy intent that is defined:

**Table 94: Firewall Policy Intent Definition for Example - 2**

Source	Destination	Action
site A	http, https, icmp-ping, dns	Permit
site B	http, https, icmp-ping, dns	Permit

Table 95 on page 311 shows how this firewall policy intent is resolved:

Table 95: Firewall Policy Intent Resolution for Example - 2

Site	Source Department	Source Address	Zone	Destination Address	Service	Intent Created
site A	Finance	[LS2]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	IT	[LSI]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__1
site B	Sales	[LS4]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__0
	Finance	[LS3]	Untrust	Any	http, https, icmp-ping, dns	Intent 1__1

### Configuration Output Sample

Sample of configuration that permits Internet access to all departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application [junos-http junos-dns-tcp junos-https
                  junos-icmp-ping];
    }
    then {
      permit;
    }
  }
}

```

```

from-zone IT to-zone untrust {
  policy Intent_1__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application [junos-http junos-dns-tcp junos-https
                  junos-icmp-ping];
    }
    then {
      permit;
    }
  }
}
policy-rematch;

```

Sample of configuration that permits Internet access to all departments in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Sales to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-203.0.113.0/24-SP50-L4;
      destination-address any;
      application [junos-http junos-dns-tcp junos-https
                  junos-icmp-ping];
    }
    then {
      permit;
    }
  }
}
from-zone Finance1 to-zone untrust {
  policy Intent_1__1 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application [junos-http junos-dns-tcp junos-https
                  junos-icmp-ping];
    }
    then {

```

```

        permit;
    }
}
policy-rematch;

```

### Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B

Define a firewall policy that permits any public Internet address access to a sales application hosted by the Sales department in site B.

**NOTE:** For this example, breakout is not enabled and MPLS link type is used.

Table 96 on page 313 shows the firewall policy intent that is defined:

Table 96: Firewall Policy Intent Definition for Example - 3

Source	Destination	Action
Internet	Sales, site B	Permit

Table 97 on page 313 shows how this firewall policy intent is resolved:

Table 97: Firewall Policy Intent Resolution for Example - 3

Source Address	Zone	Destination Address	Service	Intent Created
Any public Internet address	Trust to Sales (No breakout)	[LS4]	Any	Intent 1__0

### Configuration Output Example

Sample of configuration that permits any public Internet address to access the Sales department in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone untrust to-zone Sales {
  policy Intent_1__0 {
    match {
      source-address any;
      destination-address ls-203.0.113.0/24-SP50-L4;
      application any;
    }
    then {
      permit;
    }
  }
}

```

#### Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A

Define a firewall policy that permits all departments in site A access to Facebook.

[Table 98 on page 314](#) shows the firewall policy intent that is defined:

**Table 98: Firewall Policy Intent Definition for Example - 4**

Source	Destination	Action
site A	Facebook	Permit

[Table 99 on page 314](#) shows how this firewall policy intent is resolved:

**Table 99: Firewall Policy Intent Resolution for Example - 4**

Site	Source Address	Zone	Destination Address	Service	Intent Created	Application Firewall Profile
site A	[LS2]	Untrust	Facebook	Any	Intent 1__0	AppFwProfile_0
site A	[LS1]	Untrust	Facebook	Any	Intent 1__1	AppFwProfile_0

#### Configuration Output Example



Sample of configuration that controls access to Facebook for site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

from-zone IT to-zone untrust {
  policy Intent_1__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

policy-rematch;
```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

application-firewall {
  rule-sets AppFwProfile_0 {
    rule rule-1 {
      match {
        dynamic-application junos:FACEBOOK-APP;
        ssl-encryption any;
      }
      then {
        permit;
      }
    }
    default-rule {
      deny;
    }
  }
}

```

### Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments

Define a firewall policy that controls access to specific applications from various departments, with the following intents:

- The finance departments located in site A and site B (which are in different geographical locations) are permitted to access the news applications BBC and CNN.
- The IT department located in site A is denied access to the news applications BBC and CNN.
- Access to Telnet and SSH applications is given only to the finance departments.
- Access to Telnet and SSH applications is denied to all departments, except for the finance department.

Table 100 on page 316 shows the firewall policy intents that are to fulfil this requirement:

**Table 100: Firewall Policy Intent Definition for Example - 5**

Source	Destination	Action
Finance department, site A and Finance department, site B	BBC and CNN	Permit
IT department, site A	BBC and CNN	Deny
Finance department, site A and Finance department, site B	Telnet and SSH	Permit

Table 100: Firewall Policy Intent Definition for Example - 5 (continued)

Source	Destination	Action
Any (All addresses except the finance department)	Telnet and SSH	Deny

**NOTE:** The number of intents depends on the number of source sites within the given department and the number of destination sites.

Table 101 on page 317 shows how this firewall policy intent is resolved:

Table 101: Firewall Policy Intent Resolution for Example - 5

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
Finance	[LS2]	Trust/Untrust	Any	Any	AppFwProfile_1  Permit: CNN/BBC  Def. Rule : Permit
Finance	[LS3]	Trust/Untrust	Any	Any	AppFwProfile_1  Permit: CNN/BBC  Def. Rule : Permit
IT	[LS1]	Trust/Untrust	Any	Any	AppFwProfile_3  Deny: CNN/BBC  Def. Rule : Deny
Finance department, site A and Finance department, site B	[LS2, LS3]	Trust/Untrust	Any	Telnet, SSH	AppFwProfile_1-1  Permit: Telnet/SSH  Def. Rule : Deny

Table 101: Firewall Policy Intent Resolution for Example - 5 (continued)

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT department, site A	[LS1]	Trust/Untrust	Any	Telnet, SSH	AppFwProfile_3-1  Deny: Telnet/SSH  Def. Rule : Deny

### Configuration Output Example

Sample of configuration that controls access to specific applications for various departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone trust {
  policy Intent_3 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application [junos-telnet junos-ssh];
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1-1;
          }
        }
      }
    }
  }
}
policy Intent_1 {
  match {
    source-address ls-192.168.1.0/24-SP50-L2;
    destination-address any;
    application any;
  }
  then {
    permit {

```

```

        application-services {
            application-firewall {
                rule-set AppFwProfile_1;
            }
        }
    }
}
policy Intent_4__0 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
    then {
        permit;
    }
}
from-zone IT to-zone trust {
    policy Intent_4__1-1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address any;
            application [junos-telnet junos-ssh];
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_3-1;
                    }
                }
            }
        }
    }
}
policy Intent_2 {
    match {
        source-address ls-192.0.2.0/24-S42-L1;
        destination-address any;
        application any;
    }
}

```



```

        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_1 {
    rule rule-3 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_3-1 {
    rule rule-4 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

```

Sample of configuration that controls access to specific applications for various departments in site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone trust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_3 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application [ junos-telnet junos-ssh ];
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1-1;
          }
        }
      }
    }
  }
  policy Intent_1 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1;
          }
        }
      }
    }
  }
}

```



```

        }
    }
}
policy Intent_4__1 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
    then {
        deny;
    }
}
}
from-zone Sales to-zone trust {
    policy Intent_4__0 {
        match {
            source-address any;
            destination-address any;
            application [junos-telnet junos-ssh];
        }
        then {
            deny;
        }
    }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1-1 {
    rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}

```

```
    }
rule-sets AppFwProfile_1 {
  rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
    match {
      dynamic-application [junos:BBC junos:CNN];
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}
```

**Example 6: Firewall Policy that Denies Access to Social Networking Sites**

Define a firewall policy that denies access to networking sites such as Facebook and Twitter (defined as application group Social Networking) to the IT and finance departments located in Site A.

Table 102 on page 324 shows the firewall policy intent that is needed to fulfil this requirement:

**Table 102: Firewall Policy Intent Definition for Example - 6**

Source	Destination	Action
IT and Finance, site A	Application group Social Networking (Facebook and Twitter)	Deny

**NOTE:** Add site A if the IT or finance departments are present in different sites, but you only want to apply this firewall policy intent to the IT or finance departments present in site A.

Table 103 on page 325 shows how this firewall policy intent is resolved:

Table 103: Firewall Policy Intent Resolution for Example - 6

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
Finance	[LS2]	Trust/Untrust	Any	Any	AppFwProfile_0  Deny: Social Networking (Apps)  Def. Rule : Deny
IT	[LS1]	Trust/Untrust	Any	Any	AppFwProfile_1  Deny: Social Networking (Apps)  Def. Rule : Deny

### Configuration Output Example

Sample of configuration that denies access to social networking sites for departments in site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone IT to-zone untrust {
  policy Intent_1__0 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

```

```

    }
  }
  from-zone Finance to-zone untrust {
    policy Intent_1__1 {
      match {
        source-address ls-192.168.1.0/24-SP50-L2;
        destination-address any;
        application any;
      }
      then {
        permit {
          application-services {
            application-firewall {
              rule-set AppFwProfile_0;
            }
          }
        }
      }
    }
  }
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

application-firewall {
  rule-sets AppFwProfile_0 {
    rule rule-b7e4ed02-e196-400a-88bf-f1de8973d30c-appFwRule {
      match {
        dynamic-application-group Socialnetwork;
        ssl-encryption any;
      }
      then {
        deny;
      }
    }
    default-rule {
      deny;
    }
  }
}

```

}

### Example 7: Firewall Policy that Controls Access to an Address over the Internet (HTTP)

Define a firewall policy that controls access to an address over the Internet (HTTP) for various sites or site groups with the following intents:

- IP address prefix of site A and site B are permitted to access example.com.
- IP address prefix of site group Q1 are denied access to example-one.com. Site group Q1 consists of site A and site B.

Table 104 on page 327 shows the firewall policy intents that are needed to fulfil this requirement:

**Table 104: Firewall Policy Intent Definition for Example - 7**

Source	Service	Destination	Action
IP address prefix, site A and IP-Prefix, site B	HTTP	www.example.com	Permit
IP address prefix, site group Q1	HTTP	www.example-one.com	Deny

Table 105 on page 327 shows how this firewall policy intent is resolved:

**Table 105: Firewall Policy Intent Resolution for Example - 7**

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT, Finance departments in site A	[LS1, LS2]	Trust/Untrust	www.example.com	Any	AppFwProfile_0  Permit: HTTP  Def. Rule : Deny
Finance, Sales departments in site B	[LS3, LS4]	Trust/Untrust	www.example.com	Any	AppFwProfile_1  Permit: HTTP  Def. Rule : Deny

Table 105: Firewall Policy Intent Resolution for Example - 7 (continued)

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
IT, Finance departments in site A	[LS1, LS2]	Trust/Untrust	www.example-one.com	Any	AppFwProfile_2  Deny: HTTP  Def. Rule : Deny
Finance, Sales departments in site B	[LS3, LS4]	Trust/Untrust	www.example-one.com	Any	AppFwProfile_3  Deny: HTTP  Def. Rule : Deny

### Configuration Output Example

Sample of configuration that controls access to an address over the Internet (HTTP) for site A.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address www.example.com;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}
policy Intent_1__0 {
  match {
    source-address ls-192.168.1.0/24-SP50-L2;

```

```

        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

from-zone IT to-zone untrust {
    policy Intent_4__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address addr2;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
        }
    }
}

policy Intent_1__1 {
    match {
        source-address ls-192.0.2.0/24-S42-L1;
        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

```

```

    }
  }
}
}
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1 {
  rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
    match {
      dynamic-application junos:YOUTUBE;
      ssl-encryption any;
    }
    then {
      deny;
    }
  }
  default-rule {
    deny;
  }
}
rule-sets AppFwProfile_0 {
  rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bffa3-appFwRule {
    match {
      dynamic-application junos:CNN;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
}
rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
  match {
    dynamic-application junos:YOUTUBE;
    ssl-encryption any;
  }
  then {

```



```

        deny;
    }
}
default-rule {
    deny;
}
}

```

Sample of configuration that controls access to an address over the Internet (HTTP) for site B.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
    policy Intent_4__1 {
        match {
            source-address ls-198.51.100.0/24-SP50-L3;
            destination-address addr2;
            application junos-http;
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
        }
    }
}
policy Intent_1__1 {
    match {
        source-address ls-198.51.100.0/24-SP50-L3;
        destination-address addr2;
        application junos-http;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_1;
                }
            }
        }
    }
}

```

```

    }
  }
}
from-zone Sales to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-203.0.113.0/24-SP50-L4;
      destination-address addr2;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
  policy Intent_1__0 {
    match {
      source-address ls-203.0.113.0/24-SP50-L4;
      destination-address addr2;
      application junos-http;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_1;
          }
        }
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1 {
  rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {

```

```

        match {
            dynamic-application junos:YOUTUBE;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

rule-sets AppFwProfile_0 {
    rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bffa3-appFwRule {
        match {
            dynamic-application junos:CNN;
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    rule rule-ca2354d6-a7ba-488e-8c5a-91cbddfb9583-appFwRule {
        match {
            dynamic-application junos:YOUTUBE;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}

```

### Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service

Define a firewall policy where a specific IP address that belongs to the IT department is permitted or denied the use of HTTP or FTP as a service.

[Table 106 on page 334](#) shows the firewall policy intents that are needed to fulfil this requirement:

Table 106: Firewall Policy Intent Definition for Example - 8

Source	Service	Destination	Action
192.0.2.0	HTTP	example.com	Permit
192.0.2.0	FTP	example.com	Deny

Table 107 on page 334 shows how this firewall policy intent is resolved:

Table 107: Firewall Policy Intent Resolution for Example - 8

Source Department	Source Address	Zone	Destination Address	Service
IT, site A	192.0.2.0	Trust/Untrust	example.com	FTP
IT, site A	192.0.2.0	Trust/Untrust	example.com	HTTP

### Configuration Output Example

Sample of configuration that allows access to HTTP

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone IT to-zone trust {
  policy Intent_1__1 {
    match {
      source-address 192.0.2.0;
      destination-address example.com;
      application junos-ftp;
    }
    then {
      deny;
    }
  }
}
policy Intent_4__1 {
  match {
    source-address 192.0.2.0;
    destination-address example.com;
    application junos-http;
  }
}

```

```

        then {
            permit;
        }
    }
}
policy-rematch;

```

### Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B

Define a firewall policy that denies access to BitTorrent for the Finance departments in site A and Site B.

[Table 108 on page 335](#) shows the firewall policy intents that are needed to fulfil this requirement:

**Table 108: Firewall Policy Intent Definition for Example - 9**

Source	Destination	Action
site A, Finance department	BitTorrent	Deny
site B, Finance department	BitTorrent	Deny

[Table 109 on page 335](#) shows how this firewall policy intent is resolved:

**Table 109: Firewall Policy Intent Resolution for Example - 9**

Site	Source Address	Zone	Destination Application	Service	Application Firewall Profile
Finance department, site A	[LS2]	Trust/Untrust	BitTorrent	Any	AppFwProfile_0 Deny: BitTorrent Def. Rule : Deny
Finance department, site B	[LS3]	Trust/Untrust	BitTorrent	Any	AppFwProfile_0 Deny: BitTorrent Def. Rule : Deny

### Configuration Output Example

Sample of configuration that allows site A access to BitTorrent.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_1 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
      log {
        session-init;
        session-close;
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```
rule-sets AppFwProfile_0 {
  rule rule-2226740d-03a9-483c-b315-eddc9ae8619a-appFwRule {
    match {
      dynamic-application junos:BITTORRENT;
      ssl-encryption any;
    }
    then {
      deny;
    }
  }
  default-rule {
    deny;
  }
}
```

Sample of configuration that allows site B to access to BitTorrent.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```
from-zone Financel to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_4 {
    match {
      source-address ls-198.51.100.0/24-SP50-L3;
      destination-address any;
      application any;
    }
    then {
      permit {
        application-services {
          application-firewall {
```

```

        rule-set AppFwProfile_0;
    }
}
}
log {
    session-init;
    session-close;
}
}
}
}
policy-rematch;
```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_0 {
    rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
        match {
            dynamic-application junos:BITTORRENT;
            ssl-encryption any;
        }
        then {
            deny;
        }
    }
    default-rule {
        deny;
    }
}
```

**Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A**

Define a firewall policy where the users that are a part of user group A are provided access only to Facebook, and no other applications. User group A consists of users located in site A.

[Table 110 on page 338](#) shows the firewall policy intent that is needed to fulfil this requirement:

**Table 110: Firewall Policy Intent Definition for Example - 10**

Source	Destination	Action
user group A, site A	Facebook	Permit



Table 111 on page 339 shows how this firewall policy intent is resolved:

**Table 111: Firewall Policy Intent Resolution for Example - 10**

Site	User/User Group	Source Address Range	Destination Address	Application
site A	user group A	192.0.2.0 to 192.0.2.20	Any	Facebook

### Configuration Output Example

Sample of configuration that allows users in user group A access to Facebook.

The hierarchy level for the following configuration sample is [\[edit security policies\]](#).

```

from-zone Finance to-zone untrust {
  policy appQoe-36600-Permit-rule {
    match {
      source-address any;
      destination-address any;
      application appQoe-36000;
    }
    then {
      permit;
    }
  }
  policy Intent_4__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
      source-identity "USERFW.LOCAL\Cert Publishers";
    }
    then {
      permit {
        application-services {
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

```

```

        log {
            session-init;
            session-close;
        }
    }
}

from-zone IT to-zone untrust {
    policy appQoe-36600-Permit-rule {
        match {
            source-address any;
            destination-address any;
            application appQoe-36000;
        }
        then {
            permit;
        }
    }
    policy Intent_4__1 {
        match {
            source-address ls-192.0.2.0/24-S42-L1;
            destination-address any;
            application any;
            source-identity "USERFW.LOCAL\Cert Publishers";
        }
        then {
            permit {
                application-services {
                    application-firewall {
                        rule-set AppFwProfile_0;
                    }
                }
            }
            log {
                session-init;
                session-close;
            }
        }
    }
}

policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```
rule-sets AppFwProfile_0 {
  rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
    match {
      dynamic-application junos:FACEBOOK-APP;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}
```

The hierarchy level for the following configuration sample is **[edit services user-identification identity-management]**.

```
connection {
  connect-method https;
  port 443;
  primary {
    address 10.213.50.50;
    client-id 1234;
    client-secret "$ABC123"; ## SECRET-DATA
  }
  token-api oauth_token/oauth;
  query-api user_query/v2;
}
batch-query {
  items-per-batch 200;
  query-interval 5;
}
ip-query {
  query-delay-time 15;
}
```

### Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled

Define a firewall policy where the User B located in Site A is provided access only to YouTube with UTM enabled. The user does not have permission to access any other applications.

Table 112 on page 342 shows the firewall policy intent that is needed to fulfil this requirement:

**Table 112: Firewall Policy Intent Definition for Example - 11**

Source	Destination	Action
user B, site A	YouTube	Permit

Table 113 on page 342 shows how this firewall policy intent is resolved:

**Table 113: Firewall Policy Intent Resolution for Example - 11**

Site	Source Address	User/User Group	Destination Address	UTM	Application
site A	192.0.2.22	user B	Any	Enabled	Facebook

### Configuration Output Example

Sample of configuration that allows user B in site A access to YouTube, with UTM enabled.

The hierarchy level for the following configuration sample is **[edit security policies]**.

```

from-zone Finance to-zone untrust {
  policy Intent_4__0 {
    match {
      source-address ls-192.168.1.0/24-SP50-L2;
      destination-address any;
      application any;
      source-identity "userfw.local\CS01";
    }
    then {
      permit {
        application-services {
          utm-policy testUTM;
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
    }
  }
}

```

```

    }
  }
  log {
    session-init;
    session-close;
  }
}
}
}
from-zone IT to-zone untrust {
  policy Intent_4__1 {
    match {
      source-address ls-192.0.2.0/24-S42-L1;
      destination-address any;
      application any;
      source-identity "userfw.local\CS01";
    }
    then {
      permit {
        application-services {
          utm-policy testUTM;
          application-firewall {
            rule-set AppFwProfile_0;
          }
        }
      }
      log {
        session-init;
        session-close;
      }
    }
  }
}
policy-rematch;

```

The hierarchy level for the following configuration sample is **[edit security utm]**.

```

feature-profile {
  web-filtering {
    type juniper-local;
  }
}

```

```

    }
  }
  utm-policy testUTM {
    web-filtering {
      http-profile junos-wf-local-default;
    }
    anti-spam {
      smtp-profile junos-as-defaults;
    }
  }
  traffic-options {
    sessions-per-client {
      over-limit log-and-permit;
    }
  }
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_0 {
  rule rule-00f3879c-f3d7-4cb3-89b6-78328e3bff38-appFwRule {
    match {
      dynamic-application junos:FACEBOOK-APP;
      ssl-encryption any;
    }
    then {
      permit;
    }
  }
  default-rule {
    deny;
  }
}

```

The hierarchy level for the following configuration sample is **[edit services user-identification identity-management]**.

```

connection {
  connect-method https;
  port 443;
  primary {
    address 10.213.50.50;
  }
}

```

```

    client-id 1234;
    client-secret "$ABC123"; ## SECRET-DATA
  }
  token-api oauth_token/oauth;
  query-api user_query/v2;
}
batch-query {
  items-per-batch 200;
  query-interval 5;
}
ip-query {
  query-delay-time 15;
}

```

### Example 12: Firewall Policy that blocks access to Internet and allow access to Google Drive.

The following section provides a sample firewall policy to block access to Internet and allow access to Google Drive. The firewall policy has one enterprise-based intent and one zone-based intent.

An enterprise-based intent to block access to Internet is provided in [Table 114 on page 345](#).

**Table 114: Sample Enterprise-based Intent**

Rule Name	Source Endpoint	Destination Endpoint	Action
EnterpriseIntent_1	Engg (Department)	Internet	Deny

A zone-based intent to allow access to Google drive is provided in [Table 115 on page 345](#).

**Table 115: Sample Zone based Intent**

Rule Name	Source Endpoint	Destination Endpoint	Action
ZoneIntent_1	Engg (Zone)	untrust(zone), google-drive	Allow

The intents in [Table 114 on page 345](#) and [Table 115 on page 345](#) result in firewall rules order that is provided in [Table 116 on page 345](#).

**Table 116: Sample firewall rule**

Rule Name	Rule Order	Source Endpoint	Destination Endpoint	Action
ZoneIntent_1	1	Engg (Zone)	untrust(zone), google-drive	Allow
EnterpriseIntent_1	2	Engg (Department)	Internet	Deny

## RELATED DOCUMENTATION

---

[Firewall Policy Overview | 285](#)

---

[Adding Firewall Policy Intents | 291](#)

---

## Firewall Policy Schedules Overview

A schedule allows a policy to be active for a specified duration. If you want a policy to be active during a scheduled time, you must first create a schedule for that policy or link the policy to an existing schedule. When a schedule timeout expires, the associated policy is deactivated and all sessions associated with the policy are also timed out.

If a policy contains a reference to a schedule, that schedule determines when the policy is active. When a policy is active, it can be used as a possible match for traffic. A schedule lets you restrict access to, or remove a restriction from a resource, for a period of time.

A schedule uses the following guidelines:

- A schedule can have multiple policies associated with it; however, a policy cannot be associated with multiple schedules.
- A policy remains active as long as the schedule it refers to is also active.

A schedule can be active during a single time slot, as specified by a start date and time, and a stop date and time.

- A schedule can be active forever (recurrent), but only as specified by the daily schedule. The schedule on a specific day (time slot) takes priority over the daily schedule.
- A scheduler can be active during a time slot, as specified by the weekday schedule.
- A scheduler be active within two different time slots (daily or for a specified duration).

## RELATED DOCUMENTATION

---

[About the Firewall Policy Schedules Page | 347](#)

---

[Firewall Policy Examples | 306](#)

---

[Creating Schedules | 348](#)

---

[Editing, Cloning, and Deleting Schedules | 350](#)

---



# About the Firewall Policy Schedules Page

To access this page, select **Configuration > Firewall > Schedules**.

The **Firewall Policy Schedules** page enables you to create, modify, clone, and delete schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

## Tasks You Can Perform

You can perform the following tasks from this page:

- Create a firewall policy schedule. See [“Creating Schedules” on page 348](#).
- Modify, clone, or delete a firewall policy schedule. See [“Editing, Cloning, and Deleting Schedules” on page 350](#).
- View the configured parameters of a schedule. Click the details icon that appears when you hover over the name of an image or click **More > Detailed View**.
- Show or hide columns about the firewall policy schedule. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific firewall policy schedule. Click the Search icon in the top right corner of the page to search for a firewall policy schedule.

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

The search results are displayed on the same page.

## Field Descriptions

[Table 117 on page 347](#) provides guidelines on using the fields on the **Firewall Policy Schedules** page.

**Table 117: Fields on the Firewall Policy Schedules Page**

Field	Description
Name	Name of the schedule; maximum length is 63 characters.
Description	Description for the schedule; maximum length is 900 characters.
Start Date	The date and time from when the schedule comes into effect.
End Date	The date and time from when the schedule ends.
Second Start Date	The second date and time from when the schedule comes into effect.

Table 117: Fields on the Firewall Policy Schedules Page (*continued*)

Field	Description
Second End Date	The second date and time from when the schedule ends.

## RELATED DOCUMENTATION

[Firewall Policy Schedules Overview | 346](#)

[Firewall Policy Examples | 306](#)

[Creating Schedules | 348](#)

[Editing, Cloning, and Deleting Schedules | 350](#)

## Creating Schedules

Use the **Create Schedules** page to create schedules. A schedule allows you to restrict access to a resource, or remove a restriction to a resource, for a specified period of time.

To configure a schedule:

1. Select **Configuration > Firewall > Schedules**.

The **Firewall Policy Schedules** page appears.

2. Click the add icon (+).

The **Create Schedules** page appears.

3. Complete the configuration of the schedule according to the guidelines provided in [Table 118 on page 349](#).

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

A new schedule is created. You can use this schedule to activate firewall policies for the times and dates configured in your schedules.

[Table 118 on page 349](#) provides guidelines on using the fields to create a schedule.

Table 118: Fields on the Create Schedules Page

Field	Description
<b>General Information</b>	
Name	Required. Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
<b>Dates</b>	
Date Range	<p>Select <b>Ongoing</b> if you want your schedules to always be active.</p> <p>Select <b>Custom</b> to configure two sets of start and end dates for a single schedule. For the first set, enter dates in the <b>Start Date</b> and <b>End Date</b> fields. You must enter the days in MM/DD/YYYY format.</p> <p>For the second set of the schedule, enter the start date in the <b>Second Start Date</b> field and enter the end date in the <b>Second End Date</b> field.</p>
<b>Times</b>	
Time Ranges	Create a schedule to be active daily or for any specific times of the day.
Daily Options	<p>Select <b>Daily</b> to make the schedule applicable daily.</p> <p>Select <b>Custom</b> to enter specific days and times. Click on a specific day to specify time options for an entire day, to exclude a specific day, or to enter time ranges for the selected day. You must enter the time in HH:MM:SS format.</p> <p>For example, if you click on Monday, you get a dialog box that allows you to specify whether you want the schedule to be active all day Monday, exclude Monday from the schedule, or have the schedule be active at specific times.</p> <p>Select <b>Specify the same time for all days</b> to enter a date and time that is applicable for all days.</p>

## RELATED DOCUMENTATION

[Firewall Policy Schedules Overview | 346](#)
[About the Firewall Policy Schedules Page | 347](#)
[Firewall Policy Examples | 306](#)

## Editing, Cloning, and Deleting Schedules

### IN THIS SECTION

- [Editing Schedules | 350](#)
- [Cloning Schedules | 350](#)
- [Deleting Schedules | 351](#)

You can edit, clone, and delete schedules from the **Firewall Policy Schedules** page.

### Editing Schedules

To modify the parameters configured for a schedule:

1. Select **Configuration > Firewall > Schedules**.

The **Firewall Policy Schedules** page appears.

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

The **Edit Schedules** page appears, showing the same options as when creating a new schedule.

3. Modify the parameters according to the guidelines provided in [“Creating Schedules” on page 348](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, the modified schedule appears on the **Firewall Policy Schedules** page.

### Cloning Schedules

To clone a schedule:

1. Select **Configuration > Firewall Policy > Schedules**.

The **Firewall Policy Schedules** page appears.

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

The **Clone Schedules** page appears with editable fields. You can modify the parameters according to the guidelines provided in [“Creating Schedules” on page 348](#).

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

If you click **OK**, the cloned schedule appears under the scheduled it is cloned from, in the **Firewall Policy Schedules**.

## Deleting Schedules

To delete a schedule:

1. Select **Configuration > Firewall Policy > Schedules**.

The **Firewall Policy Schedules** page appears.

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

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

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected schedule is deleted.

## RELATED DOCUMENTATION

---

[Firewall Policy Schedules Overview | 346](#)

---

[About the Firewall Policy Schedules Page | 347](#)

---

[Creating Schedules | 348](#)

---

[Firewall Policy Examples | 306](#)

## Deploying Firewall Policies

After adding the intents to the firewall policies, you can deploy the firewall policy by clicking the **Deploy** option that is above the **End Points** panel. You can also deploy one or more policies from the **Firewall Policy** page.

To deploy firewall policies:

1. Select **Configuration > Firewall > Firewall Policy**.

The Firewall Policy page appears.

2. Select one or more policies and click **Deploy**.

The Deploy page appears.

3. In **Choose Deployment Time** options, select **Run Now** to deploy the policy immediately. Select **Schedule at a later time** and specify the date and time at which the policy should be deployed.

4. Click **Deploy**.

A job is created. Click the job ID to go to the Jobs page and view the status of the deploy operation.

**NOTE:** During deployment, CSO ensures the order of the zone-based intents and enterprise-based intents within and across the policies.

## About the Default Profiles for Unified Firewall Policy Page

To access this page, select **Configuration > Firewall > Default Settings**.

Use this page to view and edit the default settings for unified firewall policies. In a unified firewall policy, dynamic application is used as a match criteria and therefore a separate application firewall is not configured on a device (CPE or next-generation firewall) to allow or block traffic to an application.

The unified firewall takes some time to detect the application in a traffic and act upon it. The default profiles help in providing security during that time.

**NOTE:** The unified firewall policy settings are applied on a device only when Junos OS version 18.2R1 or later is installed on the device.

The default settings comprise the following:

- A UTM profile to define antispam, antivirus, content filtering and web filtering behavior.
- An SSL proxy profile to define the action to be taken when server certificates are not authenticated.

- An IPS profile to define the actions to be taken when the traffic matches the attack objects specified in the IPS profile.
- Reject Settings to define an action when the firewall blocks traffic for a particular application:
  - Take no action
  - Provide a redirect URL to redirect the traffic to another application or URL.
  - Provide a block message to display or log a message indicating that the traffic for the particular application is blocked by the firewall policy.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View the default unified firewall settings—See [Table 119 on page 353](#) describes the fields on this page.
- Modify the default profiles for the unified firewall policy—See [“Editing Default Settings for the Unified Firewall Policy” on page 354](#).

### Field Descriptions

[Table 119 on page 353](#) describes the fields on the Default Profiles for the Unified Firewall Policy page.

**Table 119: Default Profiles for the Unified Firewall Policy Page**

Setting	Guideline
Default UTM Policy	UTM profile assigned for the unified firewall policy, which is set the default UTM policy.
Default SSL Profile	SSL proxy profile assigned for the unified firewall policy, which is set as the default SSL proxy profile.
Default IPS Profile	IPS profile assigned for the unified firewall policy, which is set as the default IPS policy on the device.
<i>Reject Settings</i>	
Reject Action	The action assigned to the unified firewall policy when a firewall blocks application traffic: <ul style="list-style-type: none"> <li>• <b>None:</b> No message or redirection is provided.</li> <li>• <b>Redirect URL:</b> The firewall redirects the traffic to the specified URL.</li> <li>• <b>Text:</b> The firewall displays or logs the message configured for this field.</li> </ul>

## RELATED DOCUMENTATION

| [About the Firewall Policy Page](#) | 287

## Editing Default Settings for the Unified Firewall Policy

Use the Default Profiles for Unified Firewall Policy page to configure the default profile, SSL proxy profile, IPS profile,, and reject or redirect URL or message in the unified firewall policy for a tenant. If you enable a default SSL proxy profile for the tenant, CSO sets the default SSL proxy profile for the tenant as the the default SSL profile in the unified firewall policy.

The unified firewall takes some time to detect the application in a traffic and act upon it. The default profiles help in providing security during that time. The default settings are applicable to all the unified firewall policies belonging to a tenant and pushed to all those sites where a firewall policy is deployed.

To configure default settings for the unified firewall policy:

1. Select **Configuration > Firewall > Default Settings** in Customer Portal.

The Default Profiles for Unified Firewall Policy Settings page appears.

2. Click the **Edit** button.

The fields on the page can now be modified.

3. Complete the configuration according to the guidelines provided in [Table 120 on page 355](#).

4. Do one of the following:

- Click **Cancel** to cancel the changes.
- Click **OK** to save the changes.

The settings are saved and a confirmation message is displayed.

You can deploy the changes by editing the unified firewall policy and then redeploying it.



Table 120: Default Profiles for the Unified Firewall Policy

Setting	Guideline
<b>Default UTM Policy</b>	<p>Select a default UTM profile (policy) from the drop-down list.</p> <p>Alternatively, click the <b>Add UTM Profile</b> to add a UTM profile and use it as the default UTM profile.</p> <p>The Create UTM Profiles wizard appears. For information about creating an UTM policy, see <a href="#">“Creating UTM Profiles” on page 364</a>.</p>
<b>Default SSL Profile</b>	<p>Select a default SSL proxy profile from the drop-down list.</p> <p>Alternatively, click <b>Add SSL Profile</b> to add a new SSL proxy profile and use it as the default SSL proxy profile. .</p> <p>The Create SSL Proxy Profiles page appears. For information about configuring SSL proxy profiles, See <i>Configuring SSL Proxy Profiles</i>.</p>
<b>Default IPS Profile</b>	<p>Select the IPS profile that you want to associate with the unified firewall policy as the default IPS profile.</p>
<b>Reject Settings</b>	
<b>Reject Action</b>	<p>When the action of the firewall is set to deny a particular application traffic, provide an alternative URL to redirect such traffic or a reason for blocking the traffic and an action that a user can perform.</p> <p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>None:</b> Do nothing when an application’s traffic is blocked by the firewall.</li> <li>• <b>Redirect URL:</b> Redirect traffic to a specified URL when the firewall blocks the traffic. If you select this option, you must specify the URL to which traffic should be redirected (in the Redirect URL field).</li> <li>• <b>Text:</b> Block traffic and display a message. If you select this option, you must enter the message (in the Block Message field) to be displayed or logged when the firewall blocks the traffic.</li> </ul>
<b>Redirect URL</b>	<p>If you chose <b>Redirect URL</b> for Reject Action, enter the URL to which an application traffic must be redirected.</p>
<b>Text</b>	<p>If you choose <b>Text</b> for Reject Action, enter the reason for blocking the traffic and what a user can do subsequently.</p> <p>You can enter a maximum of 256 alphanumeric characters including spaces.</p>

## RELATED DOCUMENTATION

[UTM Overview](#) | **358**

[SSL Forward Proxy Overview](#) | **514**

---

# Managing UTM Profiles

## IN THIS CHAPTER

- UTM Overview | 358
- Configuring UTM Settings | 360
- About the UTM Profiles Page | 362
- Creating UTM Profiles | 364
- Editing, Cloning, and Deleting UTM Profiles | 367
- About the Web Filtering Profiles Page | 369
- Creating Web Filtering Profiles | 371
- Editing, Cloning, and Deleting Web Filtering Profiles | 375
- About the Antivirus Profiles Page | 377
- Creating Antivirus Profiles | 379
- Editing, Cloning, and Deleting Antivirus Profiles | 382
- About the Antispam Profiles Page | 384
- Creating Antispam Profiles | 385
- Editing, Cloning, and Deleting Antispam Profiles | 387
- About the Content Filtering Profiles Page | 389
- Creating Content Filtering Profiles | 391
- Editing, Cloning, and Deleting Content Filtering Profiles | 395
- About the URL Patterns Page | 397
- Creating URL Patterns | 398
- Editing, Cloning, and Deleting URL Patterns | 399
- About the URL Categories Page | 401
- Creating URL Categories | 402
- Editing, Cloning, and Deleting URL Categories | 404

## UTM Overview

### IN THIS SECTION

- [UTM Licensing | 359](#)
- [UTM Components | 359](#)

Unified threat management (UTM) is a term used to describe the consolidation of several security features to protect against multiple threat types. The advantage of UTM is a streamlined installation and management of multiple security capabilities.

The following security features are provided as part of the UTM solution:

- **Antispam**—This feature examines transmitted messages to identify e-mail spam. E-mail spam consists of unwanted messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated Spamhaus Block List (SBL). Sophos updates and maintains the IP-based SBL.
- **Full file-based antivirus**—A virus is an executable code that infects or attaches itself to other executable code to reproduce itself. Some malicious viruses erase files or lock up systems. Other viruses merely infect files and overwhelm the target host or network with bogus data. The full file-based antivirus feature provides file-based scanning on specific application layer traffic, checking for viruses against a virus signature database. The antivirus feature collects the received data packets until it has reconstructed the original application content, such as an e-mail file attachment, and then scans this content.
- **Express antivirus**—Express antivirus scanning is offered as a less CPU-intensive alternative to the full file-based antivirus feature. The express antivirus feature is similar to the antivirus feature in that it scans specific application layer traffic for viruses against a virus signature database. However, unlike full antivirus, express antivirus does not reconstruct the original application content. Rather, it just sends (streams) the received data packets, as is, to the scan engine. With express antivirus, the virus scanning is executed by a hardware pattern-matching engine. This improves performance while scanning is occurring, but the level of security provided is lessened. Juniper Networks provides the scan engine.
- **Content filtering**—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type.
- **Web filtering**—Web filtering enables you to manage Internet usage by preventing access to inappropriate Web content. The following types of Web filtering solutions are available:

- Integrated Web filtering—Blocks or permits Web access after the device identifies the category for a URL either from user-defined categories or from a category server (Websense provides the SurfControl Content Portal Authority (CPA) server).
- Redirect Web filtering—Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.

## UTM Licensing

All UTM components require licenses with the exception of content filtering, which uses the parameters defined in the content filtering profile. This is because Juniper Networks leverages third-party technology that is constantly updated to provide the most up-to-date inspection capabilities.

## UTM Components

UTM components include custom objects, feature profiles, and UTM profiles that can be configured on SRX Series devices. From a high level, feature profiles specify how a feature is configured and then applied to UTM profiles, which in turn is applied to firewall policies, as shown in [Figure 11 on page 359](#).

Figure 11: UTM Components



UTM profiles do not have their own seven-tuple rulebase; in a sense they inherit the rules from the firewall rule. The strength of the UTM feature comes from URL filtering, where you can have a separate configuration for different users or user groups.

- Custom objects—Although SRX Series devices support predefined feature profiles that can handle most typical use cases, there are some cases where you might need to define your own objects, specifically for URL filtering, antivirus filtering, and content filtering.
- Feature profiles—Feature profiles specify how components of each profile should function. You can configure multiple feature profiles that can be applied through different UTM profiles to firewall rules.
- UTM profiles—UTM profiles function as a logical container for individual feature profiles. UTM profiles are then applied to specific traffic flows based on the classification of rules in the firewall policy, thereby enabling you to define separate UTM profiles per firewall rule to differentiate the enforcement per

firewall rule. Essentially, the firewall rulebase acts as the match criteria, and the UTM profile is the action to be applied.

- Firewall policy—You can predefine feature profiles for the UTM profile that are then applied to the firewall rules. This gives you the advantage of using the predefined UTM profile for that one UTM technology (for example, antivirus or URL filtering), not both.

RELATED DOCUMENTATION

<a href="#">Configuring UTM Settings   360</a>
<a href="#">About the UTM Profiles Page   362</a>
<a href="#">Creating UTM Profiles   364</a>

Configuring UTM Settings

Use the Edit UTM Settings page to configure unified threat management (UTM) antispam, antivirus, and Web filtering settings for a tenant.

These settings are applicable to all the sites belonging to a tenant. The settings are pushed to all those sites where a firewall policy intent with UTM enabled is applicable.

To configure UTM settings:

1. Select **Configuration > Unified Threat Mgmt > UTM Settings** in Customer Portal.  
The Edit UTM Settings page appears.
2. Complete the configuration according to the guidelines provided in [Table 121 on page 360](#).
3. Do one of the following:
  - Click **Reset** to reset the settings to the previously saved configured.
  - Click **OK** to save the settings.

The settings are saved and a confirmation message is displayed.

Table 121: UTM Settings

Setting	Guideline
<b>Antispam Settings</b>	

Table 121: UTM Settings (*continued*)

Setting	Guideline
<b>Address Whitelist</b>	<p>Select the URL pattern to be used as the antispam allowlist.</p> <p>Alternatively, click <b>Create a New Pattern</b> to create a new URL pattern to use as a allowlist.</p> <p>The Create URL Patterns page appears. For more information, see <a href="#">“Creating URL Patterns” on page 398</a> for an explanation of the fields on this page.</p>
<b>Address Blacklist</b>	<p>Select the URL pattern to be used as the antispam blocklist.</p> <p>Alternatively, click <b>Create a New Pattern</b> to create a new URL pattern to use as a blocklist.</p>
<b>Antivirus Settings</b>	
<b>MIME Whitelist</b>	Enter one or more MIME types (separated by commas) to exclude from antivirus scanning.
<b>Exception MIME Whitelist</b>	Enter one or more MIME types (separated by commas) that are to be excluded from the list of MIME types specified as part of the MIME allowlist. This list is a subset of the MIME types that you specified in the MIME allowlist. For example, if you specify <b>video/</b> in the allowlist and <b>video/x-shockwave-flash</b> in the exception allowlist, all objects of MIME type <b>video/</b> except MIME type <b>video/x-shockwave-flash</b> are excluded from antivirus scanning.
<b>URL Whitelist</b>	Select the list of URLs the antivirus settings can allow.
<b>Web Filtering Settings</b>	
<b>URL Whitelist</b>	Select the list of URLs the Web filtering settings can allow; these URLs are excluded from Web filtering.
<b>URL Blacklist</b>	Select the list of URLs the Web filtering settings can block; these URLs are blocked from Web access.

## RELATED DOCUMENTATION

| [About the UTM Profiles Page](#) | 362

## About the UTM Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

Use this page to view and manage unified threat management (UTM) profiles. UTM profiles enable you to consolidate several security features into one system to protect against multiple threat types.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a UTM profile—See [“Creating UTM Profiles” on page 364](#).
- Edit, clone, or delete a UTM profile—See [“Editing, Cloning, and Deleting UTM Profiles” on page 367](#).
- Clear the selected UTM profiles—Click **Clear All Selections** to clear any UTM profiles that you might have selected.
- View the details of a UTM profile—Select the UTM profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The UTM Profile Details page appears. [Table 123 on page 363](#) describes the fields on this page.
- Search for UTM profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

### Field Descriptions

[Table 122 on page 362](#) describes the fields on the UTM Profiles page.

**Table 122: UTM Profiles Page Fields**

Field	Description
Name	Name of the UTM profile.
Antispam	Information about the antispam profile associated with the UTM profile.
Antivirus	Information about the antivirus profiles associated with the UTM profile.
Content Filtering	Information about the content filtering profiles associated with the UTM profile.
Web Filtering	Information about the Web filtering profile associated with the UTM profile.
Description	Description of the UTM profile.



Table 123: UTM Profile Details Page Fields

Field	Description
<b>General Information</b>	
Name	Name of the UTM profile.
Description	Description of the UTM profile.
<b>Traffic Options</b>	
Action When Connection Limit Is Reached	Action to be taken when the configured connection limit per client is reached.
<b>Web Filtering Profile</b>	
HTTP	Web filtering profile to be used for HTTP traffic.
<b>Antivirus Profile</b>	
HTTP	Antivirus profile to be used for HTTP traffic.
FTP Upload	Antivirus profile to be used for FTP upload traffic.
FTP Download	Antivirus profile to be used for FTP download traffic.
IMAP	Antivirus profile to be used for IMAP traffic.
SMTP	Antivirus profile to be used for SMTP traffic.
POP3	Antivirus profile to be used for POP3 traffic.
<b>Antispam Profile</b>	
SMTP	Antispam profile to be used for SMTP traffic.

## RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 364

## Creating UTM Profiles

Use the Create UTM Profiles page to configure UTM profiles. Unified threat management (UTM) consolidates several security features to protect against multiple threat types. The Create UTM Profiles wizard provides step-by-step procedures to create a UTM profile. You can configure antispam, antivirus, Web filtering, and content filtering profiles by launching the respective wizards from the wizard.

To create a UTM profile:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears.

2. Click the add icon (+) to create a new UTM profile.

The Create UTM Profiles wizard appears, displaying brief instructions about creating a UTM profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 124 on page 364](#).

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

5. Click **Finish**.

A UTM profile is created. You are returned to the UTM Profiles page where a confirmation message is displayed. After you create a UTM profile, you can assign it to a firewall policy intent on the Firewall Policy page.

**Table 124: UTM Profile Settings**

Setting	Guideline
<b>General</b>	
<b>Name</b>	Enter a unique name for the UTM profile. The maximum length is 29 characters.
<b>Description</b>	Enter a description for the UTM profile. The maximum length is 255 characters.
<b>Traffic Options</b>	
<p><b>NOTE:</b> In an attempt to consume all available resources, a malicious user might generate a large amount of traffic all at once. To prevent such activity from succeeding, you can impose traffic options.</p>	

Table 124: UTM Profile Settings (*continued*)

Setting	Guideline
<b>Connection Limit per Client</b>	Specify the connection limit per client for client connections on the device. The default is 2000 and a value of 0 means that there is no connection limit.
<b>Action when connection limit is reached</b>	Specify the action that must be taken when the connection limit is reached. The available actions are No action (default), Log and permit, and Block.  Click <b>Next</b> to continue.
<b>Web Filtering</b>	
<b>HTTP</b>	Select the Web filtering profile to be applied for HTTP traffic.  Alternatively, click <b>Create Another Profile</b> to create a Web filtering profile. The Create Web Filtering Profiles wizard appears. See <a href="#">“Creating Web Filtering Profiles” on page 371</a> for an explanation of the fields on this wizard.  Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.
<b>Antivirus</b>	
<b>Apply to all protocols</b>	Select this check box to apply a single antivirus profile to all traffic protocols. and then specify the profile in the <b>Default Profile</b> field.  Clear the check box if you want to apply traffic-specific profiles.
<b>Default Profile</b>	Select the antivirus profile to be applied to all traffic protocols.  Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.
<b>NOTE:</b> Click <b>Create Another Profile</b> to create an antivirus profile that you can then assign. The Create Antivirus Profiles wizard appears. See <a href="#">“Creating Antivirus Profiles” on page 379</a> for an explanation of the fields on this wizard.	
<b>HTTP</b>	Select the antivirus profile to be applied to HTTP traffic.
<b>FTP Upload</b>	Select the antivirus profile to be applied to FTP upload traffic.
<b>FTP Download</b>	Select the antivirus profile to be applied to FTP download traffic.
<b>IMAP</b>	Select the antivirus profile to be applied to IMAP traffic.
<b>SMTP</b>	Select the antivirus profile to be applied to SMTP traffic.

Table 124: UTM Profile Settings (*continued*)

Setting	Guideline
<b>POP3</b>	<p>Select the antivirus profile to be applied to POP3 traffic.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<b>Antispam</b>	
<b>SMTP</b>	<p>Select the antispam profile to be applied for SMTP traffic.</p> <p>Alternatively, click <b>Create Another Profile</b> to create an antispam profile. The Create Antispam Profiles wizard appears. See <a href="#">“Creating Antispam Profiles” on page 385</a> for an explanation of the fields on this wizard.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<b>Content Filtering</b>	
<b>Apply to all protocols</b>	<p>Select this check box to apply a single content filtering profile to all traffic protocols, and then specify the profile in the <b>Default Profile</b> field.</p> <p>Clear the check box if you want to apply traffic-specific profiles.</p>
<b>Default Profile</b>	<p>Select the content filtering profile to be applied to all traffic protocols.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<p><b>NOTE:</b> Click <b>Create Another Profile</b> to create a content filtering profile that you can then assign. The Create Content Filtering Profiles wizard appears. See <a href="#">“Creating Content Filtering Profiles” on page 391</a> for an explanation of the fields on this wizard.</p>	
<b>HTTP</b>	Select the content filtering profile to be applied to HTTP traffic.
<b>FTP Upload</b>	Select the content filtering profile to be applied to FTP upload traffic.
<b>FTP Download</b>	Select the content filtering profile to be applied to FTP download traffic.
<b>IMAP</b>	Select the content filtering profile to be applied to IMAP traffic.
<b>SMTP</b>	Select the content filtering profile to be applied to SMTP traffic.
<b>POP3</b>	<p>Select the content filtering profile to be applied to POP3 traffic.</p> <p>Click <b>Back</b> to go the preceding step.</p>

## RELATED DOCUMENTATION

[About the UTM Profiles Page | 362](#)

[Configuring UTM Settings | 360](#)

## Editing, Cloning, and Deleting UTM Profiles

### IN THIS SECTION

- [Editing UTM Profiles | 367](#)
- [Cloning UTM Profiles | 368](#)
- [Deleting UTM Profiles | 368](#)

You can edit, clone, and delete UTM profiles from the UTM Profiles page. This topic has the following sections:

### Editing UTM Profiles

To modify the parameters configured for a UTM profile:

**NOTE:** You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select the UTM profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit UTM Profiles page appears, displaying the same fields that are presented when you create a UTM profile.

3. Modify the UTM profile fields as needed.

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

You are taken to the UTM Profiles page. A confirmation message appears indicating the status of the edit operation.

## Cloning UTM Profiles

Cloning enables you to easily create a new UTM profile based on an existing one.

To clone a UTM profile:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select the UTM profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone UTM Profiles page appears, displaying the same fields that are presented when you create a UTM profile.

3. Modify the UTM profile fields as needed.

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

You are taken to the UTM Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting UTM Profiles

**NOTE:** Before deleting a UTM profile, ensure that the profile is not used in a firewall policy intent. If you try to delete a profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more UTM profiles:

1. Select **Configuration > Unified Threat Mgmt > UTM Profiles** in Customer Portal.

The UTM Profiles page appears, displaying the existing UTM profiles.

2. Select one or more UTM profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Profile**.

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

- Click **Yes** to delete the selected UTM profiles.

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

## RELATED DOCUMENTATION

[Creating UTM Profiles | 364](#)

[About the UTM Profiles Page | 362](#)

## About the Web Filtering Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

Use the Web Filtering Profiles page to view and manage Web filtering profiles. Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP. [Table 125 on page 369](#) lists the Web filtering solutions that are supported and the license requirements.

**Table 125: Web Filtering Solutions Supported**

Type	Description	License Requirement
Integrated Web Filtering	Blocks or permits Web access after the device identifies the category for a URL, either from user-defined categories or from a category server (SurfControl Content Portal Authority provided by Websense).	A separately licensed subscription service
Redirect Web Filtering	Intercepts HTTP requests and forwards the server URL to an external URL filtering server to determine whether to block or permit the requested Web access. Websense provides the URL filtering server.	Does not require a license.
Juniper Local Web Filtering	Intercepts every HTTP request in a TCP connection. In this case, the decision making is done on the device after it looks up a URL to determine whether it is in the allowlist or blocklist based on its user-defined category.	Does not require a license or a remote category server

## Tasks You Can Perform

You can perform the following tasks from this page:

- Create a Web filtering profile—See [“Creating Web Filtering Profiles” on page 371](#).
- Edit, clone, or delete a Web filtering profile—See [“Editing, Cloning, and Deleting Web Filtering Profiles” on page 375](#).
- Clear the selected Web filtering profiles—Click **Clear All Selections** to clear any Web filtering profiles that you might have selected.
- View the details of a Web filtering profile—Select the Web filtering profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Web Filtering Profile Details page appears. [Table 127 on page 370](#) describes the fields on this page.
- Search for Web filtering profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

## Field Descriptions

[Table 126 on page 370](#) describes the fields on the Web Filtering Profiles page.

**Table 126: Web Filtering Profiles Page Fields**

Field	Description
Name	Name of the Web filtering profile.
Profile Type	Type of engine used for the profile: Juniper-enhanced or Websense redirect.
Default Action	Default action taken when the specified connection limit per client is reached.
Timeout	
Description	Description of the Web filtering profile.

**Table 127: Web Filtering Profile Details Page Fields**

Field	Description
<b>General Information</b>	
Name	Name of the Web filtering profile.
Description	Description of the Web filtering profile.
Engine Type	Type of engine used for the profile: Juniper-enhanced or Websense redirect.
Default Action	Default action taken when the specified connection limit per client is reached.



Table 127: Web Filtering Profile Details Page Fields (*continued*)

Field	Description
Fallback Options	
Default Action	Action taken for URL categories with no assigned action and for uncategorized URLs. This action is taken only if no reputation action is assigned.
Global Reputation Actions	Actions taken for the following site reputations: <ul style="list-style-type: none"> <li>• Very Safe</li> <li>• Moderately Safe</li> <li>• Fairly Safe</li> <li>• Suspicious</li> <li>• Harmful</li> </ul>
URL Categories	URL categories associated with the Web filtering profile.

## RELATED DOCUMENTATION

[Creating Web Filtering Profiles | 371](#)
[Editing, Cloning, and Deleting Web Filtering Profiles | 375](#)

## Creating Web Filtering Profiles

Web filtering profiles enable you to manage Internet usage by preventing access to inappropriate Web content over HTTP.

To create a Web filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

The Web Filtering Profiles page appears.

2. Click the add icon (+) to create a new Web filtering profile.

The Create Web Filtering Profiles wizard appears, displaying brief instructions about creating a Web filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 128 on page 372](#).

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

5. Click **Finish**.

A Web filtering profile is created, which you can associate with a UTM profile. You are returned to the Web Filtering Profiles page where a confirmation message is displayed.

**Table 128: Creating Web Filtering Profiles Settings**

Setting	Guideline
<b>General Information</b>	
<b>Name</b>	Enter a unique name for the Web filtering profile. The maximum length is 29 characters.
<b>Description</b>	Enter a description for the Web filtering profile. The maximum length is 255 characters.
<b>Timeout</b>	Enter a timeout (in seconds) to wait for a response from the Websense server. The default is 15 seconds and the maximum is 1000 seconds.
<b>Engine Type</b>	<p>Select an engine type for Web filtering:</p> <ul style="list-style-type: none"> <li>• (Default) Juniper Enhanced—UTM-enhanced Web filtering.</li> <li>• Websense Redirect—Redirect Web filtering profile.</li> </ul>
<b>Safe Search</b>	<p>Select the check box (default) to ensure that embedded objects, such as images on the URLs received from the search engines, are safe and that undesirable content is not returned to the client.</p> <p>Clear the check box to disable safe search redirects.</p> <p><b>NOTE:</b> This option is available only for the Juniper Enhanced engine type. Safe search redirect supports only HTTP and you cannot extract the URL for HTTPS. Therefore, it is not possible to generate a redirect response for HTTPS search URLs.</p>
<b>Custom Block Message/URL</b>	<p>Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 512 characters.</p> <p><b>NOTE:</b> If a message begins with http: or https:, the message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>

Table 128: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
<b>Custom Quarantine Message</b>	<p>Define a custom message to allow or deny access to a blocked site based on a user's response to the message. The maximum length is 512 characters.</p> <p>The quarantine message contains the following information:</p> <ul style="list-style-type: none"> <li>• URL name</li> <li>• Quarantine name</li> <li>• Category (if available)</li> <li>• Site reputation (if available)</li> </ul> <p>For example, if you set the action for <code>Enhanced_Search_Engines_and_Portals</code> to quarantine, and you try to access <code>www.search.yahoo.com</code>, the quarantine message is as follows: <b>***The requested webpage is blocked by your organization's access policy***</b>.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<b>Account</b>	Specify the user account associated with the Websense Web filtering profile.
<b>Server</b>	Specify the hostname or IP address for the Websense server.
<b>Port</b>	Enter the number of sockets used for communication between the client and the server. The default value is 8.
<b>Sockets</b>	<p>Specify the port number to use to communicate with the Websense server. The default port value is 15968.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<b>URL Categories</b>	
<b>Deny Action List</b>	<p>Click the <b>Add URL Categories</b> button to specify a list of URL categories that should be denied access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in <a href="#">Table 129 on page 375</a>,</p> <p>The list of URL categories selected is displayed in a text box.</p>
<b>Log &amp; Permit Action List</b>	<p>Specify a list of URL categories that are logged and then permitted.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in <a href="#">Table 129 on page 375</a>.</p> <p>The list of URL categories selected is displayed in a text box.</p>

Table 128: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
<b>Permit Action List</b>	<p>Specify a list of URL categories that should be permitted access.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in <a href="#">Table 129 on page 375</a></p> <p>The list of URL categories selected is displayed in a text box.</p>
<b>Quarantine Action List</b>	<p>Specify a list of URL categories that should be quarantined.</p> <p>The Select URL Categories page appears. Complete the configuration according to the guidelines provided in <a href="#">Table 129 on page 375</a>.</p> <p>The list of URL categories selected is displayed in a text box.</p> <p>Click <b>Back</b> to go the preceding step or click <b>Next</b> to go to the next step.</p>
<b>Fallback Options</b>	
<b>Global Reputation Actions</b>	<p>Select this check box (default) if you want to apply global reputation actions.</p> <p>Enhanced Web filtering intercepts HTTP and HTTPS requests and sends the HTTP URL or the HTTPS source IP to the Websense ThreatSeeker Cloud (TSC). The TSC categorizes the URL into one of the predefined categories and also provides site reputation information for the URL to the device. The device determines if it can permit or block the request based on the information provided by the TSC.</p> <p>The URLs can be processed using their reputation score if there is no category available. Select the action that you want to take for the uncategorized URLs based on their reputation score:</p> <ul style="list-style-type: none"> <li>● <b>Very Safe</b>—Permit, log and permit, block, or quarantine a request if a site reputation of 90 through 100 is returned. By default, Permit is selected.</li> <li>● <b>Moderately Safe</b>—Permit, log and permit, block, or quarantine a request if a site reputation of 80 through 89 is returned. By default, Log and Permit is selected.</li> <li>● <b>Fairly Safe</b>—Permit, log and permit, block or quarantine a request if a site-reputation of 70 through 79 is returned. By default, Log and Permit is selected.</li> <li>● <b>Suspicious</b>—Permit, log and permit, block, or quarantine a request if a site reputation of 60 through 69 is returned. By default, Quarantine is selected.</li> <li>● <b>Harmful</b>—Permit, log and permit, block, or quarantine a request if a site reputation of zero through 59 is returned. By default, Block is selected.</li> </ul>
<b>Default Action</b>	<p>Choose the actions to be taken for URL categories with no assigned action and for uncategorized URLs. This is used only if no reputation action is assigned.</p>

Table 128: Creating Web Filtering Profiles Settings (*continued*)

Setting	Guideline
<b>Fallback Action</b>	<p>Select the fallback action, which is used when:</p> <ul style="list-style-type: none"> <li>• The ThreatSeeker Websense Cloud servers are unreachable.</li> <li>• A timeout occurs for requests to ThreatSeeker Cloud.</li> <li>• There are too many requests to be handled by the device.</li> </ul>

Table 129: Select URL Categories Settings

Setting	Guideline
<b>Show</b>	<p>Choose which URL categories should be displayed for selection: <b>All categories</b>, <b>Custom URL categories</b>, or <b>Websense URL categories</b>.</p> <p>The <b>Available</b> column of the <b>URL Categories</b> field displays URL categories based on your selection.</p>
<b>URL Categories</b>	<p>Select one or more URL categories in the <b>Available</b> column and click the forward arrow to confirm your selection. The selected URL categories are displayed in the <b>Selected</b> column.</p> <p>Alternatively, click <b>Create New URL Category</b> to create a URL category and assign it to the URL category. The Create URL Categories page appears; for more information, see <a href="#">“Creating URL Categories” on page 402</a>.</p> <p>Click <b>OK</b> to confirm your selection. You are returned to the Create Web Filtering Profiles page.</p>

## RELATED DOCUMENTATION

| [Creating UTM Profiles | 364](#)

## Editing, Cloning, and Deleting Web Filtering Profiles

### IN THIS SECTION

- [Editing Web Filtering Profiles | 376](#)
- [Cloning Web Filtering Profiles | 376](#)
- [Deleting Web Filtering Profiles | 377](#)

You can edit, clone, and delete Web filtering profiles from the Web Filtering Profiles page. This topic has the following sections:

## Editing Web Filtering Profiles

To modify the parameters configured for a Web filtering profile:

**NOTE:** You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.  
The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.
2. Select the Web filtering profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.  
The Edit Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.
3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.  
You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

## Cloning Web Filtering Profiles

Cloning enables you to easily create a new Web filtering profile based on an existing one.

To clone a Web filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.  
The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.
2. Select the Web filtering profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.  
The Clone Web Filtering Profiles page appears, displaying the same fields that are presented when you create a Web filtering profile.

3. Modify the Web filtering profile fields as needed.
4. Click **OK** to save your changes.

You are taken to the Web Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting Web Filtering Profiles

Before deleting a Web filtering profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete a Web filtering profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more Web filtering profiles:

1. Select **Configuration > Unified Threat Mgmt > Web Filtering Profiles** in Customer Portal.

The Web Filtering Profiles page appears, displaying the existing Web filtering profiles.

2. Select one or more Web filtering profiles that you want to delete and click the delete icon (X).  
Alternatively, right-click a profile and select **Delete Profile**.

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

3. Click **Yes** to delete the selected Web filtering profiles.

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

## RELATED DOCUMENTATION

[Creating Web Filtering Profiles | 371](#)

[About the Web Filtering Profiles Page | 369](#)

## About the Antivirus Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

Use the Antivirus Profiles page to view and manage antivirus profiles. Antivirus profiles enable you to inspect files transmitted over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) to determine whether the files exchanged are known malicious files, similar to how desktop antivirus software scans files for the same purpose.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antivirus profile—See [“Creating Antivirus Profiles” on page 379](#).
- Edit, clone, or delete an antivirus profile—See [“Editing, Cloning, and Deleting Antivirus Profiles” on page 382](#).
- Clear the selected antivirus profiles—Click **Clear All Selections** to clear any antivirus profiles that you might have selected.
- View the details of an antivirus profile—Select the antivirus profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antivirus Profile Details page appears. [Table 131 on page 378](#) describes the fields on this page.
- Search for antivirus profiles by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 130 on page 378](#) describes the fields on the Antivirus Profiles page.

Table 130: Antivirus Profiles Page Fields

Field	Description
Name	Name of the antivirus profile.
Profile Type	Type of engine used for the profile.
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Trickling Timeout	Number of seconds to wait for a response from the server.
Description	Description of the antivirus profile.

Table 131: Antivirus Profiles Details Page Fields

Field	Description
<b>General Information</b>	
Name	Name of the antivirus profile.
Description	Description of the antivirus profile.



Table 131: Antivirus Profiles Details Page Fields (*continued*)

Field	Description
Engine Type	Type of engine used for the profile.
Scan Options	
Content Size Limit	Content size limit, in kilobytes, refers to accumulated TCP payload size.
Fallback Options	
Default Action	Displays the default fallback action taken when the antivirus system encounters errors.
Content Size	Displays the actions taken if the content size exceeds a set limit.
Engine Error	Displays the action taken when an engine error occurs.

## RELATED DOCUMENTATION

| [Creating UTM Profiles](#) | 364

## Creating Antivirus Profiles

Use the Create Antivirus Profiles page to configure antivirus profiles. The antivirus profile defines the content to scan for any malware and the action to be taken when malware is detected. After you create a profile, you can assign it to UTM profiles.

To create an antivirus profile:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears.

2. Click the add icon (+) to create a new antivirus profile.

The Create Antivirus Profiles wizard appears, displaying brief instructions about creating an antivirus profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 132 on page 380](#).

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

5. Click **Finish**.

A summary page is displayed. Review the settings, and if you need to make any modifications, click the **Edit** link or the **Back** button.

6. Click **OK** to save the settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Antivirus Profiles page.

**Table 132: Antivirus Profile Settings**

Setting	Guideline
<b>General Information</b>	
Name	Enter a unique name for the antivirus profile. The maximum length is 29 characters.
Description	Enter a description for the antivirus profile. The maximum length is 255 characters.
Engine Type	Displays the engine type used for scanning. Currently, <b>Sophos</b> is the only antivirus engine supported.  Sophos antivirus is an in-the-cloud antivirus solution. The virus and malware database is located on external servers maintained by Sophos (Sophos Extensible List) servers, thus there is no need to download and maintain large pattern databases on the Juniper Networks device.
<b>Fallback Options</b>	

Table 132: Antivirus Profile Settings (*continued*)

Setting	Guideline
	<p>Fallback options are used when the antivirus system experiences errors and must fall back to one of the previously configured actions to either deny (block) or permit the object.</p> <p>Specify the fallback options to use when there is a failure, or select the default action if no specific options are to be configured:</p> <ul style="list-style-type: none"> <li>• <b>Content Size</b>—Select an option to specify whether the content should be blocked (default) or logged and permitted if the content size the previously defined limit.</li> <li>• <b>Content Size Limit</b>—Enter the content size limit in kilobytes (KB) based on which action is taken. The range is 20 through 40,000 KB. The content size limit check occurs before the scan request is sent. The content size refers to accumulated TCP payload size.</li> <li>• <b>Engine Error</b>—Select the action to take (<b>Block</b> [default] or <b>Log and Permit</b>) when an engine error occurs.  The term <i>engine error</i> refers all engine errors, including engine not ready, timeout, too many requests, password protected, corrupt file, decompress layer, and out of resources.</li> <li>• <b>Default Action</b>—Select the default action (<b>Block</b> [default] or <b>Log and Permit</b>) to take when an error occurs.</li> </ul>
<b>Notification Options</b>	
	<p>Use the notification options to configure a method of notifying the user when a fallback occurs or a virus is detected:</p> <ul style="list-style-type: none"> <li>• <b>Fallback Deny</b>—Select this option to notify mail senders that their messages were blocked.</li> <li>• <b>Fallback Non-Deny</b>—Select this option to warn mail recipients that they received unblocked messages despite problems.</li> <li>• <b>Virus Detected</b>—Select this option to notify mail recipients that their messages were blocked.</li> </ul>

## RELATED DOCUMENTATION

Creating UTM Profiles | 364

## Editing, Cloning, and Deleting Antivirus Profiles

### IN THIS SECTION

- [Editing Antivirus Profiles | 382](#)
- [Cloning Antivirus Profiles | 382](#)
- [Deleting Antivirus Profiles | 383](#)

You can edit, clone, and delete antivirus profiles from the Antivirus Profiles page. This topic has the following sections:

### Editing Antivirus Profiles

To modify the parameters configured for an antivirus profile:

**NOTE:** You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the antivirus profile that you want to edit and then select the edit icon (pencil). Alternatively, right-click a profile and select **Edit Antivirus Profile**.

The Edit Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.

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

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the edit operation.

### Cloning Antivirus Profiles

Cloning enables you to easily create a new antivirus profile based on an existing one.

To clone an antivirus profile:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select the antivirus profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Antivirus Profiles page appears, displaying the same fields that are presented when you create an antivirus profile.

3. Modify the antivirus profile fields as needed.

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

You are taken to the Antivirus Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting Antivirus Profiles

Before deleting an antivirus profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete an antivirus profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more antivirus profiles:

1. Select **Configuration > Unified Threat Mgmt > Antivirus Profiles** in Customer Portal.

The Antivirus Profiles page appears, displaying the existing antivirus profiles.

2. Select one or more antivirus profiles that you want to delete and then select the delete icon (X). Alternatively, right-click a profile and select **Delete Antivirus Profiles**.

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

3. Click **Yes** to delete the selected antivirus profiles.

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

## RELATED DOCUMENTATION

---

[Creating Antivirus Profiles | 379](#)

[About the Antivirus Profiles Page | 377](#)

## About the Antispam Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

Use the Antispam Profiles page to view and manage antispam profiles. An antispam profile is used to examine transmitted e-mail messages to identify e-mail spam by using a constantly updated spam block list.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create an antispam profile—See [“Creating Antispam Profiles” on page 385](#).
- Edit, clone, or delete an antispam profile—See [“Editing, Cloning, and Deleting Antispam Profiles” on page 387](#).
- Clear the selected antispam profiles—Click **Clear All Selections** to clear any antispam profiles that you might have selected.
- View the details of an antispam profile—Select the antispam profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Antispam Profile Details page appears. [Table 134 on page 385](#) describes the fields on this page.
- Search for antispam profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

### Field Descriptions

[Table 133 on page 384](#) describes the fields on the Antispam Profiles page.

**Table 133: Antispam Profiles Page Fields**

Field	Description
<b>Name</b>	Name of the antispam profile.
<b>Blacklist</b>	Indicates whether server-based spam filtering or local spam filtering is used.
<b>Action</b>	Action to be taken when spam is detected.
<b>Custom Tag</b>	Custom-defined tag that identifies an e-mail message as spam.
<b>Description</b>	Description of the antispam profile.

Table 134: Antispam Profile Details Page Fields

Field	Description
<b>Name</b>	Name of the antispam profile.
<b>Description</b>	Description of the antispam profile.
<b>Sophos Blacklist</b>	Indicates whether this field enabled (server-based filtering) or disabled (local filtering).
<b>Default Action</b>	Action to be taken when spam is detected.
<b>Custom Tag</b>	Custom-defined tag that identifies an e-mail message as spam.

## RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 364

## Creating Antispam Profiles

Use the Create Antispam Profiles page to configure antispam profiles.

E-mail spam consists of unwanted e-mail messages usually sent by commercial, malicious, or fraudulent entities. When the device detects an e-mail message deemed to be spam, it either blocks the message or tags the message header or subject field with a preprogrammed string. Antispam filtering allows you to use a third-party server-based spam block list (SBL) and to optionally create your own local allowlists (benign) and blocklists (malicious) for filtering against e-mail messages.

**NOTE:** Sophos updates and maintains the IP-based SBL. Antispam is a separately licensed subscription service.

After you create an antispam profile, you can assign it to UTM profiles.

To create an antispam profile:


- 1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears.

- 2. Click the add icon (+) to create a new antispam profile.

The Create Antispam Profiles wizard appears, displaying brief instructions about creating an antispam profile.

- 3. Complete the configuration according to the guidelines provided in [Table 135 on page 386](#).

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

- 4. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed. You are returned to the Antispam Profiles page.

Table 135: Antispam Profile Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the antispam profile. The maximum length is 29 characters.
Description	Enter a description for the antispam profile. The maximum length is 255 characters.
Sophos Blacklist	<p>Select this check box (the default) to use server-based spam filtering. If you clear the check box, local spam filtering is used.</p> <p>Server-based antispam filtering requires Internet connectivity with the spam block list (SBL) server. Domain Name Service (DNS) is required to access the SBL server. The firewall performs SBL lookups through the DNS protocol.</p> <p><b>NOTE:</b> Server-based spam filtering supports only IP-based spam block list blocklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.</p>
Action	



Table 135: Antispam Profile Settings (continued)

Setting	Guideline
Default Action	Select the action to be taken when spam is detected: <ul style="list-style-type: none"><li>• Tag Email Subject Line</li><li>• Tag SMTP Header</li><li>• Block Email</li><li>• None</li></ul>
Custom Tag	Enter a custom string for identifying a message as spam. The maximum length is 512 characters and the default is <b>***SPAM***</b> .

RELATED DOCUMENTATION

| [Creating UTM Profiles](#) | 364

Editing, Cloning, and Deleting Antispam Profiles

IN THIS SECTION

- [Editing Antispam Profiles](#) | 388
- [Cloning Antispam Profiles](#) | 388
- [Deleting Antispam Profiles](#) | 389

You can edit, clone, and delete antispam profiles from the Antispam Profiles page. This topic has the following sections:

## Editing Antispam Profiles

To modify the parameters configured for an antispam profile:

**NOTE:** You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears, displaying the existing antispam profiles.

2. Select the antispam profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Antispam Profile**.

The Edit Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.

3. Modify the antispam profile fields as needed.

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

You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the edit operation.

## Cloning Antispam Profiles

Cloning enables you to easily create a new antispam profile based on an existing one.

To clone an antispam profile:

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears displaying the existing antispam profiles.

2. Select the antispam profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Antispam Profiles page appears, displaying the same fields that are presented when you create an antispam profile.

3. Modify the antispam profile fields as needed.

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

You are taken to the Antispam Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting Antispam Profiles

Before deleting an antispam profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete an antispam profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more antispam profiles:

1. Select **Configuration > Unified Threat Mgmt > Antispam Profiles** in Customer Portal.

The Antispam Profiles page appears, displaying the existing antispam profiles.

2. Select one or more antispam profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Antispam Profiles**.

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

3. Click **Yes** to delete the selected antispam profiles.

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

## RELATED DOCUMENTATION

| [About the Antispam Profiles Page](#) | 384

## About the Content Filtering Profiles Page

To access this page, select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

Use the Content Filtering Profiles page to view and manage content filtering profiles. Content filtering profiles enable you to block or permit certain types of traffic over several protocols (HTTP, FTP upload and download, IMAP, SMTP, and POP3) based on the MIME type, file extension, protocol command, and embedded object type.

## Tasks You Can Perform

You can perform the following tasks from this page:

- Create a content filtering profile—See [“Creating Content Filtering Profiles” on page 391](#).
- Edit, clone, or delete a content filtering profile—See [“Editing, Cloning, and Deleting Content Filtering Profiles” on page 395](#).
- Clear the selected content filtering profiles—Click **Clear All Selections** to clear any content filtering profiles that you might have selected.
- View the details of a content filtering profile—Select the content filtering profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The Content Filtering Profile Details page appears. [Table 137 on page 390](#) describes the fields on this page.
- Search for content filtering profiles by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

### Field Descriptions

[Table 136 on page 390](#) describes the fields on the Content Filtering Profiles page.

**Table 136: Content Filtering Profiles Page Fields**

Field	Description
Name	Name of the content filtering profile.
Permit Command List	List of protocol commands permitted by the content filtering profile.
Block Command List	List of protocol commands blocked by the content filtering profile.
Notification Type	Type of notification that is sent when content is blocked.
Description	Description of the content filtering profile.

**Table 137: Content Filtering Profiles Details Page Fields**

Field	Description
<b>General Information</b>	
Name	Name of the content filtering profile.
Description	Description of the content filtering profile.
<b>General Information</b>	
Notify Mail Sender	Specifies whether the option to notify the e-mail sender is enabled or disabled.

Table 137: Content Filtering Profiles Details Page Fields (*continued*)

Field	Description
Notification Type	Type of notification that is sent when content is blocked.
Custom Notification Message	Custom notification message that is sent when content is blocked.
Protocol Commands	
Command Block List	List of protocol commands permitted by the content filtering profile.
Command Permit List	List of protocol commands blocked by the content filtering profile.
Content Types	
Block Content Types	List of harmful content types to be blocked.
File Extensions	
Extension Block List	File extensions to be blocked.
MIME	
MIME Block List	List of MIME types to be blocked.
MIME Permit List	List of MIME types to be permitted.

## RELATED DOCUMENTATION

| [Creating UTM Profiles](#) | 364

## Creating Content Filtering Profiles

Use the Create Content Filtering Profiles page to configure content filtering profiles. Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, and protocol command. The content filter controls file transfers across the device by checking traffic against configured filter lists. [Table 138 on page 392](#) displays the types of content filters that you can configure as part of a content filtering profile.

**NOTE:** The content filtering profile evaluates traffic before all other UTM profiles. Therefore, if traffic meets criteria configured in the content filter, the content filter acts first upon this traffic.

**Table 138: Supported Content Filter Types**

Type	Description
MIME pattern filter	<p>MIME patterns are used to identify the type of traffic in HTTP and MAIL protocols. There are two lists of MIME patterns that are used by the content filter to determine the action to be taken. The block MIME list contains a list of MIME type traffic that is to be blocked. The MIME exception list contains MIME patterns that are not to be blocked by the content filter and are generally subsets of items on the block list.</p> <p><b>NOTE:</b> The exception list has a higher priority than the block list.</p>
Block Extension List	<p>Because the name of a file is available during the transfers, using file extensions is a highly practical way to block or allow file transfers. All protocols support the use of the block extension list.</p>
Protocol Command Block and Permit Lists	<p>Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, traffic can be controlled on the protocol command level. The block or permit command lists are intended to be used in combination, with the permit list acting as an exception list to the block list.</p> <p><b>NOTE:</b> If a protocol command appears on both the permit list and the block list, the command is permitted.</p>

To create a content filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears.

2. Click the add icon (+) to create a new content filtering profile.

The Create Content Filtering Profiles wizard appears, displaying brief instructions about creating a content filtering profile.

3. Click **Next** to navigate to the next page.

4. Complete the configuration according to the guidelines provided in [Table 139 on page 393](#).

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

5. Click **Finish**.

A summary page is displayed. Review the settings and if you need to make any modifications click the **Edit** link or the **Back** button.

6. Click **OK** save the settings and create the profile.

A message indicating the status of the create operation is displayed.

7. Click **Close**.

You are returned to the Content Filtering Profiles page.

**Table 139: Content Filtering Profile Settings**

Setting	Guideline
<b>General Information</b>	
Name	Enter a unique name for the content filtering profile. The maximum length is 29 characters.
Description	Enter a description for the content filtering profile. The maximum length is 255 characters.
<b>Notification Options</b>	
Notify Mail Sender	Select this check box if you want to notify the sender when a failure occurs or a virus is detected. This check box is cleared by default.
Notification Type	Select the type of notification ( <b>Protocol</b> or <b>Message</b> ) from the drop-down list.
Custom Notification Message	Enter a custom notification message. The maximum length is 512 characters.
<b>Protocol Commands</b>	
Command Block List	<p>Enter the protocol commands to be blocked for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.</p> <p>Protocol commands allow you to control traffic at the protocol-command level.</p>

Table 139: Content Filtering Profile Settings (*continued*)

Setting	Guideline
<b>Command Permit List</b>	Enter specific commands to be permitted for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.
<b>Content Types</b>	
<b>Block Content Type</b>	<p>Use the content filter to block other types of harmful files that the MIME type or the file extension cannot control. Select from the following types of content blocking (supported only for HTTP):</p> <ul style="list-style-type: none"> <li>• Active X</li> <li>• Windows executables (.exe)</li> <li>• HTTP cookie</li> <li>• Java applet</li> <li>• ZIP files</li> </ul>
<b>File Extensions</b>	
<b>Extension Block List</b>	<p>Use a file extension list to define a set of file extensions to block over HTTP, FTP, SMTP, IMAP, and POP3.</p> <p>Enter file extensions to block separated by commas. For example, exe, pdf, js, and so on.</p>
<b>MIME Types</b>	
<b>MIME Block List</b>	Enter the MIME types you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.
<b>MIME Permit List</b>	Enter the MIME types you want to permit over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.

## RELATED DOCUMENTATION

[Creating UTM Profiles](#) | 364



## Editing, Cloning, and Deleting Content Filtering Profiles

### IN THIS SECTION

- [Editing Content Filtering Profiles | 395](#)
- [Cloning Content Filtering Profiles | 395](#)
- [Deleting Content Filtering Profiles | 396](#)

You can edit, clone, and delete content filtering profiles from the Content Filtering Profiles page. This topic has the following sections:

### Editing Content Filtering Profiles

To modify the parameters configured for a content filtering profile:

**NOTE:** You cannot modify the default profiles already present in the system.

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select the content filtering profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.

3. Modify the content filtering profile fields as needed.

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

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the edit operation.

### Cloning Content Filtering Profiles

Cloning enables you to easily create a new content filtering profile based on an existing one.

To clone a content filtering profile:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select the content filtering profile that you want to clone and then select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone Content Filtering Profiles page appears, displaying the same fields that are presented when you create a content filtering profile.

3. Modify the content filtering profile fields as needed.

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

You are taken to the Content Filtering Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting Content Filtering Profiles

Before deleting a content filtering profile, ensure that the profile is not used in a UTM profile that is, in turn, used in a firewall policy intent. If you try to delete a content filtering profile that is used in a firewall policy intent, an error message is displayed.

To delete one or more content filtering profiles:

1. Select **Configuration > Unified Threat Mgmt > Content Filtering Profiles** in Customer Portal.

The Content Filtering Profiles page appears, displaying the existing content filtering profiles.

2. Select one or more content filtering profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete Profile**.

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

3. Click **Yes** to delete the selected content filtering profiles.

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

## RELATED DOCUMENTATION

| [Creating Content Filtering Profiles](#) | 391

## About the URL Patterns Page

To access this page, select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

Use this page to view, create, edit, clone, and delete URL patterns. A URL pattern contains a list of URLs.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL pattern—See [“Creating URL Patterns” on page 398](#).
- Edit, clone, or delete a URL pattern—See [“Editing, Cloning, and Deleting URL Patterns” on page 399](#).
- Clear the selected URL patterns—Click **Clear All Selections** to clear any URL patterns that you might have selected.
- View the details of a URL pattern—Select the URL pattern for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Pattern Details page appears displaying the fields shown in [Table 140 on page 397](#).
- Search for URL patterns using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

### Field Descriptions

[Table 140 on page 397](#) describes the fields on the URL Patterns page.

Table 140: URL Patterns Page Fields

Field	Description
Name	Name of the URL pattern.
URLs	List of URLs in the URL pattern.
Description	Description of the URL pattern.

### RELATED DOCUMENTATION

[About the URL Categories Page](#) | 401

## Creating URL Patterns

Use this page to create URL patterns. You can also assign URL patterns to a URL category.

To create a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears.

2. Click the add icon (+) to create a URL pattern.

The Create URL Patterns page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 141 on page 398](#).

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

4. Click **OK**.

A new URL pattern is created and you are returned to the URL Patterns page.

**Table 141: Create URL Patterns Settings**

Settings	Guidelines
Name	Enter a unique name for the URL pattern.  The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 29 characters.
Description	Enter a description for the URL pattern. The maximum length is 255 characters.
URL Category	Select the URL category to which you want to assign the URL pattern. Alternatively, click <b>Create New URL Category</b> to create a URL category, enter the URL category name in the text box, and click <b>Save</b> to assign the URL pattern to the new category.

Table 141: Create URL Patterns Settings (continued)

Settings	Guidelines
Add URLs	<p>Enter one or more URLs (separated by commas) in the text box, and click <b>Add</b>. The URLs are displayed in the URL List table.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"><li>• The following wildcard characters are supported:<ul style="list-style-type: none"><li>• asterisk (*)</li><li>• period (.)</li><li>• square brackets ([])</li><li>• question mark (?)</li></ul></li><li>• Precede all wildcard characters with http://.</li><li>• The asterisk (*) can only be used at the beginning of a URL and must be followed by a period (.).</li><li>• The question mark (?) can only be used at the end of a URL.</li><li>• The following are examples of wildcard syntaxes that are supported: http://*.example.net, http://www.example.ne?, and http://www.example.n??.</li><li>• The following are examples of wildcard syntaxes that are not supported: *.example.???, http://*example.net, http://?, and www.example.ne?.</li></ul>

RELATED DOCUMENTATION

| [Creating URL Categories](#) | 402

Editing, Cloning, and Deleting URL Patterns

IN THIS SECTION

- [Editing URL Patterns](#) | 400
- [Cloning URL Patterns](#) | 400
- [Deleting URL Patterns](#) | 401

You can edit, clone, and delete URL patterns from the URL Patterns page. This topic has the following sections:

## Editing URL Patterns

To modify the parameters configured for a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to edit and click the edit icon (pencil). Alternatively, right-click a pattern and select **Edit URL Patterns**.

The Edit URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

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

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the edit operation.

## Cloning URL Patterns

Cloning enables you to easily create a new URL pattern based on an existing one.

To clone a URL pattern:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select the URL pattern that you want to clone and then select **More > Clone**. Alternatively, right-click a pattern and select **Clone**.

The Clone URL Patterns page appears, displaying the same fields that are presented when you create a URL pattern.

3. Modify the URL pattern fields as needed.

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

You are taken to the URL Patterns page. A confirmation message appears, indicating the status of the clone operation.

## Deleting URL Patterns

Before deleting a URL pattern, ensure that the URL pattern is not referenced in any UTM profiles that are, in turn, used in firewall policy intents or in URL categories referenced in the UTM settings. If you try to delete such a URL pattern, an error message is displayed.

To delete one or more URL patterns:

1. Select **Configuration > Unified Threat Mgmt > URL Patterns** in Customer Portal.

The URL Patterns page appears, displaying the existing URL patterns.

2. Select one or more URL patterns that you want to delete and click the delete icon (X). Alternatively, right-click a pattern and select **Delete URL Pattern**.

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

3. Click **Yes** to delete the selected URL patterns.

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

### RELATED DOCUMENTATION

| [Creating URL Patterns](#) | 398

## About the URL Categories Page

To access this page, select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

Use this page to view, create, edit, clone, and delete URL categories. A URL category is a list of URL patterns grouped under a single title.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a URL category—See [“Creating URL Categories”](#) on page 402.
- Edit, clone, or delete a URL category—See [“Editing, Cloning, and Deleting URL Categories”](#) on page 404.
- Clear the selected URL categories—Click **Clear All Selections** to clear any URL categories that you might have selected.

- View the details of a URL category—Select the URL category for which you want to view the details and from the More or right-click menu, select **Detailed View**. The URL Category Details page appears, displaying the details of the selected URL category; see [Table 142 on page 402](#) for an explanation of the fields.
- Search for URL categories by using keywords—Click the search icon, enter the search term in the text box, and press Enter. The search results are displayed on the same page.

Field Descriptions

[Table 142 on page 402](#) describes the fields on the URL Categories page.

Table 142: URL Categories Page Fields

Field	Description
Name	Name of the URL category.
URL Patterns	List of URL patterns in the URL category.
Definition Type	Indicates the type of URL category: <ul style="list-style-type: none"><li>• Predefined—URL categories that are loaded by default.</li><li>• Custom—URL categories that are created by the user.</li></ul>
Description	Description of the URL category.

RELATED DOCUMENTATION

[About the URL Patterns Page](#) | 397

Creating URL Categories

Use this page to create URL categories. A URL category is a list of URL patterns grouped under a single title.



To create a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears.

2. Click the add icon (+) to create a URL category.

The Create URL Categories page is displayed.

3. Complete the configuration according to the guidelines provided in [Table 143 on page 403](#).

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

4. Click **OK**.

A new URL category is created and you are returned to the URL Categories page.

**Table 143: Create URL Categories Settings**

Settings	Guidelines
Name	<p>Enter a unique name for the URL category.</p> <p>The name must begin with a letter or an underscore (_) and can contain alphanumeric characters and some special characters (_ -). The maximum length is 59 characters.</p>
Description	<p>Enter a description for the URL pattern. The maximum length is 255 characters.</p>
URL Patterns	<p>Select one or more URL patterns in the <b>Available</b> column and click the forward arrow to confirm your selection. The selected URL patterns are displayed in the <b>Selected</b> column.</p> <p>Alternatively, click <b>Create a New Pattern</b> to create a URL pattern and assign it to the URL category. The Create URL Patterns page appears. For more information, see <a href="#">“Creating URL Patterns” on page 398</a></p> <p><b>NOTE:</b> You must select at least one URL pattern.</p>

## RELATED DOCUMENTATION

## Editing, Cloning, and Deleting URL Categories

### IN THIS SECTION

- [Editing URL Categories | 404](#)
- [Cloning URL Categories | 404](#)
- [Deleting URL Categories | 405](#)

You can edit, clone, and delete URL categories from the URL Categories page. This topic has the following sections:

### Editing URL Categories

To modify the parameters configured for a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select the URL category that you want to edit and click the edit icon (pencil). Alternatively, right-click a category and select **Edit URL Categories**.

The Edit URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.

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

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the edit operation.

### Cloning URL Categories

Cloning enables you to easily create a new URL category based on an existing one.

To clone a URL category:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select the URL category that you want to clone and then select **More > Clone**. Alternatively, right-click a category and select **Clone**.

The Clone URL Categories page appears, displaying the same fields that are presented when you create a URL category.

3. Modify the URL category fields as needed.

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

You are taken to the URL Categories page. A confirmation message appears, indicating the status of the clone operation.

## Deleting URL Categories

Before deleting a URL category, ensure that the URL category is not referenced in any UTM profiles that are, in turn, used in firewall policy intents or in the UTM settings. If you try to delete such a URL category, an error message is displayed.

To delete one or more URL categories:

1. Select **Configuration > Unified Threat Mgmt > URL Categories** in Customer Portal.

The URL Categories page appears, displaying the existing URL categories.

2. Select one or more URL categories that you want to delete and click the delete icon (X). Alternatively, right-click a category and select **Delete URL Category**.

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

3. Click **Yes** to delete the selected URL categories.

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

## RELATED DOCUMENTATION

| [Creating URL Categories](#) | 402

# Managing SLA Profiles and SD-WAN Policies

## IN THIS CHAPTER

- [SLA Profiles and SD-WAN Policies Overview | 406](#)
- [About the SD-WAN Policy Page | 410](#)
- [Creating SD-WAN Policy Intents | 412](#)
- [Editing and Deleting SD-WAN Policy Intents | 419](#)
- [About the SLA-Based Steering Profiles Page | 420](#)
- [Adding SLA-Based Steering Profiles | 424](#)
- [Editing and Deleting SLA-Based Steering Profiles | 431](#)
- [About the Path-Based Steering Profiles Page | 432](#)
- [Adding Path-Based Steering Profiles | 435](#)
- [Editing and Deleting Path-Based Steering Profiles | 437](#)
- [Breakout and Breakout Profiles Overview | 439](#)
- [About the Breakout Profiles Page | 441](#)
- [Adding Breakout Profiles | 445](#)
- [Adding Cloud Breakout Settings | 447](#)
- [Assigning Cloud Breakout Settings to Sites | 449](#)
- [Editing Breakout Profiles and Cloud Breakout Settings | 450](#)
- [Deleting Breakout Profiles and Cloud Breakout Settings | 452](#)
- [Configuring Breakout on SD-WAN Sites | 453](#)

## SLA Profiles and SD-WAN Policies Overview

### IN THIS SECTION

- [SLA Profiles | 407](#)
- [SD-WAN Policies | 408](#)

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 144 on page 407](#) lists the categories of configurable constraints that are defined in an SLA profile.

**Table 144: SLA Profile Categories**

Category	Description
SLA profile parameters	<p>You can define one or more than one of the following SLA profile parameters:</p> <ul style="list-style-type: none"> <li>• SLA Configuration—Whether to use recommended or custom values for the SLA threshold and SLA parameters.</li> <li>• SLA Threshold—Whether to use, liberal, baseline, or conservative settings for the threshold.</li> <li>• SLA parameters: <ul style="list-style-type: none"> <li>• Packet loss—Percentage of data packets dropped by the network to manage congestion.</li> <li>• RTT—Target round-trip time (RTT) for the SLA profile.</li> <li>• Jitter—Difference between the maximum and minimum round-trip times (in ms) of a packet of data.</li> </ul> </li> </ul>
Path preference and failover	<p>Paths are the WAN links to be used for the SLA profile. You can select MPLS, Internet, or any link as the preferred path. MPLS is more latency-sensitive than Internet.</p> <p>You can trigger the path failover criteria when any of the SLA parameters is violated.or when all the SLA parameters are violated.</p>
Class of service	<p>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.</p>
Rate limiters	<p>Rate limiters are defined for traffic shaping and efficient bandwidth utilization. You can define the following rate limiters:</p> <ul style="list-style-type: none"> <li>• Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile.</li> <li>• 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.</li> </ul>

**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

Applications are classified into the following categories:

- **Cacheable applications**, which refer to applications or application groups that are stored in the application cache when they are recognized by the device. After they are stored in the application cache, subsequent sessions are routed directly through the correct WAN link.
- **Non-cacheable applications**, which refer to applications or application groups that are not stored in the application cache and all sessions are first routed through the default path, and then routed to the correct WAN link based on the SD-WAN policy.

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.
- **Traffic Steering Profile**—Depending on whether you want to apply the policy intent to site-to-site traffic or breakout traffic, you can associate the traffic steering profile with the policy intent. The following options are available:
  - **SLA-based steering profile**— Applicable for site-to-site traffic
  - **Path-based steering profile**— Applicable for site-to-site traffic
  - **Breakout profile**—Applicable for breakout traffic (local, central, or cloud).
- **Intent name**—A unique name for the SD-WAN policy intent.

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

For example, consider an application in a site. If you want the application group to use custom throughput, latency, or jitter, you can create an SLA profile with these custom values. You can then create an intent

and configure the intent with the application and apply the custom SLA profile. When the intent is deployed, CSO determines the best suited WAN link to route traffic based in the application. If the WAN link fails to meet SLA requirements in runtime, the SD-WAN network switches WAN links to the next best suited path.

On the basis of the configured traffic-based steering profile constraints, you can categorize SD-WAN policies into three types:

- **Path-based steering policy**—If only the path preference is defined and none of the SLA parameters are defined in the SLA profile, then the policy is called a path-based steering policy. In path-based steering profile, you can define the path (MPLS or Internet) that must be used for a given traffic type profile. You cannot configure SLA parameters or path failover criteria for a path-based steering profile. The traffic type profile must be in enabled state in order to be used in any profile.
- **SLA-based steering policy**—If one or more SLA parameters in the SLA profile are defined, then the policy is called an SLA-based steering policy. In an SLA-based steering profile, each profile is associated with a traffic type profile and tracks the SLA parameters such as packet loss, Jitter and RTT. The traffic type profile must be in enabled state in order to be used in any profile. Based on your requirements, you can choose the recommended SLA threshold or enter custom SLA threshold for the traffic type profile. You can even set the path preference (Any, MPLS, or Internet) to switch traffic from one WAN interface to another based on the path failover criteria.

When an intent is deployed on a site, if the WAN link chosen by the SD-WAN network does not meet the SLA requirements and the network performance deteriorates, then the site switches WAN links to meet the SLA requirements. The link switching is recorded as an SD-WAN event and displayed in the SD-WAN Events page in the customer portal and the *Tenant\_name* SLA Performance pages in the administration and customer portals.

- **Breakout policy**—If local breakout, central breakout, or cloud breakout parameters are defined, then the policy is called a breakout policy.

## RELATED DOCUMENTATION

*About the Application SLA Profiles Page*

[About the SD-WAN Policy Page | 410](#)

[Breakout and Breakout Profiles Overview | 439](#)

[SD-WAN Events Overview | 667](#)

## About the SD-WAN Policy Page

To access this page, select **Configuration > SD-WAN > SD-WAN Policy** in the Customer Portal.

SD-WAN policy intents help in optimum utilization of the WAN links and efficient load distribution of traffic. SD-WAN policy intents are applied to source endpoints (such as sites and departments) and destination endpoints (applications or application groups) and can be defined for site-to-site traffic (by using SLA profiles) or for breakout traffic (by using breakout profiles).

You can use the SD-WAN Policy page to view, create, edit, and deploy SD-WAN policy intents. SD-WAN policy intents use SLA profiles 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.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View existing SD-WAN policy intents. CSO provides pre-defined SD-WAN policy intents for the tenants. See [Table 146 on page 411](#).

**NOTE:** The pre-defined SD-WAN policy intents are available for the tenants only if the SP administrator has downloaded the signature database prior to creating the tenants.

- Create SD-WAN policy intents. See [“Creating SD-WAN Policy Intents” on page 412](#).
- Edit or delete SD-WAN policy intents. See [“Editing and Deleting SD-WAN Policy Intents” on page 419](#).
- Deploy SD-WAN policy intents. See [“Deploying Policies” on page 548](#).
- View the number of undeployed SD-WAN policy intents.
- Search for SD-WAN policy intents 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 145 on page 410](#) describes the fields on the SD-WAN Policy page.

**Table 145: Fields on the SD-WAN Policy Page**

Field	Description
Name	Displays the name of the SD-WAN policy intent.



Table 145: Fields on the SD-WAN Policy Page (continued)

Field	Description
Source	Displays the source endpoints that are configured for the policy intents. A source endpoint is chosen from sites, site groups, and departments or a combination of all of these to which the policy intent is applied.
Application	Displays the application destination endpoints that are configured for the policy intents. An application destination endpoint is chosen from a list of applications and predefined or custom application groups to which the policy intent is applied.
Traffic Steering Profile	Displays the breakout profile or the SLA profile associated with the policy intent.

Table 146: Pre-defined SD-WAN Policies

SD-WAN Policy Name	Applicable Sites	Application	Traffic Steering Profile
System-1	All Sites	CSO-Collaboration	CSO-AV
System-2	All Sites	CSO-Security	CSO-Sec
System-3	All Sites	CSO-Collaboration	CSO-Email
System-4	All Sites	CSO-Productivity	CSO-Productive
System-5	All Sites	CSO-File-Share	CSO-FileShare

## RELATED DOCUMENTATION

[SLA Profiles and SD-WAN Policies Overview | 406](#)
[Creating SD-WAN Policy Intents | 412](#)
[Editing and Deleting SD-WAN Policy Intents | 419](#)

## Creating SD-WAN Policy Intents

You can create policy intents for SD-WAN policies from the **SD-WAN Policy** page.

To create an SD-WAN policy intent:

1. Select **Configuration > SD-WAN > SD-WAN Policy** in Customer Portal.

The SD-WAN Policy page appears.

2. Click the add icon (+).

The options to create policy intents appear inline on the SD-WAN Policy page.

3. Enter the policy intent information according to the guidelines provided in [Table 147 on page 413](#).

4. Click **Save** to create the policy intent.

The SD-WAN policy intent is saved and a confirmation message is displayed.

**NOTE:** After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications. When an SD-WAN policy intent is created, the Undeployed field is incremented by one indicating that intents are pending deployment.

Table 147: Create SD-WAN Policy Intent Settings

Field	Guidelines
Source	

Table 147: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>You can select the source endpoints in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Select source endpoints from the displayed list of departments, sites, or site groups, or a combination of these. Click the source endpoints to select them.</li> <li>• Select the source endpoints from the complete list of departments, sites, and site groups.</li> </ul> <p>To view the complete list of departments, sites, and site groups.</p> <ol style="list-style-type: none"> <li>1. Click <b>View more results</b>. The complete list of departments, sites, and site groups is displayed in the <b>End Points</b> pane on the right.</li> <li>2. (Optional) Hover over a department or site group and click the edit icon to edit the department or site group. You cannot edit a site.</li> <li>3. Click the add icon (+) to select the endpoint.</li> </ol> <ul style="list-style-type: none"> <li>• Enter an abbreviation in the <b>Source</b> field to select the endpoint from a filtered list of departments, sites, or site groups. To view a filtered list of departments, sites, or site groups, enter DEPT, SITE, or STGP, respectively. The abbreviation is not case-sensitive. You can select the source endpoint in one of the following ways: <ul style="list-style-type: none"> <li>• Click the endpoints in the filtered list to select them.</li> <li>• Click <b>View more results</b> to select the endpoint from the complete list of departments, sites, and site groups.</li> <li>• Click <b>Add new department</b> or <b>Add new sitegroup</b> to create new departments or site groups and select them. The Create Site Group page or Add Department page appears based on your selection. See <a href="#">“Adding a Department” on page 602</a> and <a href="#">“Creating Site Groups” on page 145</a> for information about creating site groups and departments.</li> </ul> </li> <li>• Create site groups or departments to select the source endpoint from the newly created site group or department.</li> </ul> <p>To create site groups or departments:</p> <ol style="list-style-type: none"> <li>1. Click anywhere within the <b>Source</b> field.</li> <li>2. Click the lesser-than icon (&lt;) on the right. <p>The list of available departments, sites, and site groups is displayed in the <b>End Points</b> pane on the right.</p> </li> <li>3. (Optional) To view more information about a source endpoint, hover over the endpoint click the details icon.</li> <li>4. Click the add icon (+) on the top right of the pane.</li> </ol>

Table 147: Create SD-WAN Policy Intent Settings (continued)

Field	Guidelines
	<div>5. Click <b>Department</b> or <b>Site Group</b> as needed. The Add Department page or Create Site Group page appears based on your selection. See <a href="#">“Adding a Department” on page 602</a> and <a href="#">“Creating Site Groups” on page 145</a> for information about creating departments and site groups.</div> <div>6. Click the check mark icon (✓) if you want to save the department or site group to the policy intent. Alternatively, if you want to discard your updates, click <b>Cancel</b> instead.</div>

Table 147: Create SD-WAN Policy Intent Settings (continued)

Field	Guidelines
Application	

Table 147: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>You can select the application endpoints in one of the following ways:</p> <p><b>NOTE:</b> You can select <b>Any</b> as an application endpoint only if you are creating an SD-WAN policy intent that references a breakout profile.</p> <ul style="list-style-type: none"> <li>• Select application endpoints from the displayed list of applications and application groups. Click the endpoints to select them.</li> <li>• Select the application endpoints from the complete list of applications and application groups. To view the complete list of applications and applications groups. <ol style="list-style-type: none"> <li>1. Click <b>View more results</b>. The complete list of applications and applications groups is displayed in the <b>End Points</b> pane on the right.</li> <li>2. (Optional) Hover over an application group and click the edit icon to edit the application group.</li> <li>3. (Optional) Hover over an application and click the details icon to view details about the application.</li> <li>4. Click the add icon (+) to select the endpoint.</li> </ol> </li> <li>• Enter an abbreviation in the <b>Application</b> field to select the endpoint from a filtered list of applications and application groups. To view a filtered list of applications and application groups, enter apps or APPS. You can select the application endpoint in one of the following ways: <ul style="list-style-type: none"> <li>• Click the endpoints in the filtered list to select them.</li> <li>• Click <b>View more results</b> to select the endpoint from the complete list of applications and applications groups.</li> <li>• Click <b>Add new application</b> to create a new application group and select the application group. The Create Application Signature Group page appears. See <a href="#">“Adding Application Signature Groups” on page 599</a> for information about creating application groups.</li> </ul> </li> <li>• Create custom application groups to select the application endpoint from the newly created application group. To create an application group: <ol style="list-style-type: none"> <li>1. Click anywhere within the <b>Application</b> field.</li> <li>2. Click the lesser-than icon (&lt;) on the right.  The list of available applications, departments, sites, and site groups is displayed in the <b>End Points</b> pane on the right.</li> <li>3. Click the add icon (+) on the top right of the pane.</li> </ol> </li> </ul>

Table 147: Create SD-WAN Policy Intent Settings (*continued*)

Field	Guidelines
	<p>4. Click <b>Application</b>. The Create Application Signature Group page appears. See <a href="#">“Adding Application Signature Groups” on page 599</a> for information about creating application groups.</p> <p>5. Click the check mark icon (✓) if you want to save the application signature group to the policy intent.</p> <p>Alternatively, if you want to discard your updates, click <b>Cancel</b> instead.</p>
Traffic Steering Profile	<p>Select a breakout profile, SLA-based profile, or a path-based profile to apply to the source and application endpoints. You can select the profile in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Select the breakout profile, SLA-based profile, or the path-based profile from the displayed list of profiles. Click the profile to select it.</li> <li>• Select the profile from the complete list of breakout, SLA-based, or path-based profiles: To view the complete list of breakout, SLA-based, or path-based profiles. <ol style="list-style-type: none"> <li>1. Click <b>View more results</b>. The complete list of profiles is displayed in the <b>End Points</b> pane on the right.</li> <li>2. Click the add icon (+) to select the profile.</li> </ol> </li> <li>• Select the profile by creating a custom SLA-based, path-based, or breakout profile: <ul style="list-style-type: none"> <li>• To create a breakout profile: <ol style="list-style-type: none"> <li>1. Click anywhere within the Profile field.</li> <li>2. Click the lesser-than icon (&lt;) on the right. The list of breakout profiles is displayed in the <b>End Points</b> pane on the right.</li> <li>3. Click the add icon (+) on the top right of the pane and select <b>BRKT</b>. The Add Breakout Profile page appears. For more information, see <a href="#">“Adding Breakout Profiles” on page 445</a></li> </ol> </li> </ul> </li> </ul>
Options	
Name	Enter a name for the policy intent.
Description	Enter a description for the policy intent.



## RELATED DOCUMENTATION

[SLA Profiles and SD-WAN Policies Overview | 406](#)

[About the SD-WAN Policy Page | 410](#)

[Editing and Deleting SD-WAN Policy Intents | 419](#)

[Deploying Policies | 548](#)

## Editing and Deleting SD-WAN Policy Intents

### IN THIS SECTION

- [Editing SD-WAN Policy Intents | 419](#)
- [Deleting SD-WAN Policy Intents | 420](#)

You can edit or delete SD-WAN policy intents from the SD-WAN Policy page.

### Editing SD-WAN Policy Intents

You can edit SD-WAN policy intents from the SD-WAN Policy page.

To edit an SD-WAN policy intent:

1. Hover over the SD-WAN policy intent that you want to edit, and then click the edit icon that appears on the right side of the policy intent.

The options to create policy intents appear within the SD-WAN Policy page showing the same options that you see when you create a new SD-WAN policy intent.

2. Modify the parameters according to the guidelines provided in [“Creating SD-WAN Policy Intents” on page 412](#).
3. Click **Save** to save your changes.

Alternatively, click **Cancel** to discard your changes.

**NOTE:** After you modify an SD-WAN policy intent, you must redeploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications.

## Deleting SD-WAN Policy Intents

If an SD-WAN intent is no longer needed, you can delete the SD-WAN policy intent from the SD-WAN Policy page.

To delete one or more SD-WAN policy intents:

1. Select one or more policy intents that you want to delete and click the delete icon (trash can).

A page appears asking you to confirm the delete operation.

2. Click **Yes** to confirm that you want to delete the selected policy intents.

A confirmation message appears indicating the status of the delete operation.

**NOTE:** After you delete one or more SD-WAN policy intents, you must redeploy the policy to ensure that the changes take effect on the applicable sites, departments, or applications.

### RELATED DOCUMENTATION

[SLA Profiles and SD-WAN Policies Overview | 406](#)

[About the SD-WAN Policy Page | 410](#)

[Creating SD-WAN Policy Intents | 412](#)

## About the SLA-Based Steering Profiles Page

To access this page, select **Configuration > SD-WAN > SLA-Based Steering Profiles** in the Customer Portal.

You can use the SLA-Based Steering Profiles page to view information about service-level agreement (SLA)-based steering for the tenant profile in which you are logged in.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details of SLA profiles for the tenants.
- Add an SLA-based steering profile for the tenant. See [“Adding SLA-Based Steering Profiles” on page 424](#).

- Edit or delete an SLA-based steering profile. See [“Editing and Deleting SLA-Based Steering Profiles” on page 431](#).
- Show or hide columns that contain information about SLA-based steering profiles. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for SLA-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

## Field Descriptions

[Table 148 on page 421](#) shows the descriptions of the fields on the SLA-Based Steering Profiles page.

**Table 148: Fields on the SLA-Based Steering Profiles Page**

Field	Description	Displayed On
Name	Name of the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)  Detail for <i>SLA-Profile-Name</i> pane
Priority	Priority of the SLA-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for <i>SLA-Profile-Name</i> pane
Traffic Type Profile	Indicates the traffic type profile associated with the SLA-based steering profile. <ul style="list-style-type: none"> <li>• VOICE-VIDEO</li> <li>• HIGH_PRIORITY_VIDEO</li> <li>• HOSTED_AV</li> <li>• PREMIUM_INTERNET</li> <li>• INTERNET</li> </ul>	SLA-Based Steering Profiles page (SLA Profiles List tab)  Detail for <i>SLA-Profile-Name</i> pane
Packet Loss (%)	Target packet loss for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)  Detail for <i>SLA-Profile-Name</i> pane
Jitter (ms)	Target jitter for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)  Detail for <i>SLA-Profile-Name</i> pane

Table 148: Fields on the SLA-Based Steering Profiles Page (*continued*)

Field	Description	Displayed On
RTT	Target round-trip time (RTT) for the SLA profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)  Detail for <i>SLA-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>SLA-Profile-Name</i> pane
Created By	Name of the user who created the SLA-based steering profile.	SLA-Based Steering Profiles page (SLA Profiles List tab)
Path Preference	The preferred path for the SLA profile. The available options are: <ul style="list-style-type: none"> <li>• MPLS</li> <li>• Internet</li> <li>• Any (default)</li> </ul>	Detail for <i>SLA-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>SLA-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>SLA-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the SLA violations are counted.	Detail for <i>SLA-Profile-Name</i> pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for <i>SLA-Profile-Name</i> pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the SLA parameters is violated or when all (All) the SLA parameters are violated.	Detail for <i>SLA-Profile-Name</i> pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the SLA-based steering profile.	Detail for <i>SLA-Profile-Name</i> pane

Table 148: Fields on the SLA-Based Steering Profiles Page (continued)

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

RELATED DOCUMENTATION

| [SLA Profiles and SD-WAN Policies Overview](#) | 406

## Adding SLA-Based Steering Profiles

You can use the Add SLA Profile page to add a new service-level agreement (SLA)-based steering profile, specify the traffic type profile, SLA configuration, SLA threshold, SLA parameters, path selection criteria, and rate limiting parameters for the profile. [Table 149 on page 425](#) lists the SLA-based steering profiles that are tuned for specific application categories and traffic types.

**Table 149: Predefined SLA-Based Steering Profiles**

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-AV	VOICE-VIDEO	CSO_Collaboration_AV	Skype for Business Zoom Video GotoMeeting Jive Jabber Citrix Online WebEx Zoho Meeting Google Hangout Adobe Connect

Table 149: Predefined SLA-Based Steering Profiles (continued)

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Productivity	PREMIUM-INTERNET	CSO_Productivity	ERP: Salesforce, Oracle, SAP Office365 (including SharePoint) Zendesk HRPayroll Zoho Office Suite Slack Square Concur Adobe Quickbooks Freshbooks Workday Project Management-MS PJ Basecamp Asana
CSO-Security	INTERNET	CSO_Security	Symantec McAfee Sophos Zonealarm Lookout



Table 149: Predefined SLA-Based Steering Profiles (continued)

SLA-Based Steering Profiles	Traffic Type	Application Group	Applications Supported
CSO-Email	PREMIUM-INTERNET	CSO_Collaboration_Email	MS Exchange IMAP POP3 Gmail OWA Yahoo
CSO-FileShare	INTERNET	CSO_File_Share	Box Dropbox Gsuite OneDrive Skype for Business-File Transfer Zoho Share

To add an SLA-based steering profile to the tenant:

1. Select **Configuration > SD-WAN > SLA-Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Click the add icon (+).

The Add SLA Profile page appears.

3. Enter the SLA profile information according to the guidelines provided in [Table 150 on page 428](#).

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

4. Click **OK** to add the SLA profile.

The SLA-Based Steering Profiles page appears with the new SLA profile information. You are returned to the SLA-Based Steering Profiles page and a confirmation message indicating that the SLA-based

steering profile was added is displayed. The page refreshes to display the SLA-based steering profile that you added.

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

**NOTE:** After you add an SLA-based steering profile, you must add an SD-WAN policy intent that references the SLA-based steering profile in order to enable site-to-site traffic.

**Table 150: Fields on the Add SLA Profile page**

Field	Guidelines
<i>General</i>	
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the <b>Enabled</b> state.
SLA Configuration	Choose one of the following options: <ul style="list-style-type: none"> <li>● <b>Use Recommended:</b> To use the default SLA threshold and SLA parameters for the SLA-based steering profile.</li> <li>● <b>Enter Custom:</b> To specify customized values for SLA configuration and SLA parameters for the SLA-based steering profiles.</li> </ul>
SLA Threshold	Choose one of the following options: <ul style="list-style-type: none"> <li>● <b>Liberal</b>—To use a relaxed SLA threshold.</li> <li>● <b>Baseline</b>—To use the default SLA threshold.</li> <li>● <b>Conservative</b>—To use a strict SLA threshold.</li> </ul>
<i>SLA Parameters</i>	
Packet Loss	Enter the target packet loss (in %) for the SLA-based steering profile. Packet loss is the percentage of data packets dropped by the network to manage congestion.
RTT	Enter the target round-trip time (RTT) for the SLA-based steering profile.
Jitter	Enter the target jitter (in ms) for the SLA-based steering profile. Jitter is the difference between the maximum and minimum round-trip times of a packet of data.

Table 150: Fields on the Add SLA Profile page (continued)

Field	Guidelines
<i>Path Selection Criteria</i>	
Path Preference	<p>Select the preferred WAN link type to associate with the SLA profile. The options are Any, MPLS, and Internet. Any is the default value.</p> <p>Select the preferred path (MPLS, Internet, or Any) to be used for site-to-site traffic.</p> <p>If a WAN link type that matches the preferred path is enabled for site-to-site traffic, then that WAN link type is used for site-to-site traffic.</p> <p>If you specify that any path can be used, then there is no preference and all site-to-site-traffic-enabled links are used in a load-balancing mode.</p>
Path Failover Criteria	<p>Specify the failover criteria to determine how links are switched when the active links fail to meet the SLA criteria. In such cases, the traffic is routed to links that meet SLA criteria. Failover is supported only for MPLS or Internet links.</p> <p><b>NOTE:</b> Path failover is supported only for bandwidth-optimized SD-WAN networks.</p> <p>Choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Does not meet one or more SLA parameters</b>—This triggers the path failover if any of the SLA parameters is violated.</li> <li>• <b>Does not meet all SLA parameters</b>—This triggers the path failover only when all the SLA parameters are violated.</li> </ul>
<i>Advanced Configuration-</i>	
<b>Rate Limiting</b>	
Maximum Upstream Rate	<p>Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile.</p> <p>Range: 64 through 10,485,760 Kbps</p>
Maximum Upstream Burst Size	<p>Enter the maximum upstream burst size (in bytes).</p> <p>Range: 1 through 1,342,177,280 bytes</p>
Maximum Downstream Rate	<p>Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile.</p> <p>Range: 64 through 10,485,760 Kbps</p>

Table 150: Fields on the Add SLA Profile page (continued)

Field	Guidelines
Maximum Downstream Burst Size	Enter the maximum downstream burst size (in bytes).  Range: 1 through 1,342,177,280
Loss Priority	Select a loss priority based on which packets can be dropped or retained when network congestion occurs. The chances of a packet getting dropped is the highest when the loss priority is set to <b>High</b> . Other available values are <b>Medium High</b> , <b>Medium Low</b> , and <b>Low</b> .

*Real Time Optimized Mode Setting*

**NOTE:** The following fields are applicable only for sites configured with the real-time-optimized SD-WAN mode.

SLA Sampling	
Session-sampling %	Enter the matching percentage of sessions for which you want to run the passive probes.
SLA-violation-count	Enter the number of SLA violations after which you want CSO to switch paths. The range is 1 through 32.
Sampling-period	Enter the sampling period, in seconds, for which the SLA violations are counted. The range is 2 through 60.
Switch-cool-off-period	Enter the waiting period, in seconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links. The range is 5 through 300.

## RELATED DOCUMENTATION

[SLA Profiles and SD-WAN Policies Overview | 406](#)

[About the SLA-Based Steering Profiles Page | 420](#)

[Editing and Deleting SLA-Based Steering Profiles | 431](#)

## Editing and Deleting SLA-Based Steering Profiles

### IN THIS SECTION

- [Editing an SLA-Based Steering Profile | 431](#)
- [Deleting SLA-Based Steering Profiles | 432](#)

You can use the SLA-Based Steering Profiles page to edit and delete SLA profiles.

**NOTE:** You cannot edit the predefined SLA-Based steering profiles that are automatically created by Contrail Service Orchestration (CSO).

### Editing an SLA-Based Steering Profile

To edit an SLA-based steering profile:

**NOTE:** If you edit an SLA-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > SLA-Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profile that you want to edit, and click the Edit (pencil) icon.

The Edit SLA Profile page appears displaying the same fields that are presented when you add a SLA-based steering profile. For more information, see [“Adding SLA-Based Steering Profiles” on page 424](#).

3. Modify the fields as needed.

**NOTE:** You cannot edit the SLA-based steering profile name.

4. Click **OK**.

You are returned to the SLA-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed.

## Deleting SLA-Based Steering Profiles

You can delete the SLA-based steering profile if they are no longer needed. To delete one or more SLA-based steering profile:

**NOTE:** You cannot delete an SLA-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > SD-WAN > SLA Based Steering Profiles**.

The SLA-Based Steering Profiles page appears.

2. Select the SLA-based steering profiles that you want to delete and click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

3. Click **Yes**.

You are returned to the SLA-Based Steering Profiles page. The selected SLA-based steering profile is deleted and a confirmation message is displayed.

## RELATED DOCUMENTATION

---

[SLA Profiles and SD-WAN Policies Overview | 406](#)

---

[About the SLA-Based Steering Profiles Page | 420](#)

---

[Adding SLA-Based Steering Profiles | 424](#)

## About the Path-Based Steering Profiles Page

To access this page, select **Configuration > SD-WAN > Path-Based Steering Profiles** in the Customer Portal.

You can use the Path-Based Steering Profiles page to view information about path profiles for the tenant profile in which you are logged in.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View details of path-based steering profiles for the tenant.
- Add path-based steering profiles for the tenant. See [“Adding Path-Based Steering Profiles” on page 435](#).
- Edit or delete a path-based steering profile. See [“Editing and Deleting Path-Based Steering Profiles” on page 437](#).
- Show or hide columns that contain information about path-based steering profile. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for path-based steering profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

## Field Descriptions

[Table 151 on page 433](#) shows the descriptions of the fields on the Path-Based Steering Profiles page.

**Table 151: Fields on the Path-Based Steering Profiles Page**

Field	Description	Displayed on
Name	Name of the path-based-steering profile.	Path-Based Steering Profiles Page (Path Profiles List tab)  Detail for <i>Path-Profile-Name</i> pane
Traffic Type Profile	Indicates the traffic type profile associated with the path-based-steering profile. <ul style="list-style-type: none"> <li>• VOICE-VIDEO</li> <li>• HIGH_PRIORITY_VIDEO</li> <li>• HOSTED_AV</li> <li>• PREMIUM_INTERNET</li> <li>• INTERNET</li> </ul>	Path-Based Steering Profiles Page (Path Profiles List tab)  Detail for <i>Path-Profile-Name</i> pane
Path Preference	The preferred path for the SLA profile. The available options are: <ul style="list-style-type: none"> <li>• MPLS</li> <li>• Internet</li> </ul>	Path-Based Steering Profiles Page (Path Profiles List tab)  Detail for <i>Path-Profile-Name</i> pane
Created by	The name of the user who created the path profile.	Path-Based Steering Profiles Page (Path Profiles List tab)

Table 151: Fields on the Path-Based Steering Profiles Page (continued)

Field	Description	Displayed on
Priority	Priority of the path-based steering profile. A value zero (0) indicates lower priority and one (1) indicates highest priority.	Detail for <i>Path-Profile-Name</i> pane
Packet Loss	Target packet loss for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
RTT	Target round-trip time (RTT) for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
Jitter	Target jitter for the SLA profile.	Detail for <i>Path-Profile-Name</i> pane
SLA Probe Match	Indicates whether the profile requires the SLA probe to match all SLA criteria (All) or not (Any) .	Detail for <i>Path-Profile-Name</i> pane
Session-sampling %	Indicates the matching percentage of sessions for which you want to run the passive probes.	Detail for <i>Path-Profile-Name</i> pane
SLA Violation Counts	Indicates the number of SLA violations after which you want CSO to switch paths.	Detail for <i>Path-Profile-Name</i> pane
Sampling Period	The sampling period, in milliseconds, for which the path-based steering profile violations are counted.	Detail for <i>Path-Profile-Name</i> pane
Switch Cool-off Period	The waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links.	Detail for <i>Path-Profile-Name</i> pane
Path Failover Criteria	Indicates the path failover criteria for link switching. Path failover occurs when any (Any)of the path-based steering profile parameters is violated or when all (All) the path-based steering profile parameters are violated.	Detail for <i>Path-Profile-Name</i> pane
Maximum Upstream Rate	The maximum upstream rate (in Kbps) for all applications associated with the path-based steering profile.	Detail for <i>Path-Profile-Name</i> pane
Maximum Upstream Burst Size	The maximum upstream burst size (in bytes).	Detail for <i>Path-Profile-Name</i> pane



Table 151: Fields on the Path-Based Steering Profiles Page (*continued*)

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

## RELATED DOCUMENTATION

| [SLA Profiles and SD-WAN Policies Overview](#) | 406

## Adding Path-Based Steering Profiles

You can use the Add Path Profile page to add a new path-based steering profile, and specify the traffic type profile, path preference, and advanced configuration for the profile.

To add a path-based steering profile to the tenant:

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. Click the add (+) icon.

The Add Path Profile page appears.

3. Enter the path-based steering profile information according to the guidelines provided in [Table 152 on page 436](#).

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

4. Click **OK**.

You are returned to the Path-Based Steering Profiles page and a confirmation message indicating that the path-based steering profile was added is displayed. The page refreshes to display the path-based steering profile that you added.

**NOTE:** After you add a path-based steering profile, you must add an SD-WAN policy intent that references the path-based steering profile in order to enable site-to-site traffic.

**Table 152: Fields on the Add Path Profile page**

Field	Guidelines
Name	Enter a unique string that can contain alphanumeric characters and hyphens (-); the maximum length is 15 characters.
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the <b>Enabled</b> state.
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are MPLS, and Internet.
<i>Advanced Configuration</i>	
Maximum Upstream Rate	Enter the maximum upstream rate (in Kbps) for all applications associated with the SLA profile.  Range: 64 through 10,485,760 Kbps
Maximum Upstream Burst Size	Enter the maximum burst size (in bytes).  Range: 1 through 1,342,177,280 bytes
Maximum Downstream Rate	Enter the maximum downstream rate (in Kbps) for all applications associated with the SLA profile.  Range: 64 through 10,485,760 Kbps
Maximum Downstream Burst Size	Enter the maximum burst size (in bytes).  Range: 1 through 1,342,177,280 bytes

Table 152: Fields on the Add Path Profile page *(continued)*

Field	Guidelines
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 <b>High</b> . Other available values are <b>Medium High</b> , <b>Medium Low</b> , and <b>Low</b> .

RELATED DOCUMENTATION

<a href="#">SLA Profiles and SD-WAN Policies Overview   406</a>
<a href="#">About the Path-Based Steering Profiles Page   432</a>
<a href="#">Editing and Deleting Path-Based Steering Profiles   437</a>

## Editing and Deleting Path-Based Steering Profiles

IN THIS SECTION

- [Editing a Path-Based Steering Profile | 438](#)
- [Deleting a Path-Based Steering Profile | 439](#)

You can use the Path-Based Steering Profiles page to edit and delete path-based steering profiles.

## Editing a Path-Based Steering Profile

To edit a path-based steering profile:

**NOTE:** If you edit a path-based steering profile that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. On the Path Profiles tab, select the path-based steering profile that you want to edit.

3. Click the edit (pencil) icon.

The Edit Path Profile page appears displaying the same fields that are presented when you add a path-based steering profile. For more information, see [“Adding Path-Based Steering Profiles” on page 435](#).

4. Modify the fields as needed.

**NOTE:** You cannot edit the path profile name.

5. Click **OK**.

You are returned to the Path-Based Steering Profiles page. The modifications that you made are saved and a confirmation message is displayed..

## Deleting a Path-Based Steering Profile

You can delete path-based steering profiles if they are no longer needed. To delete one or more path-based steering profiles:

**NOTE:** You cannot delete a path-based steering profile if it is referenced by one or more SD-WAN policy intents.

1. Select **Configuration > SD-WAN > Path-Based Steering Profiles**.

The Path-Based Steering Profiles page appears.

2. On the Path Profiles List tab, select the path profiles that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Path-Based Steering Profiles page. The selected path-based steering profiles are deleted and a confirmation message is displayed.

### RELATED DOCUMENTATION

---

[SLA Profiles and SD-WAN Policies Overview | 406](#)

---

[About the Path-Based Steering Profiles Page | 432](#)

---

[Adding Path-Based Steering Profiles | 435](#)

## Breakout and Breakout Profiles Overview

### IN THIS SECTION

- [Breakout Profiles | 440](#)
- [SD-WAN Policy Intents for Breakout | 440](#)
- [Benefits of Breakout Profiles | 441](#)

Site-to-site traffic between spoke sites of a tenant is sent (on overlay tunnels) directly from one site to another depending on the tenant topology or through the hub or enterprise hub. However, for Internet-bound or Software as a Service (SaaS) traffic, you can break out the traffic in different ways:

- Local breakout—The traffic exits the VPN directly at the site and goes to the destination.
- Backhaul or central breakout—The traffic exits the VPN at the provider hub or at the enterprise hub (if a enterprise hub is associated with the spoke site) and then goes to the destination.
- Cloud breakout—The traffic is sent from the site to a designated cloud-based security platform instead of traffic being sent over an underlay.

**NOTE:** From CSO Release 4.1.0 onwards, Zscaler is the only cloud-based security platform supported.

In CSO Release 4.0, only local breakout and central breakout (backhaul) are supported and the breakout option is enabled only at the site level. However, from CSO Release 4.1.0 onward, breakout is supported at the site, department, and application (cacheable only) levels by using breakout profiles that are applied using SD-WAN policy intents. Non-cacheable applications follow the site-specific or department-specific behavior as configured in the SD-WAN policy intent.

**NOTE:** For sites added in CSO Release 4.1.0 onward, you cannot configure breakout *directly* at the site level and must use breakout profiles referenced in SD-WAN policy intents for this purpose.

## Breakout Profiles

The following three types of breakout profiles are supported in CSO:

- Local breakout (underlay)
- Backhaul (central breakout)
- Cloud breakout

After you add a breakout profile, you must create an SD-WAN policy intent specifying the source (site, site group, or department) and application and the applicable breakout profile.

## SD-WAN Policy Intents for Breakout

For SD-WAN policy intents configured at different source endpoints, the following is applicable:

- **Site**—A policy intent configured at the site level applies to all the departments within the site. In addition, by default, the site-level configuration is also applicable to all applications because the default configuration for applications is **Any**.
- **Department**—A policy intent configured at the department level (for tenants with network segmentation enabled) overrides the policy intent configured at the site level. Similar to the behavior for the site-level policy intent, by default, a department-level policy intent is also applicable to all applications because the default configuration for applications is **Any**.
- **Application (cacheable only)**—A policy intent (at the application level) where you specify one or more cacheable applications overrides the policy intent specified at either the department level or the site level *only* for the specified applications.

## Benefits of Breakout Profiles

- Breakout profiles used in intent-based Internet breakout policies (through SD-WAN policy intents) give users granular control over the Internet breakout behavior for specific applications.

## RELATED DOCUMENTATION

---

[Adding Breakout Profiles | 445](#)

---

[Adding Cloud Breakout Settings | 447](#)

---

[Creating SD-WAN Policy Intents | 412](#)

## About the Breakout Profiles Page

### IN THIS SECTION

- [Tasks You Can Perform | 442](#)
- [Breakout Profiles Field Descriptions | 443](#)
- [Cloud Breakout Settings Field Descriptions | 444](#)

To access this page, click **Configuration > SD-WAN > Breakout Profiles**.

You can use the Breakout Profiles page to view existing breakout profiles, add local, backhaul, and cloud breakout profiles, edit breakout profiles, and delete breakout profiles. You can also add settings for cloud breakout, edit cloud breakout settings, assign the settings to one or more sites, and delete the settings.

The breakout profiles are displayed on the Breakout Profiles tab and the cloud breakout settings are displayed on the Cloud Breakout Settings tab.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View existing breakout profiles—See [Table 153 on page 443](#) for a description of the fields.
- View the details of a breakout profile—On the Breakout Profiles tab, select a breakout profile and from the More menu, select **Detail View**. The Detail for *Breakout-Profile-Name* pane appears on the right-hand side of the page. See [Table 153 on page 443](#) for a description of the fields on this pane.
- View existing cloud breakout settings—See [Table 154 on page 444](#) for a description of the fields.
- View the details of cloud breakout settings—On the Cloud Breakout Settings tab, select a cloud breakout setting and from the More menu, select **Detail View**. The Detail for *Cloud-Breakout-Setting-Name* pane appears on the right-hand side of the page. See [Table 154 on page 444](#) for a description of the fields on this pane.
- Add a breakout profile—See [“Adding Breakout Profiles” on page 445](#).
- Edit a breakout profile—See [“Editing Breakout Profiles and Cloud Breakout Settings” on page 450](#).
- Delete a breakout profile—See [“Deleting Breakout Profiles and Cloud Breakout Settings” on page 452](#).
- Add cloud breakout settings—See [“Adding Cloud Breakout Settings” on page 447](#).
- Edit cloud breakout settings—See [“Editing Breakout Profiles and Cloud Breakout Settings” on page 450](#).
- Delete cloud breakout settings—See [“Deleting Breakout Profiles and Cloud Breakout Settings” on page 452](#).
- Assign cloud breakout settings to one or more sites—See [“Assigning Cloud Breakout Settings to Sites” on page 449](#).



## Breakout Profiles Field Descriptions

Table 153: Breakout Profiles Field Descriptions

Field	Description	Displayed On
Name	Name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)  Detail for <i>Breakout-Profile-Name</i> pane
Type	Indicates whether the breakout profile is for local breakout (underlay) or backhaul (central breakout) or cloud breakout.	Breakout Profiles page (Breakout Profiles tab)  Detail for <i>Breakout-Profile-Name</i> pane
Description	Description of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Path Preference	Indicates the preferred path to be used for breakout traffic: <ul style="list-style-type: none"> <li>• MPLS</li> <li>• Internet</li> <li>• Any, which indicates no preference.</li> </ul>	Breakout Profiles page (Breakout Profiles tab)
Added by	Username of the user who added the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
FqName	Internal name of the breakout profile.	Breakout Profiles page (Breakout Profiles tab)
Rate Limiting	Indicates whether rate limiting is enabled or disabled for the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Downstream Rate	Indicates the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Downstream Burst Size	Indicates the maximum downstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Upstream Rate	Indicates the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane

Table 153: Breakout Profiles Field Descriptions (*continued*)

Field	Description	Displayed On
Upstream Burst Size	Indicates the maximum upstream burst size (in bytes) for all cacheable applications associated with the breakout profile.	Detail for <i>Breakout-Profile-Name</i> pane
Loss Priority	Indicates the loss priority associated with the breakout profile. The loss priority determines which packets are dropped or retained when network congestion occurs.	Detail for <i>Breakout-Profile-Name</i> pane

## Cloud Breakout Settings Field Descriptions

Table 154: Cloud Breakout Settings Field Descriptions

Field	Description	Displayed On
Name or Profile-Name	Name of the cloud breakout setting.	Breakout Profiles page (Cloud Breakout Settings tab)  Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Primary Gateway IP	IPv4 address of the primary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab)  Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Primary Link Type	Preferred type of WAN link to be used for breaking out the traffic to the primary cloud breakout node.  If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.	Breakout Profiles page (Cloud Breakout Settings tab)  Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Secondary Gateway IP	IPv4 address of the secondary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab)  Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Secondary Type	Preferred type of WAN link to be used for breaking out the traffic to the secondary cloud breakout node.	Breakout Profiles page (Cloud Breakout Settings tab)  Detail for <i>Cloud-Breakout-Setting-Name</i> pane

Table 154: Cloud Breakout Settings Field Descriptions (*continued*)

Field	Description	Displayed On
Sites	If the cloud breakout settings are assigned to one or more sites, the names of the sites are displayed; if not, this field is blank.	Breakout Profiles page (Cloud Breakout Settings tab)
Added By	Username of the user who added the cloud breakout settings.	Breakout Profiles page (Cloud Breakout Settings tab)
Provider	Name of the cloud service provider.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane
Tunnel Type	Type of overlay tunnel.	Detail for <i>Cloud-Breakout-Setting-Name</i> pane

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview](#) | 439

## Adding Breakout Profiles

You use the Add Breakout Profile page to add a local breakout (underlay), backhaul, or a cloud breakout profile. A cloud breakout profile is added by Contrail Service Orchestration (CSO) by default.

To add a breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, click the add icon (+).

The Add Breakout Profile page appears.

3. Complete the configuration according to the guidelines provided in [Table 155 on page 446](#).

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

4. Click **OK**.

You are returned to the Breakout Profiles page (Breakout Profiles tab) and a confirmation message indicating that the breakout profile was added is displayed. The page refreshes to display the breakout profile that you added.

**NOTE:** After you add a breakout profile, you must add an SD-WAN policy intent that references the breakout profile in order to enable breakout traffic.

**Table 155: Fields on the Add Breakout Profile Page**

Field	Description
<b>Type</b>	<p>Select the type of breakout profile that you want to add:</p> <ul style="list-style-type: none"> <li>• <b>Local Breakout (Underlay)</b>—Select this option if you want traffic to break out locally (on the underlay) from the site.</li> <li>• <b>Backhaul</b>—Select this option if you want traffic to break out through a hub or a enterprise hub (if configured).</li> <li>• <b>Local Breakout (Cloud)</b>—Select to break out traffic through a cloud-based security platform. Currently, Zscaler is the only cloud-based security platform supported.</li> </ul>
<b>Name</b>	Enter a unique name for the breakout profile. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.
<b>Description</b>	Enter a description for the breakout profile.
<b>Traffic Type Profile</b>	Select a traffic type profile to apply class of service parameters to the breakout traffic. You can select only a traffic type profile that is enabled.
<b>Preferred Path</b>	<p>Select the preferred path (MPLS, Internet, or Any) to be used for breaking out the traffic.</p> <p>If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.</p> <p>If you specify that any path can be used, then there is no preference and all breakout-enabled links are used in a load-balancing mode.</p>
<b>Advanced Configuration</b>	
<b>Rate Limiting</b>	<p>Click the toggle button to enable rate limiting of breakout traffic for cacheable applications. By default, rate limiting is disabled.</p> <p>If you enable rate limiting, you must specify the upstream and downstream parameters, and the loss priority.</p>

Table 155: Fields on the Add Breakout Profile Page (*continued*)

Field	Description
<b>Upstream Rate</b>	Specify the maximum upstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
<b>Upstream Burst Size</b>	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the upstream rate limit for short periods.
<b>Downstream Rate</b>	Specify the maximum downstream rate (in Kbps) for all cacheable applications associated with the breakout profile.
<b>Downstream Burst Size</b>	Specify the maximum size (in bytes) of a steady stream of traffic sent at average rates that exceed the downstream rate limit for short periods.
<b>Loss Priority</b>	Select a loss priority based on which packets are dropped or retained when network congestion occurs. Packet drops are most likely when the loss priority is High and least likely when the loss priority is Low.

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview](#) | 439

[Creating SD-WAN Policy Intents](#) | 412

## Adding Cloud Breakout Settings

You use the Add Cloud Breakout Settings page to add cloud breakout settings that you can then apply to sites.

To add cloud breakout settings:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, click the add icon (+).

The Add Cloud Breakout Settings page appears.

3. Complete the configuration according to the guidelines provided in [Table 156 on page 448](#).

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

4. Click **OK**.

You are returned to the Breakout Profiles page (Cloud Breakout Settings tab) and a confirmation message indicating that the breakout settings are added is displayed.

After you add cloud breakout settings, you can assign the settings to one or more sites. Assigning cloud breakout settings to sites provisions the cloud breakout node (Zscaler) overlay. For traffic to flow, you must reference the cloud breakout profile in an SD-WAN policy intent.

**Table 156: Fields on the Add Cloud Breakout Settings Page**

Field	Description
<b>Name</b>	Enter a unique name for the cloud breakout settings. You can use alphanumeric characters and hyphens (-); the maximum length is 15 characters.
<b>Primary Gateway IP Address</b>	Enter the IPv4 address of the primary cloud breakout node. Currently, Zscaler is the only cloud-based security platform supported.
<b>Primary Preferred Link Type</b>	Select the preferred type of WAN link (MPLS or Internet) to be used for breaking out the traffic to the primary cloud breakout node.  If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.
<b>Primary Preshared Key</b>	Enter the preshared key used for IKE authentication with the primary cloud breakout node.  The key that you enter is masked.
<b>Secondary Gateway IP Address</b>	Enter the IPv4 address of the secondary cloud breakout node. Currently, Zscaler is the only cloud-based security platform supported.
<b>Secondary Preferred Link Type</b>	Select the preferred type of WAN link (MPLS or Internet) to be used for breaking out the traffic to the secondary cloud breakout node.  If a WAN link type that matches the preferred path is enabled for breakout, then that WAN link type is used for breakout traffic.
<b>Secondary Preshared Key</b>	Enter the preshared key used for IKE authentication with the secondary cloud breakout node.  The key that you enter is masked.

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 439](#)[Creating SD-WAN Policy Intents | 412](#)

## Assigning Cloud Breakout Settings to Sites

You use the Assign Cloud Breakout Settings to Sites page to assign cloud breakout settings to one or more sites. You assign cloud breakout settings to one or more sites to provision tunnels from the sites to the cloud breakout node. For breakout traffic from the site, the cloud breakout profile must be referenced in an SD-WAN policy intent.

**NOTE:**

- If you want a site to have cloud breakout enabled, you must assign cloud breakout settings for that site.
- A site can have only one cloud breakout setting associated with it at any given time.

To assign one or more sites to a cloud breakout profile:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select a cloud breakout profile and click **Assign Sites**.

The Assign Cloud Breakout Settings to Sites page appears displaying the name of the cloud breakout setting and the existing sites to which you can assign to the setting.

3. In the Sites field, select one or more sites in the Available column and click the right arrow icon to move the selected sites to the Selected column. You can also use the search icon on the top right of each column to search for sites names.

Alternatively, if you want to remove sites that you previously selected for assignment, select one or more sites in the Selected column and click the left arrow icon to move the selected sites back to the Available column.

**NOTE:** You must select at least one site before proceeding.

4. Click **Save**.

A Job is created and you are returned to the Breakout Profiles page (Cloud Breakout Settings tab). After successful completion of the job, the names of the sites to which the settings are assigned are displayed in the Sites column.

#### RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 439](#)

## Editing Breakout Profiles and Cloud Breakout Settings

### IN THIS SECTION

- [Editing Breakout Profiles | 451](#)
- [Editing Cloud Breakout Settings | 451](#)

On the Breakout Profiles page, you can edit breakout profiles and cloud breakout settings that are not assigned to sites.

**NOTE:** You cannot edit the cloud breakout profile that is automatically created by Contrail Service Orchestration (CSO).



## Editing Breakout Profiles

To edit a breakout profile:

**NOTE:** If you edit a breakout policy that is used in an SD-WAN policy intent, then that SD-WAN policy is marked for redeployment.

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to edit.

3. Click the edit (pencil) icon.

The Edit Breakout Profile page appears displaying the same fields that are presented when you add a breakout profile. For more information, see [“Adding Breakout Profiles” on page 445](#).

4. Modify the fields as needed.

**NOTE:** You can modify only some fields when you are editing a breakout profile

5. Click **OK**.

You are returned to the Breakout Profiles page. The modifications that you made are saved and a confirmation message is displayed.

## Editing Cloud Breakout Settings

To edit cloud breakout settings that are not assigned to sites:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select the cloud breakout setting that you want to edit.

3. Click the edit (pencil) icon.

The Edit Cloud Breakout page appears displaying the same fields that are presented when you add cloud breakout settings. For more information, see [“Adding Cloud Breakout Settings” on page 447](#).

4. Modify the fields as needed.

**NOTE:** You can modify only some fields when you are editing a breakout profile

5. Click **OK**.

You are returned to the Breakout Profiles page. The modifications that you made are saved and a confirmation message is displayed.

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 439](#)

[About the Breakout Profiles Page | 441](#)

## Deleting Breakout Profiles and Cloud Breakout Settings

### IN THIS SECTION

- [Deleting Breakout Profiles | 452](#)
- [Deleting Cloud Breakout Settings | 453](#)

On the Breakout Profiles page, you can delete breakout profiles that are not used in SD-WAN policy intents and cloud breakout settings that are not assigned to sites.

### Deleting Breakout Profiles

To delete a breakout profile that is not used in an SD-WAN policy intent:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Breakout Profiles** tab, select the breakout profile that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Breakout Profiles page. The selected breakout profile is deleted and a confirmation message is displayed.

## Deleting Cloud Breakout Settings

To delete cloud breakout settings that are not assigned to sites:

1. Select **Configuration > SD-WAN > Breakout Profiles**.

The Breakout Profiles page appears.

2. On the **Cloud Breakout Settings** tab, select the cloud breakout setting that you want to delete.

3. Click the delete (trash can) icon.

A popup dialog appears asking you to confirm the deletion.

4. Click **Yes**.

You are returned to the Breakout Profiles page. The selected cloud breakout setting is deleted and a confirmation message is displayed.

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview | 439](#)

[About the Breakout Profiles Page | 441](#)

## Configuring Breakout on SD-WAN Sites

The following is the workflow for configuring breakout (local breakout [underlay], backhaul [central breakout], or cloud breakout):

1. *Before* configuring breakout, ensure that you complete the following tasks:
  - a. If you are using enterprise hub sites, add, configure, and activate one or more enterprise hub sites. See [“Adding Enterprise Hubs with SD-WAN Capability or SD-WAN and LAN Capabilities”](#) on page 48.

- b. Add, configure, and activate one or more on-premise spoke sites with SD-WAN capability. See [“Adding an On-Premise Spoke Site with SD-WAN Capability” on page 81.](#)

**NOTE:** You must attach an on-premise spoke site with SDWAN capability to a provider hub site or an enterprise hub site, or to both hub sites.

- c. (Optional) If you are using application-based breakout, ensure that you install the application ID license (if it is required for the device) and signatures on the devices (associated with the sites).
2. Depending on the type of breakout you are configuring, add one or more breakout profiles for the following types of breakout:
    - Local breakout (underlay)
    - Backhaul (central breakout)
    - Cloud breakout

See [“Adding Breakout Profiles” on page 445.](#)
  3. For cloud breakout, add cloud breakout settings and then assign the cloud breakout settings to one or more on-premise spoke or enterprise hub sites. See [“Adding Cloud Breakout Settings” on page 447](#) and [“Assigning Cloud Breakout Settings to Sites” on page 449.](#)
  4. Add one or more SD-WAN policy intents in which you reference the previously-added breakout profiles. See [“Creating SD-WAN Policy Intents” on page 412.](#)
  5. Deploy the SD-WAN policy. See [“Deploying Policies” on page 548.](#)
  6. Configure firewall policy intents to allow Internet-bound traffic from the sites or departments for which you configured breakout (through the SD-WAN policy intent). See [“Adding Firewall Policy Intents” on page 291.](#)
  7. Deploy the firewall policy. See [“Deploying Policies” on page 548.](#)
  8. For cloud breakout using Zscaler, ensure that the user IDs in the Zscaler account are configured as follows:
    - *Site-Name.primary.1@Tenant-Name.com* for the primary tunnel
    - *Site-Name.backup.1@Tenant-Name.com* for the secondary tunnel

Where *Site-Name* is the name of the site (in CSO) for which the breakout is configured and *Tenant-Name* is the name of the tenant (in CSO) to which the site belongs.

## RELATED DOCUMENTATION

[Breakout and Breakout Profiles Overview](#) | 439

# Managing NAT Policies

## IN THIS CHAPTER

- [NAT Policies Overview | 457](#)
- [About the NAT Policies Page | 460](#)
- [Creating NAT Policies | 461](#)
- [Editing and Deleting NAT Policies | 463](#)
- [About the Single NAT Policy Page | 464](#)
- [Creating NAT Policy Rules | 466](#)
- [Editing, Cloning, and Deleting NAT Policy Rules | 473](#)
- [Deploying NAT Policy Rules | 475](#)
- [Selecting NAT Source | 476](#)
- [Selecting NAT Destination | 480](#)
- [NAT Pools Overview | 484](#)
- [About the NAT Pools Page | 484](#)
- [Creating NAT Pools | 486](#)
- [Editing, Cloning, and Deleting NAT Pools | 488](#)

## NAT Policies Overview

Network Address Translation (NAT) is a form of network masquerading where you can hide devices or sites between zones or interfaces. A trusted zone is a segment of a network on which security measures are applied. It is usually assigned to the internal LAN. An example of an untrusted zone is the internet. NAT modifies the IP addresses of the packets moving between the trusted and untrusted zones.

Whenever a packet exits a NAT device (when traversing from the internal LAN to the external WAN), the device performs a translation on the packet's IP address by rewriting it with an IP address that was specified for external use. After translation, the packet appears to have originated from the gateway rather than from the original device within the network. This process hides your internal IP addresses from the other networks and keeps your network secure.

Using NAT also enables you to use more internal IP addresses. As these IP addresses are hidden, there is no risk of conflict with an IP address from a different network. This helps you conserve IP addresses.

CSO supports three types of NAT:

- **Source NAT**— Translates the source IP address of a packet leaving a trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. The source IP address of the traffic (which is a private IP address), is translated to a public IP address that can be accessed by the destination device specified in the NAT rule. The destination IP address is not translated.

The following uses cases show the support for source NAT translation between IPv6 and IPv4 address domains:

- Translation from one IPv6 subnet to another IPv6 subnet without Network Address Port Translation (NAPT), also known as Port Address Translation (PAT).
- Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation.
- Translation from IPv6 hosts to IPv6 hosts with or without NAPT.
- Translation from IPv6 hosts to IPv4 hosts with or without NAPT.
- Translation from IPv4 hosts to IPv6 hosts with or without NAPT.
- **Destination NAT**—Translates the destination IP address of a packet. Using destination NAT, an external device can send packets to a hidden internal device. As an example, consider the case of a webserver behind a NAT device. Traffic to the WAN-facing public IP address (the destination IP address) is translated to the internal webserver private IP address.

The following uses cases show the support for destination NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet
- Mapping between one IPv6 host and another IPv6 host

- Mapping of one IPv6 host (and optional port number) to another special IPv6 host (and optional port number)
- Mapping of one IPv6 host (and optional port number) to another special IPv4 host (and optional port number)
- Mapping of one IPv4 host (and optional port number) to another special IPv6 host (and optional port number)
- Static NAT— Always translates a private IP address to the same public IP address. It translates traffic from both sides of the network (both source and destination). For example, a web-server with a private IP address can access the Internet using a static, one-to-one address translation. In this case, outgoing traffic from the web-server undergoes source NAT translation, and incoming traffic to the web-server undergoes destination NAT translation.

The following uses cases show the support for static NAT translation between IPv6 and IPv4 address domains:

- Mapping of one IPv6 subnet to another IPv6 subnet.
- Mapping between one IPv6 host and another IPv6 host.
- Mapping between IPv4 address *a.b.c.d* and IPv6 address *Prefix::a.b.c.d*.
- Mapping between IPv4 hosts and IPv6 hosts.
- Mapping between IPv6 hosts and IPv4 hosts.

CSO also supports persistent NAT where address translations are maintained in the database for a configurable amount of time after a session ends.

[Table 157 on page 458](#) shows the persistent NAT support for different source NAT and destination NAT addresses.

**Table 157: Persistent NAT Support**

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

[Table 158 on page 459](#) and [Table 159 on page 459](#) show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.



Table 158: Translated Address Pool Selection for Source NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4
IPv4	IPv6 - Subnet must be greater than 96	IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv6

Table 159: Translated Address Pool Selection for Destination NAT And Static NAT

Source NAT Address	Destination Address	Pool Address
IPv4	IPv4	IPv4 or IPv6
IPv4	IPv6 - Subnet must be greater than 96	IPv4 or IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv4 or IPv6

**NOTE:**

- For source NAT, the proxy Neighbor Discovery Protocol (NDP) is available for NAT pool addresses. For destination NAT and static NAT, the proxy NDP is available for destination NAT addresses.
- A NAT pool can have a single IPv6 subnet or multiple IPv6 hosts.
- You cannot configure the overflow pool if the address type is IPv6.
- NAT pools permit address entries of only one version type: IPv4 or IPv6.

**RELATED DOCUMENTATION**
[About the NAT Policies Page | 460](#)
[Creating NAT Policies | 461](#)
[Editing and Deleting NAT Policies | 463](#)
[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

## About the NAT Policies Page

To access this page, select **Configuration > NAT > NAT Policies**.

Use the **NAT Policies** page to create, modify, clone, and delete NAT policies and policy rules. You can filter and sort this information to get a better understanding of what you want to configure.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT policy. See [“Creating NAT Policies” on page 461](#).
- Modify or delete a NAT policy. See [“Editing and Deleting NAT Policies” on page 463](#).
- Create, modify, clone, and delete NAT policy rules. See [“About the Single NAT Policy Page” on page 464](#).
- Search for a specific NAT policy. Click the Search icon in the top right corner of the page to search for a NAT policy.

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

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

### Field Descriptions

[Table 160 on page 460](#) provides guidelines on using the fields on the **NAT Policies** page.

**Table 160: Fields on the NAT Policies Page**

Field	Description
Name	Displays the name of the NAT policy.
Installed On	Displays the sites on which the NAT policy is assigned.
Rules	Number of rules assigned to the NAT policy.
Undeployed	Number of undeployed rules associated with the NAT policy.

### RELATED DOCUMENTATION

[NAT Policies Overview | 457](#)

## Creating NAT Policies

Use the **Create NAT Policy** page to create NAT policies.

To create a NAT policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Click the add icon (+).

The **Create NAT Policy** page displays fields required for creating and configuring a NAT policy.

3. Complete the configuration according to the guidelines provided in [Table 161 on page 461](#).

**NOTE:** You can associate only a single device or a device cluster with a site.

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

A NAT policy with the configuration you provided is created.

**Table 161: Fields on the Create NAT Policy Page**

Field	Description
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the policy; the maximum length is 1024 characters.

Table 161: Fields on the Create NAT Policy Page (*continued*)

Field	Description
Manage Auto-Proxy ARP	<p>The Address Resolution Protocol (ARP) protocol translates IPv4 addresses to MAC addresses. Typically, an interface responds with its MAC address only when an ARP request for its IP address is received.</p> <p>A proxy ARP implies that the same interface will proxy for other IP addresses (that is, respond to ARP requests for other IP addresses).</p> <p>Managing a proxy ARP automatically enables the selection of an appropriate interface for any address (as part of a NAT rule) that is not an actual interface address. Proxy ARP management applies to translated addresses in a source NAT rule or to a destination address in a destination NAT rule.</p> <p><b>NOTE:</b> When creating a source NAT rule with pool translation, the address pool assigned must be in the same subnet as the outgoing interface selected.</p> <p><b>NOTE:</b> When creating a destination NAT rule, the external WAN interface can be a proxy for another IP address in the same subnet as the original IP address of the interface.</p>
Sites Applied On	<p>Select the sites on which you want to apply the policy in the <b>Available</b> column and move them to the <b>Selected</b> column by clicking the greater-than icon (&gt;).</p> <p><b>NOTE:</b> The <b>Available</b> column lists only those sites that do not have a NAT policy associated with them.</p>
Sequence No.	<p>Click <b>Select Policy Sequence</b>. The <b>Select Policy Sequence</b> page appears, displaying all NAT policies. Select the policy you want to reorder and select <b>Move Policy Up</b> or <b>Move Policy Down</b> to reorder your NAT policy among the existing policies.</p>

## RELATED DOCUMENTATION

[NAT Policies Overview | 457](#)
[About the NAT Policies Page | 460](#)
[Editing and Deleting NAT Policies | 463](#)
[About the Single NAT Policy Page | 464](#)
[Creating NAT Policy Rules | 466](#)
[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

## Editing and Deleting NAT Policies

### IN THIS SECTION

- [Editing NAT Policies | 463](#)
- [Deleting NAT Policies | 463](#)

You can edit or delete a NAT policy from the **NAT Policies** page.

### Editing NAT Policies

To modify the parameters configured for a NAT Policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Hover over the NAT policy you want to edit, and then click on the edit icon (pencil symbol) on the right side of the table.

The **Edit NAT Policy** page appears, showing the same fields as those seen when you create a new NAT policy.

3. Modify the parameters according to the guidelines provided in [“Creating NAT Policies” on page 461](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, you will see the modified NAT policy in the **NAT Policies** page.

### Deleting NAT Policies

To delete a NAT policy:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears.

2. Hover over the NAT policy you want to delete and then click the delete icon (X).

An alert message appears, verifying that you want to delete your selection.

3. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the NAT policy is deleted.

**NOTE:** When the NAT policy is deleted, the NAT rules associated with the policy are deleted from device.

## RELATED DOCUMENTATION

[NAT Policies Overview | 457](#)

[About the NAT Policies Page | 460](#)

[Creating NAT Policies | 461](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

## About the Single NAT Policy Page

To access this page, select **Configuration > NAT > NAT Policies**. The **NAT Policies** page appears displaying all existing NAT policies. Click on a NAT policy to view the rules associated with it.

The *Single NAT Policy* page displays the NAT rules associated with the NAT policy, and keep track of the number and order of rules for each policy. You can also create a new NAT rule, modify the configured parameters of existing NAT rules, clone, and delete NAT rules, using this page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT rule. See [“Creating NAT Policy Rules” on page 466](#).
- Update the sequence of the NAT rules using the up and down arrows that appear when you hover over the NAT rule.
- Modify, clone, and delete NAT rules. See [“Editing, Cloning, and Deleting NAT Policy Rules” on page 473](#).
- Deploy a NAT rule. See [“Deploying NAT Policy Rules” on page 475](#).
- Search for a specific NAT rule. Click the Search icon in the top right corner of the page to search for a NAT rule.
- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

Table 162 on page 465 provides information on the fields in the NAT rules contained within this NAT policy.

Table 162: Fields on the Single NAT Policy Page

Field	Description
Source	Displays the source endpoint on which the NAT policy applies. A source endpoint can be an address, protocol, interface, routing instance, zone, or port.
Destination	Displays the destination endpoint on which the NAT policy applies. A destination endpoint can be an address, interface, service, routing instance, zone, or port.
Translation	Displays the translation type applied on the incoming or outgoing traffic.
Details	Displays the type of NAT rule. A NAT rule can be of type source, static, or destination.

The **Total Rules** field on the top right corner of the page displays the total number of rules associated with the NAT policy. The **Undeployed** field displays the number of undeployed rules associated with the NAT policy. To deploy undeployed rules, click **Deploy**. See “[Deploying NAT Policy Rules](#)” on page 475.

RELATED DOCUMENTATION

<a href="#">NAT Policies Overview</a>	<a href="#">  457</a>
<a href="#">About the NAT Policies Page</a>	<a href="#">  460</a>
<a href="#">Creating NAT Policies</a>	<a href="#">  461</a>
<a href="#">Editing and Deleting NAT Policies</a>	<a href="#">  463</a>
<a href="#">Creating NAT Policy Rules</a>	<a href="#">  466</a>
<a href="#">Editing, Cloning, and Deleting NAT Policy Rules</a>	<a href="#">  473</a>
<a href="#">Deploying NAT Policy Rules</a>	<a href="#">  475</a>

## Creating NAT Policy Rules

NAT processing centers on the evaluation of NAT rule sets and rules. A rule set determines the overall direction of the traffic to be processed. After a rule set that matches the traffic is found, each rule in the rule set is evaluated for a match. NAT rules can match on the following packet information:

- Source and destination address
- Source port (for source and static NAT only)
- Destination port

The first rule in the rule set that matches the traffic is used. If a packet matches a rule in a rule set during session establishment, traffic is processed according to the action specified by that rule.

To create a new NAT rule, click the NAT policy name. The *Single NAT Policy* page appears, providing you with options to configure NAT rules. Alternately, you can click on the rule number listed under **Rules** against the policy, to create a new rule. You can configure the following types of NAT rules:

- **Static**—To add a static NAT rule, click **Add Static NAT Rule** or click **Create** on the top right corner and select **Static**.
- **Source**—To add a source NAT rule, click **Add Source NAT Rule** or click **Create** on the top right corner and select **Source**.
- **Destination**—To add a destination NAT rule, click **Add Destination NAT Rule** or click **Create** on the top right corner and select **Destination**.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. In addition to defining rules between zones and interfaces, you can define NAT rules with virtual routers defined on the device. These rules can be successfully published and updated on the device.

To create a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the existing NAT policies.

2. Click the name of the NAT policy for which you want to create rules. Alternately, you can click on the number listed under **Rules** against a NAT policy.

The *Single NAT Policy* page appears.

3. Click **Create** and select either **Source**, **Static**, or **Destination**. The page displays fields for creating a NAT rule.



4. Complete the configuration according to the guidelines provided in [Table 163 on page 467](#).
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A NAT rule with the configuration you provided is created.

[Table 163 on page 467](#) provides guidelines on using the fields on the **Single NAT Policy** page.

**Table 163: Fields on the Single NAT Policy Page for Creating NAT Rules**

Field	Description
Source	<p>Click the add icon (+) to select the source endpoints on which the NAT policy rule applies, from the displayed list of addresses, protocols, interfaces, routing instances, zones, or ports.</p> <p>The possible endpoints for source differ based on whether the NAT rule is a source, destination, or static NAT rule.</p> <ul style="list-style-type: none"> <li>• The possible endpoints for source for a source NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Routing instances, interfaces, or zones</li> <li>• Protocols</li> <li>• Ports</li> </ul> </li> <li>• The possible endpoints for source for a destination NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Routing instances, interfaces, or zones</li> <li>• Protocols</li> </ul> </li> <li>• The possible endpoints for source for a static NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Routing instances, interfaces, or zones</li> <li>• Ports</li> </ul> </li> </ul> <p>You can also select a source endpoint by using the methods described in <a href="#">"Selecting NAT Source" on page 476</a>.</p>

Table 163: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Destination	<p>Click the add icon (+) to select the destination endpoints on which the NAT policy rule applies, from the displayed list of addresses, interfaces, services, routing instances, zones, or ports.</p> <p>The possible endpoints for destination differ based on whether the NAT rule is a source, destination, or static NAT rule.</p> <ul style="list-style-type: none"> <li>• The possible endpoints for destination for a source NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Routing instances, interfaces, or zones</li> <li>• Services</li> <li>• Ports</li> </ul> </li> <li>• The possible endpoints for destination for a destination NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Services</li> <li>• Ports</li> </ul> </li> <li>• The possible endpoints for destination for a static NAT rule are: <ul style="list-style-type: none"> <li>• Addresses</li> <li>• Ports</li> </ul> </li> </ul> <p>You can select a destination endpoint by using the methods described in <a href="#">“Selecting NAT Destination” on page 480</a>.</p> <p><b>NOTE:</b> When you create a destination NAT rule for traffic arriving on an interface that terminates a VPN link, the translation process may break the VPN link. This will happen if the destination address in a destination NAT rule is specified only as the WAN-facing IP address of that interface. For example, in the following NAT rule, any traffic destined to Wan.IP will get translated to the destination pool and will break functionality of the VPN link packets terminating on this interface.</p> <p><b>[Any.Address] --&gt; [Wan.IP] :: [Dest-Pool-1]</b></p> <p>Therefore, the recommendation in such cases is to use a destination NAT rule with destination field as <b>[Address + Port]</b>. For example:</p> <p><b>[Any.Address] --&gt; [Wan.IP + Port] :: [Dest-Pool-1]</b></p>
Translation	

Table 163: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Translation Type	<p>Specify the translation type for the incoming traffic. The translation options vary based on whether you are creating a source, static, or destination NAT rule.</p> <p>Chose one among the following translation types for a source NAT rule:</p> <ul style="list-style-type: none"> <li>• None—No translation is required for the incoming traffic.</li> <li>• Interface—Performs interface-based translations on the source or destination packet.</li> <li>• Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the <b>Select Pool</b> field to choose the translation pool.</li> </ul> <p>You can also create a new pool by clicking <b>Add new pool</b>. See <a href="#">“Creating NAT Pools” on page 486</a>.</p> <p>Chose one among the following translation types for a static NAT rule:</p> <ul style="list-style-type: none"> <li>• Address—Performs address-based translations on the source or destination packet. Click on the add icon (+) in the <b>Select Address</b> field to choose the translation address.</li> </ul> <p>You can also create a new address by clicking <b>Add new address</b>. See <a href="#">“Creating Addresses or Address Groups” on page 573</a>.</p> <p><b>NOTE:</b> In an SD-WAN environment, it is mandatory that you select the routing instance corresponding to the translation address. You can select the routing instance for a translation address using the <b>Advanced Settings</b> page. For more information on <b>Advanced Settings</b>, see <a href="#">Table 165 on page 472</a>.</p> <ul style="list-style-type: none"> <li>• Corresponding IPv4—Uses the corresponding IPv4 address to perform translations on the source or destination packet.</li> </ul> <p>Chose one among the following translation types for a destination NAT rule:</p> <ul style="list-style-type: none"> <li>• None—No translation is required for the incoming traffic.</li> <li>• Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the <b>Select Pool</b> field to choose the translation pool.</li> </ul> <p>You can also create a new pool by clicking <b>Add new pool</b>. See <a href="#">“Creating NAT Pools” on page 486</a>.</p> <p><b>NOTE:</b> In an SD-WAN environment, the destination NAT pool selected should be configured with a site and a routing instance corresponding to the pool address. For example, a webserver with IP address (IP1) is running in the HR department. To create a destination NAT pool corresponding to this webserver IP address, you must specify the following mandatory fields while creating the NAT pool:</p> <p><b>Address - IP1</b></p> <p><b>Site - the site hosting the webserver</b></p> <p><b>Routing instance - natVR_HR</b></p>

Table 163: Fields on the Single NAT Policy Page for Creating NAT Rules (*continued*)

Field	Description
Advanced Settings (Optional)	Click <b>Configure</b> to configure advance settings for a source or static NAT rule. For more information about advanced settings for the translation types <b>Interface</b> and <b>Pool</b> for a source NAT rule, see <a href="#">Table 164 on page 470</a> . For more information about advanced settings for the translation types <b>Interface</b> and <b>Pool</b> for a static NAT rule, see <a href="#">Table 165 on page 472</a>
<b>Details</b>	
Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.
Description	Enter a description for the policy intent; maximum length is 1024 characters.
End Points	<p>Create source and destination endpoints such as addresses and services.</p> <ul style="list-style-type: none"> <li>• To create an address, click the add icon (+) and select <b>Address</b>. See <a href="#">“Creating Addresses or Address Groups” on page 573</a> to configure the parameters of the address.</li> <li>• To create a service, click the add icon (+) and select <b>Service</b>. See <a href="#">“Creating Services and Service Groups” on page 579</a> to configure the parameters of the service.</li> </ul> <p>To edit the configured parameters of an address or service, hover over it and click on the edit icon (pencil symbol).</p>

[Table 164 on page 470](#) provides guidelines on using the fields on the **Advanced Settings** page for a source NAT rule.

Table 164: Fields on the Advanced Settings Page for Source NAT Rule

Field	Description
Persistent	<p>Enable the check box to ensure that all requests from the same internal transport address are mapped to the same reflexive transport address.</p> <p><b>NOTE:</b> For persistence to be applicable for the NAT policy, ensure that port overloading is turned off for the device to which the NAT policy is applicable. Use the following command to turn off port overloading for a device:</p> <pre>[Edit mode] set security nat source interface port-overloading off</pre>

Table 164: Fields on the Advanced Settings Page for Source NAT Rule (*continued*)

Field	Description
Persistent NAT Type	<p>Configure persistent NAT mappings.</p> <ul style="list-style-type: none"> <li>• Permit any remote host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. (The reflexive transport address is the public IP address and port created by the NAT device closest to the STUN server.) Any external host can send a packet to the internal host by sending the packet to the reflexive transport address.</li> <li>• Permit target host—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address.</li> <li>• Permit target host port—All requests from a specific internal IP address and port are mapped to the same reflexive transport address. An external host can send a packet to an internal host by sending the packet to the reflexive transport address. The internal host must have previously sent a packet to the external host's IP address and port.</li> </ul>
Inactivity Timeout	<p>The amount of time, in seconds, that the persistent NAT binding remains in the site's memory when all the sessions of the binding entry have ended. When the configured timeout is reached, the binding is removed from memory. The value of the inactivity timeout can range from 60 through 7200 seconds. The default value of the inactivity timeout is 60 seconds.</p>
Maximum Session Number	<p>Maximum session number—The maximum number of sessions with which a persistent NAT binding can be associated. For example, if the maximum session number of the persistent NAT rule is 65,536, then a 65,537th session cannot be established if that session uses the persistent NAT binding created from the persistent NAT rule.</p> <p>The range is 8 through 65,536. The default is 30 sessions.</p>
Address Mapping	<p>Select an address from the available list.</p>
Pool Address	<p>Displays the NAT pool address.</p>
Host Address Base	<p>Displays the base address of the original source IP address range. The host address base is used for IP address shifting.</p>
Port Translation	<p>Displays whether port translation is enabled or disabled for this NAT rule.</p>
Overflow Pool Type	<p>Displays the source pool to be used when the current address pool is exhausted.</p>
Overflow Pool Name	<p>Displays the name of the overflow pool.</p>

Table 164: Fields on the Advanced Settings Page for Source NAT Rule (*continued*)

Field	Description
Mapped Port Type	<p>Specify the type of port mapping:</p> <ul style="list-style-type: none"> <li>• Port—Enter a value for <b>Port</b>, ranging from 0 through 65,535.</li> <li>• Range—Enter the port range values in the <b>Start</b> and <b>End</b> fields, ranging from 0 through 65,535.</li> </ul>

[Table 165 on page 472](#) provides guidelines on using the fields on the **Advanced Settings** page for a static NAT rule.

Table 165: Fields on the Advanced Settings Page for Static NAT Rule

Field	Description
Mapped Port Type	<p>Specify the type of port mapping:</p> <ul style="list-style-type: none"> <li>• Port—Enter a value for <b>Port</b>, ranging from 0 through 65,535.</li> <li>• Range—Enter the port range values in the <b>Start</b> and <b>End</b> fields, ranging from 0 through 65,535.</li> </ul>
Routing Instance	Select the routing instance for the static NAT rule.

## RELATED DOCUMENTATION

[About the Single NAT Policy Page | 464](#)

[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

[Deploying NAT Policy Rules | 475](#)

[NAT Policies Overview | 457](#)

[About the NAT Policies Page | 460](#)

[Creating NAT Policies | 461](#)

[Editing and Deleting NAT Policies | 463](#)

## Editing, Cloning, and Deleting NAT Policy Rules

### IN THIS SECTION

- [Editing NAT Policy Rules | 473](#)
- [Cloning NAT Policy Rules | 473](#)
- [Deleting NAT Policy Rules | 474](#)

You can edit, clone, or delete a NAT policy rule from the **NAT Policy** page.

### Editing NAT Policy Rules

To modify the parameters configured for an NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rules you want to edit.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule that you want to modify and click on the edit icon (pencil symbol) that appears on the right side of the NAT policy rule. The page changes to display the same fields that you use to create a NAT policy rule.

4. Complete the configuration according to the guidelines provided in [“Creating NAT Policy Rules” on page 466](#).

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

The modified NAT policy rule appears on the **NAT Policy** page.

### Cloning NAT Policy Rules

To clone a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rule you want to clone.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule that you want to clone and click on the clone icon that appears on the right side of the NAT policy rule.

The cloned NAT policy rule appears below the current rule.

You can modify the parameters configured for the cloned NAT policy rule or rename it as required.

## Deleting NAT Policy Rules

To delete a NAT policy rule:

1. Select **Configuration > NAT > NAT Policies**.

The **NAT Policies** page appears, displaying the NAT policies.

2. Select the NAT policy whose rule you want to delete.

The selected **NAT Policy** appears, displaying the rules associated with the NAT policy.

3. Hover over the NAT policy rule you want to delete and then click the delete icon **(X)**.

An alert message appears, verifying that you want to delete your selection.

4. Click **Yes** to delete the selection. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected NAT policy rule is deleted.

## RELATED DOCUMENTATION

[About the Single NAT Policy Page | 464](#)

[Creating NAT Policy Rules | 466](#)

[Deploying NAT Policy Rules | 475](#)

[NAT Policies Overview | 457](#)

[About the NAT Policies Page | 460](#)

[Creating NAT Policies | 461](#)

[Editing and Deleting NAT Policies | 463](#)



## Deploying NAT Policy Rules

To deploy an NAT policy rule:

1. Select **Configuration > NAT Policy > Policies**.

2. Click on the name of the NAT policy rules displayed.

The NAT policy rule page appears.

3. Click **Deploy**.

The **Deploy** page appears.

4. Configure your deployment as required. See [“Deploying Policies” on page 548](#).

All the NAT policy rules associated with the NAT policy are deployed. That is, the entire NAT policy is deployed.

**NOTE:** By default, all the NAT policy rules associated with the NAT policy (the entire NAT policy) are deployed when you click **Deploy**. Suppose you select a particular NAT policy rule and click **Deploy**, even then, all the NAT policy rules associated with that NAT policy are deployed.

### RELATED DOCUMENTATION

---

[About the Single NAT Policy Page | 464](#)

---

[Creating NAT Policy Rules | 466](#)

---

[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

---

[NAT Policies Overview | 457](#)

---

[About the NAT Policies Page | 460](#)

---

[Creating NAT Policies | 461](#)

---

[Editing and Deleting NAT Policies | 463](#)

## Selecting NAT Source

### IN THIS SECTION

- [Adding an Endpoint as NAT Source | 476](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box | 476](#)
- [Selecting NAT Source Using Abbreviations | 477](#)
- [Selecting a NAT Source from the End Points Panel | 478](#)
- [Creating and Selecting a NAT Source from the End Points Panel | 478](#)
- [Creating Addresses from Source Field | 479](#)

The following procedures provides various methods using which you can choose an endpoint as a NAT source:

### Adding an Endpoint as NAT Source

View and select the source endpoint from the complete list of addresses, protocols, interfaces, zones, routing instances, or ports.

1. Click the **Source** field. A list of relevant endpoints are displayed.
2. Click the **View more results** link provided at the bottom of the source endpoints. The complete list of addresses, protocols, interfaces, and ports is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, protocol, interface, zones, routing instances, or port endpoint.
4. Click check mark icon (✓) to select the endpoint as a source.

### Selecting Interfaces when GWR Resides Inside an NFX Box

The physical interfaces of an NFX box are mapped to the virtual interfaces of the Gateway Router (GWR) (vSRX) as given in [Table 166 on page 477](#). These are the default mappings provided by CSO. You may change these interface mappings based on your requirements.

Table 166: NFX and GWR Interface Mapping

NFX Physical Interface	GWR Virtual Interface
WAN 0 (ge-0/0/10)	ge-0/0/2
WAN 1 (ge-0/0/11)	ge-0/0/3
WAN 2 (xe-0/0/12)	ge-0/0/7
WAN 3 (xe-0/0/13)	ge-0/0/8
LAN-X (ge-0/0/X)	Ge-0/0/06.<vlan-id-for-X>

When you create a new NAT rule and an NFX physical interface is intended as the source endpoint, select the respective mapped GWR interface.

### Selecting NAT Source Using Abbreviations

Enter an abbreviation in the **Source** field to select the source endpoint from a filtered list of source endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of protocols, enter **PROT** or **prot**.
- To view a filtered list of interfaces, enter **INTR** or **intr**.
- To view a filtered list of zones, enter **ZONE** or **zone**.
- To view a filtered list of routing instances, enter **ROUT** or **rout**.

Click the endpoints in the filtered list to select them.

You can add a port number as a source endpoint. To do so:

1. Type **PORT** or **port** in the **Source** field.
2. Press Tab.
3. Enter the port number and press Enter.

You can also enter a range of ports by using the separator -. For example, you can enter **10-20**.

The entered port value is selected as a source endpoint.

You can also select the endpoint from the complete list of addresses, protocols, interfaces, zones, and routing instances. See [“Adding an Endpoint as NAT Source” on page 476](#).

## Selecting a NAT Source from the End Points Panel

You can select a NAT source endpoint from the **End Points** panel. Alternately, you can create a new NAT source endpoint from the **End Points** panel, see [“Creating and Selecting a NAT Source from the End Points Panel” on page 478](#).

To select an NAT source endpoint from the **End Points** panel:

1. Click the **Source** field.

2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, interfaces, protocols, zones, and routing instances.

3. (Optional) To view more information about a source endpoint, click the details icon on the right of the endpoint. To edit the source endpoint, click the edit icon (pencil symbol) on the right of the endpoint.

**NOTE:** You can only edit or view details of a source endpoint if these options appear on right side of the endpoint when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the endpoint as a source.

## Creating and Selecting a NAT Source from the End Points Panel

To create a new source endpoint from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of endpoint you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new endpoint.

- To create a new address, see [“Creating Addresses or Address Groups” on page 573](#).
- To create a new service, see [“Creating Services and Service Groups” on page 579](#).
- To create a new NAT pool, see [“Creating NAT Pools” on page 486](#).

After the endpoint is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new endpoint as a source.

## Creating Addresses from Source Field

You can use one of the following ways to create a new address from the **Source** field and use the newly created address as a source endpoint:

- Type the address directly in the **Source** field. If the address is valid, it is created immediately and added as a source endpoint.
- Create an address from the **Source** field, using the following steps:
  1. In the **Source** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.
  2. Click **Add new address** to create a new address.  
The **Create Addresses** page appears.
  3. Configure the new address. See [“Creating Addresses or Address Groups” on page 573](#).
  4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the source. Select the new address to add it to the source.

## RELATED DOCUMENTATION

---

[Selecting NAT Destination | 480](#)

---

[Creating NAT Policy Rules | 466](#)

---

[Editing, Cloning, and Deleting NAT Policy Rules | 473](#)

---

[Deploying NAT Policy Rules | 475](#)

---

[About the Single NAT Policy Page | 464](#)

---

[NAT Policies Overview | 457](#)

---

[About the NAT Policies Page | 460](#)

---

[Creating NAT Policies | 461](#)

---

[Editing and Deleting NAT Policies | 463](#)

## Selecting NAT Destination

### IN THIS SECTION

- [Adding an Endpoint as NAT Destination | 480](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box | 480](#)
- [Selecting NAT Destination Using Abbreviations | 481](#)
- [Selecting a NAT Destination from the End Points Panel | 482](#)
- [Creating and Selecting a NAT Destination from the End Points Panel | 482](#)
- [Creating Addresses from Destination Field | 483](#)
- [Creating Services from Destination Field | 483](#)

The following procedures provides various methods that you can use to choose an endpoint as a NAT destination:

### Adding an Endpoint as NAT Destination

View and select the destination endpoint from the complete list of addresses, interfaces, services, zones, routing instances, or ports.

1. Click the **Destination** field. A list of relevant endpoints are displayed.
2. Click the **View more results** link provided at the bottom of the destination endpoints. The complete list of addresses, interfaces, services, zones, and routing instances, is displayed in the **End Points** panel on the right.
3. (Optional) Click the edit icon to edit the address, service, or port endpoint.
4. Click check mark icon (✓) to select the endpoint as a destination.

### Selecting Interfaces when GWR Resides Inside an NFX Box

The physical interfaces of an NFX box are mapped to the virtual interfaces of the Gateway Router (GWR) (vSRX) as given in [Table 167 on page 481](#). These are the default mappings provided by CSO. You may change these interface mappings based on your requirements.

Table 167: NFX and GWR Interface Mapping

NFX Physical Interface	GWR Virtual Interface
WAN 0 (ge-0/0/10)	ge-0/0/2
WAN 1 (ge-0/0/11)	ge-0/0/3
WAN 2 (xe-0/0/12)	ge-0/0/7
WAN 3 (xe-0/0/13)	ge-0/0/8
LAN-X (ge-0/0/X)	Ge-0/0/06.<vlan-id-for-X>

When you create a new NAT rule and an NFX physical interface is intended as the destination endpoint, select the respective mapped GWR interface.

### Selecting NAT Destination Using Abbreviations

Enter an abbreviation in the **Destination** field to select the destination endpoint from a filtered list of destination endpoints.

- To view a filtered list of addresses, enter **ADDR** or **addr**.
- To view a filtered list of interfaces, enter **INTR** or **intr**.
- To view a filtered list of services, enter **SVCS** or **svcs**.
- To view a filtered list of zones, enter **ZONE** or **zone**.
- To view a filtered list of routing instances, enter **ROUT** or **rout**.

Click the endpoints in the filtered list to select them.

You can add a port number as a destination endpoint. To do so:

1. Enter **PORT** or **port** in **Destination**.
2. Press Tab.
3. Enter the port number and press Enter.

You can also enter a range of ports by using the separator -. For example, you can enter **10-20**.

The entered port value is selected as a destination endpoint.

You can also select the endpoint from the complete list of addresses, interfaces, services, zones, and routing instances. See [“Adding an Endpoint as NAT Destination” on page 480](#).

## Selecting a NAT Destination from the End Points Panel

You can select a NAT destination endpoint from the **End Points** panel. Alternately, you can create a new NAT destination endpoint from the **End Points** panel, see [“Creating and Selecting a NAT Destination from the End Points Panel” on page 482](#).

To select a NAT destination endpoint from the **End Points** panel:

1. Click the **Destination** field.

2. Click the lesser-than icon (<) on the right.

The **End Points** panel appears, displaying the list of available addresses, interfaces, services, zones, and routing instances.

3. (Optional) To view more information about a destination endpoint, click the details icon on the right of the endpoint. To edit the destination endpoint, click the edit icon (pencil symbol) on the right of the endpoint.

**NOTE:** You can only edit or view details of a destination endpoint if these options appear on right side of the endpoint when you hover over it. Not all endpoints provide these options.

4. Click the check mark icon (✓) to add the endpoint as a destination.

## Creating and Selecting a NAT Destination from the End Points Panel

To create a new destination endpoint from the **End Points** panel:

1. Click the add icon (+) on the top right of the panel and select the type of endpoint you want to create, among the options provided.

Based on the option you select, the respective page appears. Fill in the required details to create a new endpoint.

- To create a new address, see [“Creating Addresses or Address Groups” on page 573](#).
- To create a new service, see [“Creating Services and Service Groups” on page 579](#).

After the endpoint is created, it appears in the **Endpoints** panel.

2. Click the check mark icon (✓) to add the new endpoint as a destination.



## Creating Addresses from Destination Field

You can use one of the following ways to create a new address from the **Destination** and use the newly created address as a destination endpoint:

- Type the address directly in the **Destination** field. If the address is valid, it is created immediately and added as a destination endpoint.

- Create an address from the **Destination** field, using the following steps:

1. In the **Destination** field, type **addr**. The **Add new address** link appears at the bottom of the list of addresses.

2. Click **Add new address** to create a new address.

The **Create Addresses** page appears.

3. Configure the new address. See [“Creating Addresses or Address Groups” on page 573](#).

4. Click **Save** to save the new address.

The new address is created, and will be listed as an option for the destination. Select the new address to add it to the destination.

## Creating Services from Destination Field

To create a new service from the **Destination** field and use the newly created service as a destination endpoint:

1. In the **Destination** link, type **svcs**. The **Add new service** link appears at the bottom of the list of services.

2. Click **Add new service** to create a new service.

The **Create Services** page appears.

3. Configure the new service. See [“Creating Services and Service Groups” on page 579](#).

4. Click **Save** to save the new service.

The new service is created, and will be listed as an option for the destination. Select the new service to add it to the destination.

## RELATED DOCUMENTATION

<a href="#">About the Single NAT Policy Page   464</a>
<a href="#">Editing, Cloning, and Deleting NAT Policy Rules   473</a>
<a href="#">Creating NAT Policy Rules   466</a>
<a href="#">Deploying NAT Policy Rules   475</a>
<a href="#">NAT Policies Overview   457</a>
<a href="#">About the NAT Policies Page   460</a>
<a href="#">Creating NAT Policies   461</a>
<a href="#">Editing and Deleting NAT Policies   463</a>

## NAT Pools Overview

A NAT pool is a set of IP addresses that you can define and use for address translation. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools. Unlike static NAT, where there is a one-to-one mapping that includes destination IP address translation in one direction and source IP address translation in the reverse direction, with source NAT, you translate the original source IP address to an IP address in the address pool. With destination NAT, you translate the original destination address to an IP address in the address pool.

### RELATED DOCUMENTATION

<a href="#">NAT Policies Overview   457</a>
<a href="#">About the NAT Pools Page   484</a>
<a href="#">Creating NAT Pools   486</a>
<a href="#">Editing, Cloning, and Deleting NAT Pools   488</a>

## About the NAT Pools Page

To access this page, select **Configuration > NAT > Pools**.

Use the **NAT Pools** page to create, modify, clone, and delete NAT pools. You can filter and sort this information to get a better understanding of what you want to configure.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a NAT pool. See [“Creating NAT Pools” on page 486](#).
- Modify, clone, or delete a NAT pool. See [“Editing, Cloning, and Deleting NAT Pools” on page 488](#).
- View unused NAT pools by selecting **More > Show Unused**. Delete unused NAT pools by selecting **More > Delete Unused Items**.
- View duplicate NAT pools. Select **More > Show Duplicates**. The **Show Duplicates** page appears, displaying duplicate NAT pools. To delete a duplicate NAT pool, select it and click the delete icon (X).
- View the details of a NAT pool by selecting **More > Detailed View**, or by right-clicking a NAT pool and select **Detailed View**.
- Search for a specific NAT pool. Click the Search icon in the top right corner of the page to search for a NAT pool.

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

The search results are displayed on the same page.

- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

[Table 168 on page 485](#) provides description of the fields on the **NAT Pools** page.

Table 168: Fields on the NAT Pools Page

Field	Description
Name	Displays the name of the NAT pool.
Pool Address	Displays the IP address of the NAT pool.
Description	Displays the description provided about the NAT pool when it was created.
Pool Type	Displays the NAT pool type. A NAT pool can be of type <b>Source</b> or <b>Destination</b> .

RELATED DOCUMENTATION

<a href="#">NAT Pools Overview   484</a>
<a href="#">Creating NAT Pools   486</a>
<a href="#">Editing, Cloning, and Deleting NAT Pools   488</a>

# Creating NAT Pools

Use the **Create NAT Pools** page to create NAT pools.

To create a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Click the add icon (+).

The **Create NAT Pool** page displays fields required for creating and configuring a NAT pool.

3. Complete the configuration according to the guidelines provided in [Table 169 on page 486](#).

4. Click **OK** to save the changes. A NAT pool with the configuration you provided is created.

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

[Table 169 on page 486](#) provides guidelines on using the fields on the **Create NAT Pool** page.

**Table 169: Fields on the Create NAT Pool Page**

Field	Description
<b>General Information</b>	
Name	Enter a unique string of alphanumeric characters, dashes, and underscores. Colons, and periods are not allowed, and the maximum length is 31 characters.
Description	Enter a description for the new NAT pool; maximum length is 1024 characters.
Pool Type	Select a NAT pool type to configure: <ul style="list-style-type: none"> <li>• Source</li> <li>• Destination</li> </ul>
Pool Address	Select a NAT pool address or click <b>Add new address</b> to create a new NAT pool address.
<b>Routing Instance</b>	
Site	Select the site to which the NAT pool is applicable. <p><b>NOTE:</b> In a hub and spoke topology, both hub and spoke sites are listed in the <b>Site</b> drop-down. Ensure that you select only a spoke site, when you are creating a destination NAT pool.</p>

Table 169: Fields on the Create NAT Pool Page (*continued*)

Field	Description
Routing Instance	Select the required routing instance from the list of available routing instances for the selected site.
<b>Advanced</b>	
Host Address Base	Enter the base address of the original source IP address range. The <b>Host Address Base</b> is used for IP address shifting.
Translation	<p>Select the translation type for the incoming traffic:</p> <ul style="list-style-type: none"> <li>• No Translation—There is no translation required for the incoming traffic.</li> <li>• Port/Range—Set the global default single port range for source NAT pools with port translation.</li> <li>• Overload—Multiple source addresses are translated to pool addresses. If you set <b>Overload</b> as the translation type, the value of the <b>Pool Address</b> field cannot be an IP range or subnet, but it will be a single address.</li> </ul>
Address Pooling	<p>Select a NAT address pooling behavior:</p> <ul style="list-style-type: none"> <li>• Paired—Use this option for applications that require all sessions associated with one internal IP address to be translated to the same external IP address for multiple sessions.</li> <li>• Non-Paired—Use this option for applications that can be assigned IP addresses in a round-robin fashion.</li> </ul>
Port	Enter the port number for the destination NAT pool type.
Start	Enter the start port range for the source NAT pools, if the translation type is Port/Range. The value of the port range can be any value between 1024 to 65535.
End	Enter the end port range. The value of the port range can be any value between 1024 to 65535.
Port Overloading Factor	Configure the port overloading capacity for a source NAT pool. If the factor is set to x, each translated IP address has x times the maximum number of ports available. The value of the port overloading factor can range between 2 and 32.
Address Sharing	Enable address sharing so that multiple internal IP addresses can be mapped to the same external IP address. Select this option only when the source NAT pool is configured with no port translation. When a source NAT pool has only one or a few external IP addresses available, the address sharing option with a many-to-one address mapping increases NAT resources and improves traffic.

Table 169: Fields on the Create NAT Pool Page (continued)

Field	Description
Overflow Pool Type	Select a source pool to use when the current address pool is exhausted. <ul style="list-style-type: none"><li>• Interface—Allow the egress interface IP address to support overflow.</li><li>• Pool—Name of the source address pool.<ul style="list-style-type: none"><li>• Overflow Pool—When addresses from the original source NAT pool are exhausted, IP addresses and port numbers are allocated from the overflow pool. A user-defined source NAT pool or an egress interface can be used as the overflow pool. (When the overflow pool is used, the pool ID is returned with the address.)</li></ul></li></ul>

RELATED DOCUMENTATION

[NAT Pools Overview | 484](#)

[About the NAT Pools Page | 484](#)

[Editing, Cloning, and Deleting NAT Pools | 488](#)

## Editing, Cloning, and Deleting NAT Pools

IN THIS SECTION

- [Editing NAT Pools | 488](#)
- [Cloning NAT Pools | 489](#)
- [Deleting NAT Pools | 489](#)

### Editing NAT Pools

To modify the parameters configured for a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool that you want to edit, and click the edit icon (pencil symbol) at the top right corner of the table, or right-click and select **Edit NAT Pool**.

The **Edit NAT Pool** page appears, displaying the same options that are displayed when creating a new NAT pool.

3. Modify the parameters according to the guidelines provided in [“Creating NAT Pools” on page 486](#).
4. Click **OK** to save the changes. If you click **OK**, you see the modified NAT pool in the **NAT Pools** page.  
If you want to discard your changes, click **Cancel** instead.

## Cloning NAT Pools

To clone a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

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

The **Clone NAT Pool** page appears with editable fields. Modify the parameters of the cloned NAT pool as per your requirements.

3. Click **OK** to save the changes. If you click **OK**, the cloned NAT pool appears at the end of the NAT pools list in the **NAT Pools** page.  
If you want to discard your changes, click **Cancel** instead.

## Deleting NAT Pools

To delete a NAT pool:

1. Select **Configuration > NAT > Pools**.

The **NAT Pools** page appears.

2. Select the NAT pool you want to delete and then click the delete icon **(X)**.

An alert message appears, verifying that you want to delete the NAT pool.

3. Click **Yes** to delete the NAT pool. If you click **Yes**, the selected NAT pool is deleted.  
If you do not want to delete, click **Cancel** instead.

## RELATED DOCUMENTATION

[NAT Pools Overview | 484](#)

[About the NAT Pools Page | 484](#)

[Creating NAT Pools | 486](#)



# Managing IPS Signatures and Profiles

## IN THIS CHAPTER

- [About the IPS Signatures Page | 491](#)
- [About the IPS Profiles Page | 496](#)
- [Create IPS Profiles | 498](#)
- [Edit, Clone, and Delete IPS Profiles | 499](#)
- [About the <IPS-Profile-Name> / Rules Page | 501](#)
- [Create IPS or Exempt Rules | 502](#)
- [Edit, Clone, and Delete IPS or Exempt Rules | 511](#)

## About the IPS Signatures Page

### IN THIS SECTION

- [Tasks You Can Perform | 492](#)
- [Field Descriptions | 492](#)

To access this page, select **Configure > IPS > IPS Signature**.

Use intrusion prevention system (IPS) signatures to monitor and prevent intrusions. IPS compares traffic against signatures of known threats and blocks traffic when a threat is detected.

### Tasks You Can Perform

- View the details of an IPS signature—Select an IPS signature and click **More > Details**, or mouse over the IPS signature and click the **Detailed View** icon. The IPS Signature Details View page appears. See [Table 171 on page 493](#) for an explanation of fields on this page.
- View the details of an IPS signature static group—Select an IPS signature static group and click **More > Details**, or mouse over the IPS signature static group and click the **Detailed View** icon. The IPS Static Group Details page appears. See [Table 172 on page 495](#) for an explanation of fields on this page.
- View the details of an IPS signature dynamic group—Select an IPS signature dynamic group and click **More > Details**, or mouse over the IPS signature dynamic group and click the **Detailed View** icon. The IPS Signature Dynamic Details View page appears. See [Table 173 on page 495](#) for an explanation of fields on this page.
- Search for IPS signatures, static groups or dynamic groups by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter IPS signatures, static groups or dynamic groups—Click the filter icon (funnel) and specify one or more filtering criteria. The filtered results are displayed on the same page.
- Sort IPS signatures, static groups or dynamic groups—Click a column name to sort the data in the grid (table) based on the column name.

**NOTE:** Sorting is applicable only to some fields.

- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you want displayed on the page.

### Field Descriptions

[Table 170 on page 492](#) describes the field on the IPS Signatures page.

**Table 170: Fields on the IPS Signatures Page**

Field	Description
Name	Name of the IPS signature, IPS signature static group, or IPS signature dynamic group.
Severity	Severity level of the attack that the signature will report.
Category	Category of the attack object.

Table 170: Fields on the IPS Signatures Page (*continued*)

Field	Description
Object Type	Displays the type of attack object: <ul style="list-style-type: none"> <li>• Static Group</li> <li>• Dynamic Group</li> <li>• Signature</li> <li>• Protocol Anomaly</li> <li>• Compound Attack</li> </ul>
Recommended	Indicates whether the attack objects are recommended by Juniper (True) or not (False).
Action	Action taken when the monitored traffic matches the attack objects specified in the IPS rules.
Definition Type	Displays PREDEFINED, which indicates that the IPS signature, static group, or dynamic group was created by CSO.
CVE	Displays the Common Vulnerabilities and Exposures (CVE) identifier or name associated with the threat.
CERT	Displays the computer emergency response team (CERT) advisory number associated with the threat.
BUG	Displays the list of bugs that are related to the signature attack.
False Positives	Displays the frequency with which the attack produces a false positive on your network.
Service	Protocol or service that the attack uses to enter your network.
Performance Impact	Performance impact of the IPS signature.
Direction	Direction of the traffic for which the attack is detected; for example, client to server.

Table 171: Fields on the IPS Signature Details View Page

Field	Description
Name	Name of the IPS signature.
Description	Description of the IPS signature.

Table 171: Fields on the IPS Signature Details View Page (*continued*)

Field	Description
URL(s)	Displays the URLs that have the details about the signature attack. For example, <a href="http://www.faqs.org/rfcs/rfc2865.html">http://www.faqs.org/rfcs/rfc2865.html</a> .
Category	See <a href="#">Table 170 on page 492</a> .
Recommended	See <a href="#">Table 170 on page 492</a> .
Action	See <a href="#">Table 170 on page 492</a> .
Keywords	Keywords associated with the IPS signature.
Severity	See <a href="#">Table 170 on page 492</a> .
BUGS	See <a href="#">Table 170 on page 492</a> .
CERT	See <a href="#">Table 170 on page 492</a> .
CVE	See <a href="#">Table 170 on page 492</a> .
<i>Signature Details</i>	
Binding	Protocol or service that the attack uses to enter your network.
Service	For service binding, displays the service the attack uses to enter your network.
Time Count	Number of time that IPS detects the attack in a specified time scope.
Signature	<p>Displays (in a table) the signature attack objects configured as part of the IPS signature. For each row, the following fields are displayed:</p> <ul style="list-style-type: none"> <li>• No.—Unique identifier for the signature attack object.</li> <li>• Context—Attack context, which defines the location of the signature where IPS should look for the attack.</li> <li>• Direction—Connection direction of the attack.</li> <li>• Pattern—Signature pattern (in Juniper’s proprietary regular expression syntax) of the attack to be detected.</li> <li>• Regex—Regular expression to match malicious or unwanted behavior over the network.</li> <li>• Negated—Indicates whether the pattern should be excluded from being matched (true) or not (false).</li> </ul>

Table 171: Fields on the IPS Signature Details View Page (*continued*)

Field	Description
Anomaly	<p>Displays (in a table) the protocol anomaly attack objects configured as part of the IPS signature. For each row, the following fields are displayed:</p> <ul style="list-style-type: none"> <li>• No.—Unique identifier for the anomaly.</li> <li>• Anomaly—Protocol or service for which the anomaly is defined.</li> <li>• Direction—Connection direction of the attack.</li> </ul>

Table 172: Fields on the IPS Static Group Details Page

Field	Description
Name	Name of the IPS signature static group.
Description	Description of the IPS signature static group.
Group Members	<p>Displays the IPS signatures or IPS signature dynamic groups that are part of the IPS static group. See <a href="#">Table 170 on page 492</a> for an explanation of the fields in the table.</p> <p>To view the details, select a row, click <b>More &gt; Details</b>, or mouse over a row and click the <b>Detailed View</b> icon. Depending on the object type, the IPS Signature Details View page or IPS Signature Dynamic Details View page appears. See <a href="#">Table 171 on page 493</a> and <a href="#">Table 173 on page 495</a> for an explanation of the fields on these pages.</p>

Table 173: Fields on the IPS Signature Dynamic Details View Page

Field	Description
Name	Name of the IPS signature dynamic group.
Severity	Severity filters used for the dynamic group.
Service	Services filters used for the dynamic group.
Category	Category filters used for the dynamic group.
Recommended	Indicates whether predefined attack objects recommended by Juniper are added to the dynamic group (true) or not (false).
Direction	Traffic direction (for which the attack is detected) filters used for the dynamic group.
Performance Impact	Performance impact filter used for the dynamic group.

Table 173: Fields on the IPS Signature Dynamic Details View Page (*continued*)

Field	Description
False Positive	False positive filter used for the dynamic group.
Age of Attack	Age of the attack (in years) used as a filter for the dynamic group.
CVSS Score	Common Vulnerability Scoring System (CVSS) score used as a filter for the dynamic group.
File Type	File type of the attack used as a filter for the dynamic group.
Vulnerability Type	Vulnerability type of the attack used as a filter for the dynamic group.
Object Type	Type of object (anomaly or signature) used as a filter for the dynamic group.
Vendor Description	Vendor or product that the attack belongs to.

## RELATED DOCUMENTATION

[About the IPS Profiles Page](#) | 496

## About the IPS Profiles Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 497
- [Field Descriptions](#) | 497

To access this page, select **Configure > IPS > IPS Profiles**.

Use intrusion prevention system (IPS) IPS Profiles page to manage IPS profiles. IPS profiles can be associated with IPS or exempt rules and deployed on a device by associating a profile with a firewall intent and deploying the firewall policy on the device.

Tasks You Can Perform

- Create an IPS profile—See [“Create IPS Profiles” on page 498](#).
- Edit, clone, or delete an IPS profile—See [“Edit, Clone, and Delete IPS Profiles” on page 499](#).
- Manage the IPS rules associated with an IPS profile—Click the **IPS-Profile-Name** to manage the IPS rules associated with the IPS profile. See [“About the <IPS-Profile-Name> / Rules Page” on page 501](#).
- Search for IPS profiles by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort IPS profiles—Click a column name to sort the data in the grid (table) based on the column name.

**NOTE:** Sorting is applicable only to some fields.

Field Descriptions

[Table 174 on page 497](#) describes the field on the IPS Profiles page.

Table 174: Fields on the IPS Profiles Page

Field	Description
Name	Name of the IPS profile.  Click the <b>IPS-Profile-Name</b> to manage the IPS rules associated with the IPS profile. The <i>IPS-Profile-Name</i> / Rules page appears. See <a href="#">“About the &lt;IPS-Profile-Name&gt; / Rules Page” on page 501</a> .
Definition Type	Indicates whether the IPS profile was system-generated (PREDEFINED) or created by a user (CUSTOM).
Description	Description of the IPS profile.

RELATED DOCUMENTATION

| [About the IPS Signatures Page](#) | 491

# Create IPS Profiles

Contrail Service Orchestration (CSO) contains predefined intrusion prevention system (IPS) profiles that you can use. You can create customized IPS profiles from the Create IPS Profile page.

To create a customized IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click the add (+) icon.

The Create IPS Profile page appears.

3. Complete the configuration according to the guidelines in [Table 175 on page 498](#).

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

4. Click **OK**.

You are returned to the IPS Profiles page and a confirmation message is displayed indicating that the IPS profile is created.

After you create an IPS profile, you can add one or more IPS or exempt rules to the profile, and use the IPS profile in a firewall policy intent.

**Table 175: Create IPS Profile Settings**

Setting	Guideline
<b>Name</b>	Enter a unique name for the IPS profile that is a string of alphanumeric characters and some special characters (colon, hyphen, period, and underscore). No spaces are allowed and the maximum length is 255 characters.
<b>Description</b>	Enter a description for the IPS profile; the maximum length is 255 characters.

## RELATED DOCUMENTATION

<a href="#">Create IPS or Exempt Rules   502</a>
<a href="#">Adding Firewall Policy Intents   291</a>



## Edit, Clone, and Delete IPS Profiles

### IN THIS SECTION

- [Edit IPS Profiles | 499](#)
- [Clone IPS Profiles | 500](#)
- [Delete IPS Profiles | 500](#)

You can edit, clone, or delete IPS profiles.

### Edit IPS Profiles

You can edit only customized IPS profiles and not predefined (system-generated) profiles.

To edit a customized IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select a customized IPS profile and click the edit (pencil) icon.

The Edit IPS Profile page appears, displaying the same fields that are presented when you create an IPS profile.

3. Modify the IPS profile fields as needed. See [“Create IPS Profiles” on page 498](#).

**NOTE:** You can only modify the description and not the name.

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

You are returned to the IPS Profiles page and a message that the IPS profile was successfully updated is displayed.

If the IPS profile is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

## Clone IPS Profiles

Cloning enables you to easily create a new IPS profile based on an existing one. You can clone predefined or customized IPS profiles and modify the parameters as needed.

To clone an IPS profile:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select an IPS profile and select **More > Clone**.

The Clone IPS Profile page appears, displaying the same fields that are presented when you create an IPS profile.

3. Modify the IPS profile fields as needed. See [“Create IPS Profiles” on page 498](#).

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

You are returned to the IPS Profiles page and a message that the IPS profile was successfully created is displayed.

## Delete IPS Profiles

### NOTE:

- You can delete only customized IPS profiles that are not referenced in a firewall policy intent.
- You cannot delete predefined (system-generated) IPS profiles.

To delete one or more customized IPS profiles:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Select one or more customized IPS profiles and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

3. Click **Yes** to proceed with the deletion.

You are returned to the IPS Profiles page and a message indicating the status of the delete operation is displayed.

RELATED DOCUMENTATION

| [About the <IPS-Profile-Name> / Rules Page](#) | 501

## About the <IPS-Profile-Name> / Rules Page

### IN THIS SECTION

- [Tasks You Can Perform](#) | 501
- [Field Descriptions](#) | 501

To access this page, select **Configure > IPS > IPS Profiles > *IPS-Profile-Name***.

Use the *IPS-Profile-Name* / Rules page to manage intrusion prevention system (IPS) rules and exempt rules. IPS profiles can be associated with IPS or exempt rules and deployed on a device by associating the IPS profile with a firewall policy intent and deploying the firewall policy on the device.

### Tasks You Can Perform

- Create an IPS rule—See [“Create IPS or Exempt Rules” on page 502](#).
- Create an exempt rule—See [“Create IPS or Exempt Rules” on page 502](#).
- Edit, clone, or delete IPS or exempt rules—See [“Edit, Clone, and Delete IPS or Exempt Rules” on page 511](#).
- Search for rules by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter rules—Click the filter icon (funnel) and specify one or more filtering criteria. The filtered results are displayed on the same page.

**NOTE:** Filtering is applicable only to some fields.

### Field Descriptions

[Table 176 on page 502](#) describes the field on the *IPS-Profile-Name* / Rules page.

Table 176: Fields on the &lt;IPS-Profile-Name&gt; / Rules Page

Field	Description
Name	Name of the IPS rule or exempt rule.
IPS Signatures	Displays the IPS signatures associated with the IPS rule or exempt rule. If there is more than one signature associated with the rule, the number of additional signatures is displayed. Mouse over the number to view the full list of signatures.
IPS Action	<ul style="list-style-type: none"> <li>For IPS rules, displays the action to be taken when the rule is matched.</li> <li>For exempt rules, displays <b>Not Applicable</b> because exempt rules are not associated with an action.</li> </ul>
Additional Actions	<ul style="list-style-type: none"> <li>For IPS rules, displays: <ul style="list-style-type: none"> <li>Configured, if additional actions (to be taken when the rule is matched) are configured. Mouse over the gear icon to view the additional actions configured.</li> <li>Not Configured, if no additional actions are configured.</li> </ul> </li> <li>For exempt rules, displays <b>Not Applicable</b> because exempt rules are not associated with any actions.</li> </ul>
Details	<p>Displays whether the rule is an IPS rule or an exempt rule.</p> <p>Mouse over the <b>Details</b> field and then mouse over the ellipsis (...) displayed to access a menu to edit, clone, or delete the rule. See <a href="#">“Edit, Clone, and Delete IPS or Exempt Rules” on page 511</a>.</p>

## RELATED DOCUMENTATION

[About the IPS Signatures Page | 491](#)
[About the IPS Profiles Page | 496](#)

## Create IPS or Exempt Rules

## IN THIS SECTION

- [Create IPS Rules | 503](#)
- [Create Exempt Rules | 510](#)

You can create intrusion prevention system (IPS) rules or exempt rules only for customized IPS profiles.

Create IPS Rules

To create an IPS rule:

- 1. Select **Configuration > IPS > IPS Profiles**.  
The IPS Profiles page appears.
- 2. Click **IPS-Profile-Name** for the profile for which you want to create a rule.  
The *IPS-Profile-Name* / Rules page appears.
- 3. Select **Create > IPS Rule**.  
The parameters for an IPS rule appear inline at the top of the page.
- 4. Complete the configuration according to the guidelines in [Table 177 on page 503](#).

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

- 5. Click **Save** to save your changes.  
The changes are saved and a confirmation message appears at the top of the page.  
You can use the IPS profile in a firewall policy intent and deploy the firewall policy on the device, which deploy the IPS and exempt rules associated with the profile.

Table 177: Create IPS Rule Settings

Setting	Guideline
Rule Name	CSO generates a unique rule name by default. You can modify the name if needed.  The name must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (colons, hyphens, forward slashes, periods, and underscores); 63-character maximum.
Description	Enter a description for the rule; the maximum length is 1024 characters.

Table 177: Create IPS Rule Settings (continued)

Setting	Guideline
IPS Signatures	<p>You can add one or more IPS signatures and IPS signature static and dynamic groups to be associated with the rule:</p> <ol style="list-style-type: none"><li>1. Click inside the text box with the + icon. A list of IPS signatures and IPS signature static and dynamic groups appears.</li><li>2. (Optional) Enter a search term and press Enter to filter the list of items displayed.</li><li>3. Click a list item to add it to the IPS signatures and IPS signature static or dynamic groups associated with the rule.</li><li>4. (Optional) Repeat the preceding step to add more signatures, static groups, and dynamic groups.</li><li>5. Click the <b>View more results</b> link to view the full list of IPS signatures and IPS signature static and dynamic groups. The full list is displayed in the End Points panel on the right. To add one or more signatures, static groups, or dynamic groups:<ol style="list-style-type: none"><li>a. Mouse over a list item and select the check box that appears.</li><li>b. Repeat the preceding step for the other signatures, static groups, or dynamic groups that you want to add.</li><li>c. Click the check mark icon ( ✓ ) at the top of the End Points panel, and select <b>Signatures</b>. The signatures, static groups, or dynamic groups that you selected are added and displayed in the IPS Signatures field.</li></ol></li></ol>

Table 177: Create IPS Rule Settings (continued)

Setting	Guideline
IPS Action	<p>Select the action to be taken when the monitored traffic matches the attack objects specified in the rules:</p> <ul style="list-style-type: none"> <li>• None—No action is taken. Use this action to only generate logs for some traffic.</li> <li>• Ignore—Stops scanning traffic for the rest of the connection if an attack match is found. IPS disables the rulebase for the specific connection.</li> <li>• Close Client and Server—Closes the connection and sends a TCP reset (RST) packet to both the client and the server.</li> <li>• Close Client—Closes the connection and sends an RST packet to the client, but not to the server.</li> <li>• Close Server—Closes the connection and sends an RST packet to the server, but not to the client.</li> <li>• Drop Connection—Drops all packets associated with the connection, preventing traffic for the connection from reaching its destination. Use this action to drop connections for traffic that is not prone to spoofing.</li> <li>• Drop Packet—Drops a matching packet before it can reach its destination but does not close the connection. Use this action to drop packets for attacks in traffic that is prone to spoofing, such as UDP traffic. Dropping a connection for such traffic could result in a denial of service that prevents you from receiving traffic from a legitimate source-IP address.</li> <li>• Recommended (default)—Uses the action that Juniper Networks recommends when that attack is detected. All predefined attack objects have a default action associated with them.</li> <li>• Diffserv Marking—Assigns the specified differentiated services code point (DSCP) value to the packet in an attack and pass the packet on normally.</li> </ul> <p>When you select Diffserv Marking, you must enter a DSCP value:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Code Point: Vaule</b> hyperlink. The Code point for Diffserve Marking action popup appears.</li> <li>2. In the <b>Code Point</b> field, enter a DSCP value from 0 through 63.</li> <li>3. Click <b>OK</b>. You are returned to the previous page; the value that you entered is displayed</li> </ol>

Table 177: Create IPS Rule Settings (continued)

Setting	Guideline
Additional Actions	



Table 177: Create IPS Rule Settings (continued)

Setting	Guideline
	<p>In addition to the IPS action, you can configure one or more of the following additional actions:</p> <ul style="list-style-type: none"> <li> <b>Notifications</b>—When attacks are detected, you can choose to log the attack and create log records with attack information and send that information to the log server.            To configure notifications:           <ol style="list-style-type: none"> <li>Click the <b>Notification</b> link.                The Notification page appears.</li> <li>Complete the configuration according to the guidelines shown in <a href="#">Table 178 on page 508</a>.</li> <li>Click <b>OK</b>.                You are returned to the previous page. A gear icon next to the Notification link indicates that you have configured notification settings.</li> </ol> </li> <li> <b>IP actions</b>—When attacks are detected, you can configure actions that you want IPS to take against future connections that use the same IP address.            To configure IP actions:           <ol style="list-style-type: none"> <li>Click the <b>IP Action</b> link.                The IP Action page appears.</li> <li>Complete the configuration according to the guidelines shown in <a href="#">Table 179 on page 509</a>.</li> <li>Click <b>OK</b>.                You are returned to the previous page. A gear icon next to the IP Action link indicates that you have configured IP action settings.</li> </ol> </li> <li> <b>Additional actions</b>—When attacks are detected, you can configure additional actions that you want CSO to take.            To configure additional actions:           <ol style="list-style-type: none"> <li>Click the <b>Additional</b> link.                The Additional page appears.</li> <li>Complete the configuration according to the guidelines shown in <a href="#">Table 180 on page 510</a>.</li> <li>Click <b>OK</b>.</li> </ol> </li> </ul>

Table 177: Create IPS Rule Settings (continued)

Setting	Guideline
	You are returned to the previous page. A gear icon next to the Additional link indicates that you have configured additional settings.

Table 178: Notification Settings

Setting	Guideline
<b>Attack Logging</b>	Select the <b>Enable</b> check box to log an attack when it is detected.
<b>Alert Flag</b>	Select the <b>Enable</b> check box to set the alert flag in the attack log.
<b>Log Packets</b>	<p>Select the <b>Enable</b> check box to log packets when an attack is detected.</p> <p>In response to a rule match, you can capture the packets received before and after the attack for further offline analysis of attacker behavior. You can configure the number of pre-attack and post-attack packets to be captured for this attack, and limit the duration of post-attack packet capture by specifying a timeout value.</p> <p>You must specify at least one of the Packets Before, Packets After, or Post Window Timeout fields.</p>
<b>Packets Before</b>	<p>Specify the number of packets received before an attack that should be captured for further analysis of the behavior of the attack.</p> <p>Range: 1 through 255.</p>
<b>Packets After</b>	<p>Specify the number of packets received after an attack that should be captured for further analysis of attacker behavior.</p> <p>Range: 1 through 255.</p>
<b>Post Window Timeout</b>	<p>Specify a time limit (in seconds) for capturing packets received after an attack. No packets are captured after the specified timeout has elapsed.</p> <p>Range: 1 through 1800.</p>

Table 179: IP Action Settings

Setting	Guideline
<b>IP Action</b>	<p>Select the action to be taken on future connections that use the same IP address:</p> <p><b>NOTE:</b> If there is an IP action match with more than one rule, then the most severe IP action of all the matched rules is applied. In decreasing order of severity, the actions are block, close, and notify.</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)—Do not take any action. This is similar to if you did not configure the IP action.</li> <li>• <b>IP Notify</b>—Don't take any action on future traffic but log the event.</li> <li>• <b>IP Close</b>—Close future connections of new sessions that match the IP address by sending RST packets to the client and server.</li> <li>• <b>IP Block</b>—Block future connections of any session that matches the IP address.</li> </ul>
<b>IP Target</b>	<p>Specify how the traffic should be matched for the configured IP actions:</p> <ul style="list-style-type: none"> <li>• <b>None</b>—Do not match any traffic.</li> <li>• <b>Destination Address</b>—Match traffic based on the destination IP address of the attack traffic.</li> <li>• <b>Service</b>—For TCP and UDP, matches traffic based on the source IP address, source port, destination IP address, and destination port of the attack traffic.</li> <li>• <b>Source Address</b>—Matches traffic based on the source IP address of the attack traffic.</li> <li>• <b>Source Zone</b>—Matches traffic based on the source zone of the attack traffic.</li> <li>• <b>Source Zone Address</b>—Matches traffic based on the source zone and source IP address of the attack traffic.</li> <li>• <b>Zone Service</b>—Matches traffic based on the source zone, destination IP address, destination port, and protocol of the attack traffic.</li> </ul>
<b>Refresh Timeout</b>	<p>Select the <b>Enable</b> check box to refresh the IP action timeout (that you specify in the Timeout Value field) if future traffic matches the IP actions configured.</p>
<b>Timeout Value</b>	<p>Configure the number of seconds that you want the IP action to remain in effect. For example, if you configure a timeout of 3600 seconds (1 hour) and traffic matches the IP actions configured, the IP action remains in effect for 1 hour.</p> <p>Range: 0 through 64,800 seconds.</p>
<b>Log Taken</b>	<p>Select the <b>Enable</b> check box to log the information about the IP action against the traffic that matches a rule.</p>
<b>Log Creation</b>	<p>Select the <b>Enable</b> check box generate an event when the IP action filter is triggered.</p>

Table 180: Additional Settings

Setting	Guideline
<b>Severity</b>	<p>Select a severity level to override the inherited attack severity in the rules.</p> <p>The most dangerous level is critical, which attempts to crash your server or gain control of your network. Informational is the least dangerous level and is used by network administrators to discover holes in their security systems.</p>
<b>Terminal</b>	Select the <b>Enable</b> check box to mark the IPS rule as terminal. When a terminal rule is matched, the device stops matching for the rest of the rules in that IPS profile.

## Create Exempt Rules

To create an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to create a rule.

The *IPS-Profile-Name* / Rules page appears.

3. Select **Create > Exempt Rule**.

The parameters for an exempt rule appear inline at the top of the page.

4. You can configure only the following fields:

- Rule Name
- Description
- IPS Signatures

See [Table 177 on page 503](#) for an explanation of these fields.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message appears at the top of the page.

You can use the IPS profile in a firewall policy intent and deploy the firewall policy on the device, which deploy the IPS and exempt rules associated with the profile.

## RELATED DOCUMENTATION

| [Adding Firewall Policy Intents](#) | 291

## Edit, Clone, and Delete IPS or Exempt Rules

### IN THIS SECTION

- [Edit IPS or Exempt Rules](#) | 511
- [Clone IPS or Exempt Rules](#) | 512
- [Delete IPS or Exempt Rules](#) | 512

You can edit, clone, or delete IPS or exempt rules.

### Edit IPS or Exempt Rules

You can edit IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To edit an IPS or an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to edit a rule.

The *IPS-Profile-Name* / Rules page appears.

3. Mouse over the **Details** field, then mouse over the ellipsis (...) that appears, and from the menu, select **Edit**.

The rule that you selected for editing appears inline at the top of the page.

4. Modify the rule as needed. See [“Create IPS or Exempt Rules” on page 502](#).

**NOTE:** You can modify all fields except the name.

5. Click **Save** to save your changes.

The changes are saved and a confirmation message appears at the top of the page.

If the IPS or exempt rule belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

### Clone IPS or Exempt Rules

Cloning enables you to easily create a new IPS or exempt rule based on an existing one. You can clone IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To clone an IPS or an exempt rule:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click **IPS-Profile-Name** for the profile for which you want to clone a rule.

The *IPS-Profile-Name / Rules* page appears.

3. Select a rule and select **More > Clone**. Alternatively, Mouse over the **Details** field, then mouse over the ellipsis (...) that appears, and from the menu, select **Clone**.

The rule that you selected for cloning appears inline at the top of the page.

4. Modify the rule as needed. See [“Create IPS or Exempt Rules” on page 502](#).

5. Click **Save** to save your changes.

The new rule is created and a confirmation message appears at the top of the page.

### Delete IPS or Exempt Rules

You can delete IPS and exempt rules associated only with customized IPS profiles and not rules associated with predefined (system-generated) profiles.

To delete one or more IPS or exempt rules:

1. Select **Configuration > IPS > IPS Profiles**.

The IPS Profiles page appears.

2. Click ***IPS-Profile-Name*** for the profile for which you want to delete one or more rules.

The *IPS-Profile-Name* / Rules page appears.

3. Select one or more rules and click the delete (trash can) icon

A warning message appears asking you to confirm the deletion.

4. Click **Yes** to proceed with the deletion.

A message indicating the status of the delete operation appears at the top of the page.

If the IPS or exempt rule that you deleted belongs to an IPS profile that is referenced in a firewall policy intent, then the firewall policy is marked for deployment. You must deploy the firewall policy for the changes to take effect on the device.

## RELATED DOCUMENTATION

# Managing SSL Proxies

## IN THIS CHAPTER

- [SSL Forward Proxy Overview | 514](#)
- [About the SSL Proxy Policy Page | 520](#)
- [Creating SSL Proxy Policy Intents | 522](#)
- [Editing, Cloning, and Deleting SSL Proxy Policy Intents | 526](#)
- [Understanding How SSL Proxy Policy Intents Are Applied | 529](#)
- [About the SSL Proxy Profiles Page | 531](#)
- [Creating SSL Forward Proxy Profiles | 533](#)
- [Editing, Cloning, and Deleting SSL Forward Proxy Profiles | 539](#)
- [Configuring and Deploying an SSL Forward Proxy Policy | 542](#)

## SSL Forward Proxy Overview

### IN THIS SECTION

- [Supported Ciphers in Proxy Mode | 516](#)
- [Server Authentication | 517](#)
- [Root CA | 518](#)
- [Trusted CA List | 518](#)
- [Session Resumption | 519](#)
- [SSL Proxy Logs | 519](#)

Secure Sockets Layer (SSL) is an application-level protocol that provides encryption technology for the Internet. SSL, also called *Transport Layer Security* (TLS), ensures the secure transmission of data between a client and a server through a combination of privacy, authentication, confidentiality, and data integrity. SSL relies on certificates and private–public key exchange pairs for this level of security.



Server authentication guards against fraudulent transmissions by enabling a Web browser to validate the identity of a Web server. Confidentiality mechanisms ensure that communications are private. SSL enforces confidentiality by encrypting data to prevent unauthorized users from eavesdropping on electronic communications. Finally, message integrity ensures that the contents of a communication have not been tampered with.

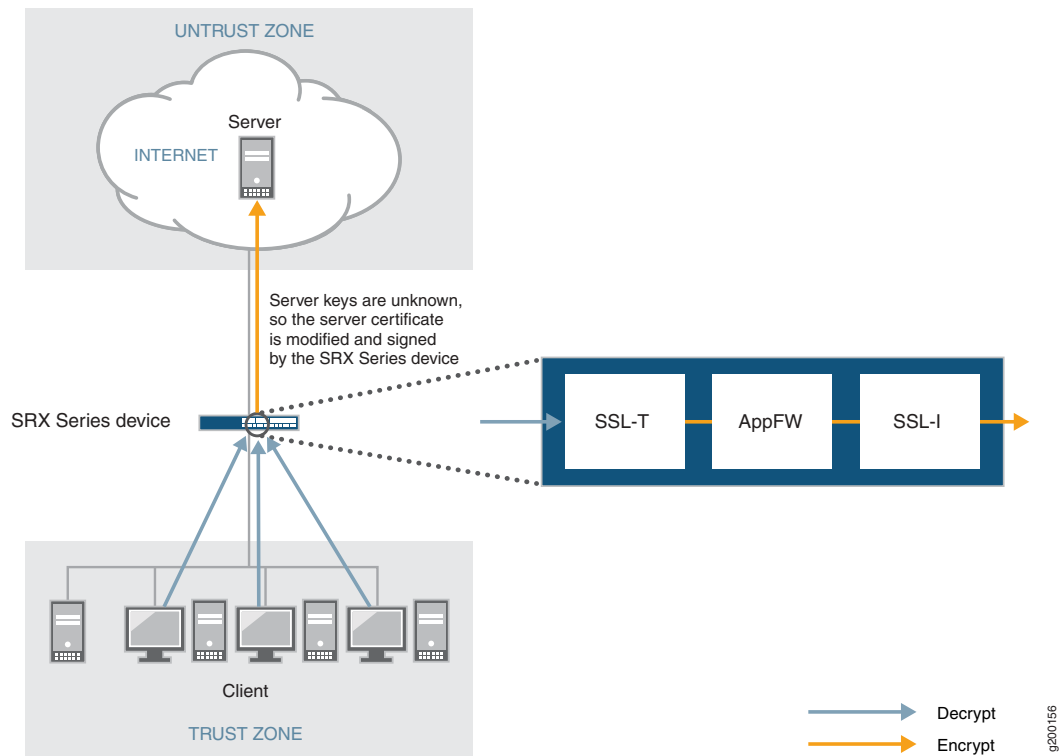
SSL forward proxy is a transparent proxy; that is, it performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL forward proxy ensures that it has the keys to encrypt and decrypt the payload:

- For the server, SSL forward proxy acts as a client—Because SSL forward proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL forward proxy acts as a server—SSL forward proxy first authenticates the original server and replaces the public key in the original server certificate with a key that is known to it. It then generates a new certificate by replacing the original issuer of the certificate with its own identity and signs this new certificate with its own public key (provided as a part of the proxy profile configuration). When the client accepts such a certificate, it sends a shared pre-master key encrypted with the public key on the certificate. Because SSL forward proxy replaced the original key with its own key, it is able to receive the shared pre-master key. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

[Figure 12 on page 516](#) shows how SSL forward proxy works on an encrypted payload. When application firewall (AppFW) is configured, SSL forward proxy acts as an SSL server terminating the SSL session from the client and a new SSL session is established to the server. The device decrypts and then re-encrypts all SSL forward proxy traffic. SSL forward proxy uses the following services:

- SSL-T-SSL terminator on the client side.
- SSL-I-SSL initiator on the server side.
- Configured AppFW services use the decrypted SSL sessions.

Figure 12: SSL Forward Proxy on an Encrypted Payload



This topic has the following sections:

Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. [Table 181 on page 516](#) displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 181: Supported Ciphers in Proxy Mode

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_MD5	RSA key exchange	128-bit RC4	Message Digest 5 (MD5) hash

Table 181: Supported Ciphers in Proxy Mode (*continued*)

SSL Cipher	Key Exchange Algorithm	Data Encryption	Message Integrity
RSA_WITH_RC4_128_SHA	RSA key exchange	128-bit RC4	Secure Hash Algorithm (SHA) hash
RSA_WITH_DES_CBC_SHA	RSA key exchange	DES CBC	SHA hash
RSA_WITH_3DES_EDE_CBC_SHA	RSA key exchange	3DES EDE/CBC	SHA hash
RSA_WITH_AES_128_CBC_SHA	RSA key exchange	128-bit AES/CBC	SHA hash
RSA_WITH_AES_256_CBC_SHA	RSA key exchange	256-bit AES/CBC	SHA hash
RSA_EXPORT_WITH_RC4_40_MD5	RSA-export	40-bit RC4	MD5 hash
RSA_EXPORT_WITH_DES40_CBC_SHA	RSA-export	40-bit DES/CBC	SHA hash
RSA_EXPORT1024_WITH_DES_CBC_SHA	RSA 1024 bit export	DES/CBC	SHA hash
RSA_EXPORT1024_WITH_RC4_56_MD5	RSA 1024 bit export	56-bit RC4	MD5 hash
RSA_EXPORT1024_WITH_RC4_56_SHA	RSA 1024 bit export	56-bit RC4	SHA hash
RSA-WITH-AES-256-GCM-SHA384	RSA key exchange	256-bit AES/GCM	SHA384 hash
RSA-WITH-AES-256-CBC-SHA256	RSA key exchange	256-bit AES/CBC	SHA256 hash
RSA-WITH-AES-128-GCM-SHA256	RSA key exchange	128-bit AES/GCM	SHA256 hash
RSA-WITH-AES-128-CBC-SHA256	RSA key exchange	128-bit AES/CBC	SHA256 hash

## Server Authentication

Implicit trust between the client and the device (because the client accepts the certificate generated by the device) is an important aspect of SSL proxy. It is extremely important that server authentication is not compromised; however, in reality, self-signed certificates and certificates with anomalies are in abundance. Anomalies can include expired certificates, instances of common name not matching a domain name, and so forth.

You can specify that the SSL forward proxy should ignore server authentication completely. In this case, SSL forward proxy ignores errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry).

You can specify whether the SSL proxy should ignore server authentication errors or not during the creation of an SSL forward proxy profile.

- If you specify that server authentication errors should *not* be ignored, the following scenarios occur:
  - If authentication succeeds, a new certificate is generated by replacing the keys and changing the issuer name to the issuer name that is configured in the root CA certificate in the proxy profile.
  - If authentication fails, the connection is dropped.
- If you specify that server authentication errors should be ignored, the following scenarios occur:

**NOTE:** We do not recommend that you configure this option for authentication because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.

- If the certificate is self-signed, a new certificate is generated by replacing the keys only. The issuer name is not changed. This ensures that the client browser displays a warning that the certificate is not valid.
- If the certificate has expired or if the common name does not match the domain name, a new certificate is generated by replacing the keys and changing the issuer name to SSL-PROXY: DUMMY\_CERT:GENERATED DUE TO SRVR AUTH FAILURE. This ensures that the client browser displays a warning that the certificate is not valid.

## Root CA

In a public key infrastructure (PKI) hierarchy, the root CA is at the top of the trust path. The root CA identifies the server certificate as a trusted certificate.

## Trusted CA List

SSL forward proxy ensures secure transmission of data between a client and a server. Before establishing a secure connection, SSL forward proxy checks certificate authority (CA) certificates to verify signatures on server certificates. For this reason, a reasonable list of trusted CA certificates is required to effectively authenticate servers.

### Session Resumption

An SSL session refers to the set of parameters and encryption keys that are created when a full handshake is performed. A connection is the conversation or active data transfer that occurs within the session. The computational overhead of a complete SSL handshake and generation of master keys is considerable. In short-lived sessions, the time taken for the SSL handshake can be more than the time for data transfer. To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a mechanism for caching sessions so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and the server. The cached information is identified by a session ID. In subsequent connections, both parties agree to use the session ID to retrieve the information rather than create a new pre-master secret key. Session resumption shortens the handshake process and accelerates SSL transactions.

### SSL Proxy Logs

When logging is enabled in an SSL proxy profile, the SSL proxy can generate the messages shown in [Table 182 on page 519](#).

**Table 182: SSL Proxy Logs**

Log Type	Description
SSL_PROXY_SSL_SESSION_DROP	Logs generated when a session is dropped by SSL proxy.
SSL_PROXY_SSL_SESSION_ALLOW	Logs generated when a session is processed by SSL proxy even after encountering some minor errors.
SSL_PROXY_SESSION_IGNORE	Logs generated if non-SSL sessions are initially mistaken as SSL sessions.
SSL_PROXY_SESSION_WHITELIST	Logs generated when a session is added to an allowlist.
SSL_PROXY_ERROR	Logs used for reporting errors.
SSL_PROXY_WARNING	Logs used for reporting warnings.
SSL_PROXY_INFO	Logs used for reporting general information.

All logs contain similar information; the message field contains the reason for the log generation. One of three prefixes shown in [Table 183 on page 520](#) identifies the source of the message. Other fields are descriptively labeled.

Table 183: SSL Proxy Log Prefixes

Prefix	Description
system	Logs generated because of errors related to the device or an action taken as part of the SSL proxy profile. Most logs fall into this category.
openssl error	Logs generated during the handshake process if an error is detected by the openssl library.
certificate error	Logs generated during the handshake process if an error is detected in the certificate (X.509 related errors).

## RELATED DOCUMENTATION

[About the SSL Proxy Policy Page | 520](#)

[About the SSL Proxy Profiles Page | 531](#)

[Certificates Overview | 265](#)

## About the SSL Proxy Policy Page

To access this page, select **Configuration > SSL Proxy > Policy** in Customer Portal.

Use the SSL Proxy Policy page to view and manage SSL proxy policy intents. You can also deploy the SSL proxy policy immediately or schedule the deployment for later.

### NOTE:

- When an SSL proxy intent is deployed, the corresponding certificates used in the SSL profile (associated with the SSL proxy intent) are automatically deployed to the applicable sites.
- If the application firewall (AppFW) service is not configured in the corresponding firewall policy intent, then the SSL forward proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy. Therefore, ensure that AppFW is configured for the firewall policy intents that should go through SSL inspection. If AppFW is not included in the policy intent, this does not cause an error; however, the SSL proxy action does not take place even though sessions are matched.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create SSL proxy policy intents—See [“Creating SSL Proxy Policy Intents” on page 522](#).
- Edit, clone, or delete SSL proxy policy intents—See [“Editing, Cloning, and Deleting SSL Proxy Policy Intents” on page 526](#).
- Search for SSL proxy policy intents by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Filter SSL proxy policy intents—Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. Depending on your selection, you can filter the policy intents based on source, destination, or both, or view the filtered results. The filtered results are displayed on the same page.
- Deploy the SSL proxy policy—See [“Deploying Policies” on page 548](#).

Field Descriptions

[Table 184 on page 521](#) describes the fields on SSL Proxy Policy page.

Table 184: SSL Proxy Policy Page Fields

Field	Description
Total Intents	Total number of policy intents in the SSL proxy policy.
Undeployed	Number of SSL proxy policy intents that have not yet been deployed.
For each SSL proxy policy intent, the following information is displayed in a grid:	
Source	Source endpoints to which an SSL proxy policy intent applies.
Destination	Destination endpoints to which an SSL proxy policy intent applies..
SSL Proxy Profile	Name of the SSL proxy profile associated with the policy intent.
Options	Name and description of the SSL proxy policy intent.

RELATED DOCUMENTATION

## Creating SSL Proxy Policy Intents

You can configure an SSL proxy policy intent inline on the SSL Proxy Policy page. An SSL proxy policy intent enables you to configure an SSL proxy between source and destination endpoints by associating the latter with an SSL proxy profile.

To create an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The SSL Proxy Policy page appears.

2. Click the add icon (+).

The options to create policy intents appear inline on the SSL Proxy Policy page.

3. Enter the policy intent information according to the guidelines provided in [Table 185 on page 523](#)

4. Click **Save**.

The SSL proxy policy intent is saved and a confirmation message is displayed.

**NOTE:** After the policy intent is created, you must deploy the policy to ensure that the changes take effect on the applicable sites. When an SSL proxy policy intent is created, the **Undeployed** field is incremented by one indicating that intents are pending deployment.



Table 185: Create SSL Proxy Policy Intent Settings

Setting	Guideline
Source	<p>A source endpoint can be an IP address, an IP address group, a site, a site group, or a department, or or a combination of these.</p> <p><b>NOTE:</b> A source IP address value of <b>Any</b> signifies any IP address from any site.</p> <p>Specify one or more source endpoints in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Click the add icon (+) and select the endpoints from the list of previously configured endpoints.</li> <li>• Filter the endpoints by entering a search term or one or more predefined keywords in the <b>Source</b> field and select one or more endpoints.</li> </ul> <p><a href="#">Table 186 on page 525</a> displays the list of predefined keywords.</p> <ul style="list-style-type: none"> <li>• Click the <b>View more results</b> link to view additional configured endpoints. The list of endpoints is displayed in the <b>End Points</b> panel on the right.</li> </ul> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint.</li> <li>• To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the <b>End Points</b> panel, and select <b>Source</b>.</li> <li>• Filter the endpoints by entering a search term or one or more predefined keywords in the <b>End Points</b> field and select one or more endpoints.</li> </ul> <p><a href="#">Table 186 on page 525</a> displays the list of predefined keywords.</p> <p><b>NOTE:</b> You can also create endpoints by clicking the add icon (+) in the End Points panel.</p> <p><a href="#">Table 187 on page 526</a> displays the endpoints that can be created.</p>

Table 185: Create SSL Proxy Policy Intent Settings (*continued*)

Setting	Guideline
<b>Destination</b>	<p>A destination endpoint can be an IP address, an IP address group, a site, a site group, or a department, or or a combination of these.</p> <p><b>NOTE:</b> A destination IP address value of <b>Any</b> signifies traffic going to the Internet (any address). Traffic within sites (internal traffic) is not covered by the destination IP address value of <b>Any</b>.</p> <p>If you want to cover traffic between two sites, ensure that the sites are included in both the source and destination endpoints.</p> <p>Specify one or more destination endpoints in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Click the add icon (+) and select the endpoints from the list of previously configured endpoints.</li> <li>• Filter the endpoints by entering a search term or one or more predefined keywords in the <b>Destination</b> field and select one or more endpoints.</li> </ul> <p><a href="#">Table 186 on page 525</a> displays the list of predefined keywords.</p> <ul style="list-style-type: none"> <li>• Click the <b>View more results</b> link to view additional configured endpoints. The list of endpoints is displayed in the <b>End Points</b> panel on the right.</li> </ul> <p>Do one of the following:</p> <ul style="list-style-type: none"> <li>• To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint.</li> <li>• To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the <b>End Points</b> panel, and select <b>Destination</b>.</li> <li>• Filter the endpoints by entering a search term or one or more predefined keywords in the <b>End Points</b> field and select one or more endpoints.</li> </ul> <p><a href="#">Table 186 on page 525</a> displays the list of predefined keywords.</p> <p><b>NOTE:</b> You can also create endpoints by clicking the add icon (+) in the End Points panel.</p> <p><a href="#">Table 187 on page 526</a> displays the endpoints that can be created.</p>

Table 185: Create SSL Proxy Policy Intent Settings (*continued*)

Setting	Guideline
<b>SSL Proxy Profile</b>	<p>Specify an SSL proxy profile to associate with the SSL proxy policy intent in one of the following ways:</p> <ul style="list-style-type: none"> <li>Click the add icon (+) and select the SSL proxy profile from the list of previously configured profiles.</li> <li>Filter the profiles by entering a search term in the <b>SSL Proxy Profile</b> field and select a profile.</li> <li>Create a SSL proxy profile—Click the <b>Add New Profile</b> link. The Create SSL Proxy Profiles page appears. See <a href="#">“Creating SSL Forward Proxy Profiles” on page 533</a>.</li> </ul> <p><b>NOTE:</b> You can also create profiles by clicking the add icon (+) in the End Points panel and selecting <b>SSL Proxy Profiles</b>.</p> <ul style="list-style-type: none"> <li>Click the <b>View more results</b> link to view additional configured profiles. The list of SSL proxy profiles is displayed in the <b>End Points</b> panel on the right.</li> </ul> <p>To add a profile, select it and click the check mark icon (✓) that appears when you hover over the profile.</p>
<b>Details</b>	<p>Enter the name of the SSL proxy policy intent in the first text box. If you do not enter a name, the system-generated name is used. The name that you enter must begin with an alphanumeric character and can contain alphanumeric characters and some special characters (- _). The maximum length is 63 characters.</p> <p>Enter the description of the SSL proxy policy intent in the second text box.</p>

Table 186: Keywords for Filtering Endpoints

Endpoint	Keyword	Applicable to
Address or Address Group	<b>addr</b> or <b>ADDR</b>	Source Destination
Site	<b>site</b> or <b>SITE</b>	Source Destination
Site Group	<b>stgp</b> or <b>STGP</b>	Source Destination
Department	<b>dept</b> or <b>DEPT</b>	Source Destination

Table 187: Creating Endpoints

Endpoint	Procedure
Address or Address Group	Click the add icon (+) and select <b>Address</b> . The Create Addresses page appears. See <a href="#">“Creating Addresses or Address Groups” on page 573</a> .
Site Group	Click the add icon (+) and select <b>Site Group</b> . The Create Site Group page appears. See <a href="#">“Creating Site Groups” on page 145</a> .
Department	Click the add icon (+) and select <b>Department</b> . The Create Department page appears. See <a href="#">“Adding a Department” on page 602</a> .

RELATED DOCUMENTATION

| [SSL Forward Proxy Overview](#) | [514](#)

## Editing, Cloning, and Deleting SSL Proxy Policy Intents

IN THIS SECTION

- [Editing SSL Proxy Policy Intents](#) | [527](#)
- [Cloning SSL Proxy Policy Intents](#) | [527](#)
- [Deleting SSL Proxy Policy Intents](#) | [528](#)

You can edit, clone, and delete SSL proxy policy intents from the SSL Proxy Policy page. This topic has the following sections:

## Editing SSL Proxy Policy Intents

To modify the parameters configured for an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The SSL Proxy Policy page appears, displaying the intents associated with the policy.

2. Hover over the SSL proxy policy intent that you want to edit, and then click the edit icon (pencil symbol) that appears on the right side of the intent.

You can now modify the policy intent inline on the SSL Proxy Policy page.

3. Modify the parameters following the guidelines provided in [“Creating SSL Proxy Policy Intents” on page 522](#).

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

The SSL proxy policy intent is saved and a confirmation message is displayed.

**NOTE:** After a policy intent is modified, you must redeploy the policy to ensure that the changes take effect on the relevant sites. When an SSL proxy policy intent is modified, the **Undeployed** field is incremented by one indicating that intents are pending deployment.

## Cloning SSL Proxy Policy Intents

Cloning enables you to easily create a new SSL proxy policy intent based on an existing one.

To clone an SSL proxy policy intent:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The **SSL Proxy Policy** page appears, displaying the intents associated with the policy.

2. Hover over the SSL proxy policy intent that you want to clone, and then click the clone icon that appears on the right side of the intent.

You can modify the cloned policy intent inline on the SSL Proxy Policy page.

3. Modify the parameters following the guidelines provided in [“Creating SSL Proxy Policy Intents” on page 522](#).

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

The SSL proxy policy intent is cloned and a confirmation message is displayed.

**NOTE:** After a policy intent is cloned, you must redeploy the policy to ensure that the changes take effect on the relevant sites. When an SSL proxy policy intent is cloned, the **Undeployed** field is incremented by one indicating that one or more intents are pending deployment.

## Deleting SSL Proxy Policy Intents

To delete one or more SSL proxy policy intents:

1. Select **Configuration > SSL Proxy > Policy** in Customer Portal.

The **SSL Proxy Policy** page appears, displaying the intents associated with the policy.

2. Select the SSL proxy policy intents that you want to delete and then click the delete icon (X).

You are asked to confirm the delete operation.

3. Click **Yes** to delete the selected SSL proxy policy intents.

A confirmation message appears indicating the status of the delete operation.

**NOTE:** After one or more policy intents are deleted, you must redeploy the policy to ensure that the changes take effect on the applicable sites.

## RELATED DOCUMENTATION

| [About the SSL Proxy Policy Page](#) | 520

# Understanding How SSL Proxy Policy Intents Are Applied

## IN THIS SECTION

- [Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match | 529](#)
- [Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match | 530](#)
- [Example 3: Applying SSL Proxy Policy Intents on Internal \(Site-to-Site\) Traffic | 530](#)

When you deploy an SSL proxy policy, SSL proxy profiles are deployed to the applicable sites based on SSL proxy policy intents. The deployments of firewall and SSL policies are related in that firewall policy deployments take into account the last-deployed SSL snapshots and vice versa. Therefore, even if an SSL proxy profile is deployed to the applicable sites, it is *applied* only to traffic to which the firewall policy intent applies.

The decision regarding *which* SSL proxy profile is attached to a firewall policy intent is based on matching criteria between SSL proxy policy and firewall policy intents. In addition, if there is a match between the SSL proxy policy intent and the firewall policy intent, the SSL profile is applied *only* to the policy intents that are common between the firewall and the SSL proxy policies.

The following examples demonstrate the matching logic between SSL proxy policy and firewall policy intents.

### Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match

[Table 188 on page 529](#) shows an example of a firewall policy intent and an SSL proxy policy intent that match, which means that the SSL proxy profile attaches to the firewall policy intent. In this case, the firewall policy intent has a source and destination of **Any** IP address, which signifies traffic from any IP address from any site to any IP address on the Internet. The SSL proxy policy intent has a source of **Any** IP address, which signifies any IP address *from* any site, and a destination IP address of 198.51.100.0.

Therefore, there is a match between the firewall policy intent and the SSL proxy policy intent and the SSL proxy profile is applied *only* to traffic from any IP address of any site to the IP address 198.51.100.0.

**Table 188: (Example) Match Between Firewall Policy Intent and SSL Proxy Policy Intent**

Type	Source	Destination	Action or Profile
Firewall policy intent	IP address—Any	IP address—Any	Allow
SSL proxy policy intent	IP address—Any	IP address—198.51.100.0	SSL-Profile-1

### Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match

Table 189 on page 530 shows an example of a firewall policy intent and an SSL proxy policy intent that do not match, which means that the SSL proxy profiles do not attach.

Although, at first glance, it *appears* that an SSL proxy policy intent with a source and destination IP address **Any** should match a firewall policy intent with a source IP address **Any** and destination department Finance, this is not the case because of what the IP address **Any** signifies in the destination.

For both firewall and SSL proxy policy intents:

- A source IP address value of **Any** signifies any IP address *from* any site.
- A destination IP address value of **Any** signifies traffic going *to* the Internet—that is, to any IP address on the Internet. Traffic *within* sites (internal traffic) is not covered by the destination IP address value of **Any**.

In this example, the firewall policy intent applies to traffic from any IP address (from any site) to the Finance department. However, the SSL proxy policy intent applies to traffic from any IP address (from any site) to any IP address on the Internet. This means that there is no match between the firewall policy intent and the SSL proxy policy intent and the SSL proxy profile does not attach.

**Table 189: (Example) No Match Between Firewall Policy Intent and SSL Proxy Policy Intent**

Type	Source	Destination	Action or Profile
Firewall policy intent	IP address—Any	Department—Finance	Allow
SSL proxy policy intent	IP address—Any	IP address—Any	SSL-Profile-2

### Example 3: Applying SSL Proxy Policy Intents on Internal (Site-to-Site) Traffic

**NOTE:** SSL forward proxy typically might not be used for site-to-site traffic, but this example is provided as an explanation of how an SSL proxy policy intent applies to site-to-site traffic.

Consider a scenario in which you have three sites (A, B, C) and you want to configure an SSL proxy for traffic between the sites. Table 190 on page 531 displays the firewall policy and SSL proxy policy intents that you can use for such a scenario.

Both the firewall policy intent and the SSL proxy policy intent use Site A, Site B, and Site C as the source and destination. Therefore, the firewall policy intent and the SSL proxy policy intent match, and the SSL proxy profile attaches to the firewall policy intent.



**NOTE:** The destination must be Site A, Site B, and Site C because the destination IP address **Any** signifies any IP address on the *Internet*.

**Table 190: (Example) Firewall Policy and SSL Proxy Policy Intents for Site-to-Site Traffic**

Type	Source	Destination	Action or Profile
Firewall Policy Intent	Site A, Site B, Site C	Site A, Site B, Site C	Allow
SSL Proxy Policy Intent	Site A, Site B, Site C	Site A, Site B, Site C	SSL-Profile-3

## RELATED DOCUMENTATION

[SSL Forward Proxy Overview | 514](#)

[Configuring and Deploying an SSL Forward Proxy Policy | 542](#)

## About the SSL Proxy Profiles Page

To access this page, click **Configuration > SSL Proxy > Profiles** in Customer Portal.

Use the SSL Proxy Profiles page to view and manage SSL proxy profiles.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create an SSL proxy profile—See [“Creating SSL Forward Proxy Profiles” on page 533](#).
- Edit, clone, or delete an SSL proxy profile—See [“Editing, Cloning, and Deleting SSL Forward Proxy Profiles” on page 539](#).
- View the details of an SSL proxy profile—Select the SSL proxy profile for which you want to view the details and from the More or right-click menu, select **Detailed View**. The View SSL Proxy Profile Details page appears. [Table 192 on page 532](#) describes the fields on this page.
- Search for SSL proxy profiles using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.

## Widget Descriptions

Table 191 on page 532 describes the fields on the SSL Proxy Profiles page.

Table 191: Fields on the SSL Proxy Profiles Page

Field	Description
<b>Name</b>	Name of the SSL proxy profile.
<b>Preferred Cipher</b>	Preferred cipher associated with the profile.
<b>Custom Ciphers</b>	The set of ciphers, if the preferred cipher is <b>Custom</b> , which the SSH server uses to perform encryption and decryption functions.
<b>Exempted Address</b>	Addresses that can are exempted from SSL forward proxy processing.
<b>Description</b>	Description of the SSL proxy profile.
<b>Root Certificate</b>	Root certificate associated with the SSL proxy profile.

Table 192: View SSL Forward Proxy Profile Details Page Fields

Field	Description
<b>General Information</b>	
<b>Name</b>	Name of the SSL proxy profile.
<b>Description</b>	Description of the SSL proxy profile.
<b>Preferred Cipher</b>	Preferred cipher associated with the proxy profile.
<b>Custom Ciphers</b>	The set of ciphers, if the preferred cipher is <b>Custom</b> , which the SSH server uses to perform encryption and decryption functions.
<b>Flow Trace Enabled</b>	Indicates whether flow tracing is enabled or disabled.
<b>Certificates</b>	Displays the root certificate and the trusted certificate authorities associated with the root certificate.
<b>Exempted Address</b>	Addresses that can are exempted from SSL forward proxy processing.
<b>Exempted URL Categories</b>	URL categories that are exempted from SSL forward proxy processing.
<b>Actions</b>	

Table 192: View SSL Forward Proxy Profile Details Page Fields (*continued*)

Field	Description
<b>Ignore</b>	Indicates whether server authentication failure is ignored ( <b>Enabled</b> ) or not ( <b>Disabled</b> ).
<b>Session Resumption</b>	Indicates whether session information is cached to enable session resumption ( <b>Enabled</b> ) or not ( <b>Disabled</b> ).
<b>Logging</b>	If logging is enabled, indicates the type of events that are logged.
<b>Renegotiation</b>	Indicates the type of renegotiation required if there is a change in SSL parameters after a session is created and SSL tunnel transport is established.

## RELATED DOCUMENTATION

[About the SSL Proxy Policy Page | 520](#)

## Creating SSL Forward Proxy Profiles

Use this page to configure SSL forward proxy profiles. SSL proxy is enabled as an application service within a security policy. You specify the traffic that you want the SSL proxy enabled on as match criteria and then specify the SSL proxy profile to be applied to the traffic.

To create an SSL forward proxy profile:

**NOTE:** Ensure that you have a root certificate imported for the tenant before you create an SSL forward proxy profile. You can import SSL certificates (root and trusted) from the Certificates page (**Administration > Certificates**) and associate the certificates with SSL forward proxy profiles.

1. Select **Configuration > SSL Proxy > Profiles** in Customer Portal.

The SSL Proxy Profiles page appears.

2. Click the add icon (+) to create an SSL forward proxy profile.

The Create SSL Proxy Profiles page appears.

3. Complete the configuration according to the guidelines provided in [Table 193 on page 534](#).

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

4. Click **OK**.

An SSL forward proxy profile is created. You are returned to the SSL Proxy Profiles page where a confirmation message is displayed.

The SSL forward proxy profile can be used in an SSL proxy policy intent (**Configuration > SSL Proxy > Policy**).

Table 193: Creating SSL Forward Proxy Profile Settings

Setting	Guideline
<b>General Information</b>	
<b>Name</b>	Enter a unique name for the profile, which is string of alphanumeric characters and some special characters (- _). No spaces are allowed and the maximum length is 63 characters.
<b>Description</b>	Enter a description for the profile. The maximum length is 255 characters.
<b>Preferred Cipher</b>	<p>Select a preferred cipher. Preferred ciphers enable you to define an SSL cipher that can be used with acceptable key strength. You can select from the following categories:</p> <ul style="list-style-type: none"><li>• <b>None</b> (Default)—Do not specify a preferred cipher.</li><li>• <b>Medium</b>—Use ciphers with key strength of 128 bits or greater.</li><li>• <b>Strong</b>—Use ciphers with key strength of 168 bits or greater.</li><li>• <b>Weak</b>—Use ciphers with key strength of 40 bits or greater.</li><li>• <b>Custom</b>—Configure a custom cipher suite.</li></ul>

Table 193: Creating SSL Forward Proxy Profile Settings (continued)

Setting	Guideline
Custom Ciphers	

Table 193: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
	<p>If you specified <b>Custom</b> as the preferred cipher, you can define a custom cipher list by selecting ciphers.</p> <p>Select the set of ciphers that the SSH server can use to perform encryption and decryption functions.</p> <p>The available custom ciphers are:</p> <ul style="list-style-type: none"> <li>• <code>rsa-with-RC4-128-md5</code>—RSA, 128-bit RC4, MD5 hash</li> <li>• <code>rsa-with-RC4-128-sha</code>—RSA, 128-bit RC4, SHA hash</li> <li>• <code>rsa-with-des-cbc-sha</code>—RSA, DES/CBC, SHA hash</li> <li>• <code>rsa-with-3DES-ede-cbc-sha</code>—RSA, 3DES EDE/CBC, SHA hash</li> <li>• <code>rsa-with-aes-128-cbc-sha</code>—RSA, 128-bit AES/CBC, SHA hash</li> <li>• <code>rsa-with-aes-256-cbc-sha</code>—RSA, 256 bit AES/CBC, SHA hash</li> <li>• <code>rsa-export-with-rc4-40-md5</code>—RSA-export, 40 bit RC4, MD5 hash</li> <li>• <code>rsa-export-with-des40-cbc-sha</code>—RSA-export, 40 bit DES/CBC, SHA hash</li> <li>• <code>rsa-export1024-with-des-cbc-sha</code>—RSA 1024 bit export, DES/CBC, SHA hash</li> <li>• <code>rsa-export1024-with-rc4-56-md5</code>—RSA 1024 bit export, 56 bit RC4, MD5 hash</li> <li>• <code>rsa-export1024-with-rc4-56-sha</code>—RSA 1024 bit export, 56 bit RC4, SHA hash</li> <li>• <code>rsa-with-aes-256-gcm-sha384</code>—RSA, 256 bit AES/GCM, SHA384 hash</li> <li>• <code>rsa-with-aes-256-cbc-sha256</code>—RSA, 256 bit AES/CBC, SHA256 hash</li> <li>• <code>rsa-with-aes-128-gcm-sha256</code>—RSA, 128 bit AES/GCM, SHA256 hash</li> <li>• <code>rsa-with-aes-128-cbc-sha256</code>—RSA, 256 bit AES/CBC, SHA256 hash</li> <li>• <code>ecdhe-rsa-with-aes-256-gcm-sha384</code>—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash</li> <li>• <code>ecdhe-rsa-with-aes-256-cbc-sha384</code>—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash</li> <li>• <code>ecdhe-rsa-with-aes-256-cbc-sha</code>—ECDHE, RSA, 256 bit AES/CBC, SHA hash</li> <li>• <code>ecdhe-rsa-with-aes-3des-ede-cbc-sha</code>—ECDHE, RSA, 3DES, EDE/CBC, SHA hash</li> <li>• <code>ecdhe-rsa-with-aes-128-gcm-sha256</code>—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash</li> <li>• <code>ecdhe-rsa-with-aes-128-cbc-sha256</code>—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash</li> <li>• <code>ecdhe-rsa-with-aes-128-cbc-sha</code>—ECDHE, RSA, 128 bit AES/CBC, SHA</li> </ul>

Table 193: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
	hash
<b>Flow Trace</b>	Select this option to enable flow tracing to enable the troubleshooting of policy-related issues.
<b>Root Certificate</b>	Select or add a root certificate. In a public key infrastructure (PKI) hierarchy, the root certificate authority (CA) is at the top of the trust path.
<b>Trusted Certificate Authorities</b>	<p>Choose whether you want to add all trusted certificates present on the device (<b>All</b>) or select specific trusted certificates. Before establishing a secure connection, the SSL proxy checks CA certificates to verify signatures on server certificates.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• Specifying that all trusted certificates should be used means that all trusted certificates on a particular device (site) will be used during SSL policy deployment.</li> <li>• If you specify that all trusted certificates should be used in an SSL forward proxy profile, you must ensure that at least one trusted certificate is installed on the device.</li> </ul>
<b>Actions</b>	

Table 193: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
Exempted Addresses	<p>Exempted addresses include addresses that you want to exempt from undergoing SSL proxy processing.</p> <p>To specify exempted addressees, select one or more addresses in the <b>Available</b> column and click the forward arrow to confirm your selection. The selected addresses are then displayed in the <b>Selected</b> column. These addresses are used to create allowlists that bypass SSL forward proxy processing.</p> <p>Because SSL encryption and decryption are complicated and expensive procedures, network administrators can selectively bypass SSL proxy processing for some sessions.</p> <p>Such sessions typically include connections and transactions with trusted servers or domains with which network administrators are very familiar. There are also legal requirements to exempt financial and banking sites. Such exemptions are achieved by configuring the IP addresses or domain names of the servers under allowlists.</p> <p><b>NOTE:</b> You can also add addresses by clicking <b>Add New Address</b>. The Create Addresses page appears. See <a href="#">“Creating Addresses or Address Groups” on page 573</a>.</p>
Exempted URL Categories	<p>Select the previously defined URL categories to create allowlists that bypass SSL forward proxy processing. The selected URL categories are exempted during SSL inspection.</p>
Server Auth Failure	<p>Select this check box to ignore errors encountered during the server certificate verification process (such as CA signature verification failure, self-signed certificates, and certificate expiry). This check box is cleared by default.</p> <p>We do not recommend this option for authentication, because configuring it results in websites not being authenticated at all. However, you can use this option to effectively identify the root cause for dropped SSL sessions.</p>
Session Resumption	<p>Select this check box to disable session resumption. This check box is cleared by default.</p> <p>To improve throughput and still maintain an appropriate level of security, SSL session resumption provides a session-caching mechanism so that session information, such as the pre-master secret key and agreed-upon ciphers, can be cached for both the client and server.</p>



Table 193: Creating SSL Forward Proxy Profile Settings (*continued*)

Setting	Guideline
<b>Logging</b>	Select one or more events to be logged. You can choose to log all events, warnings, general information, errors, or different sessions (allowlisted, allowed, dropped, or ignored). Logging is disabled by default.
<b>Renegotiation</b>	<p>Select one of the following options if a change in SSL parameters requires renegotiation:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)—Indicates that renegotiation is not required.</li> <li>• <b>Allow</b>—Allow secure and nonsecure renegotiation.</li> <li>• <b>Allow-secure</b>—Allow secure negotiation only.</li> <li>• <b>Drop</b>—Drop session on renegotiation request.</li> </ul> <p>After a session is created and SSL tunnel transport has been established, a change in SSL parameters requires renegotiation. SSL forward proxy supports both secure (RFC 5746) and nonsecure (TLS v1.0 and SSL v3) renegotiation.</p> <p>When session resumption is enabled, session renegotiation is useful in the following situations:</p> <ul style="list-style-type: none"> <li>• Cipher keys need to be refreshed after a prolonged SSL session.</li> <li>• Stronger ciphers need to be applied for a more secure connection.</li> </ul>

## RELATED DOCUMENTATION

| [About the SSL Proxy Policy Page](#) | 520

## Editing, Cloning, and Deleting SSL Forward Proxy Profiles

### IN THIS SECTION

- [Editing SSL Forward Proxy Profiles](#) | 540
- [Cloning SSL Forward Proxy Profiles](#) | 540
- [Deleting SSL Forward Proxy Profiles](#) | 541

You can edit, clone, and delete SSL forward proxy profiles from the SSL Proxy Profiles page. This topic has the following sections:

## Editing SSL Forward Proxy Profiles

To modify the parameters configured for an SSL forward proxy profile:

**NOTE:** If an SSL forward proxy profile is already used in an SSL proxy policy intent, we recommend that you do not modify the profile name. If you want to create a profile with a new name, clone the existing profile and modify the name.

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears, displaying the existing SSL forward proxy profiles.

2. Select the SSL forward proxy profile that you want to edit and click the edit icon (pencil). Alternatively, right-click a profile and select **Edit Profile**.

The Edit SSL Proxy Profile page appears showing the same fields that are presented when you create an SSL forward proxy profile.

3. Modify the SSL forward proxy profile fields as needed.

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

You are taken to the SSL Proxy Profiles page. A confirmation message appears, indicating the status of the edit operation.

**NOTE:** If an SSL forward proxy profile that is associated with an SSL proxy policy intent is modified, you must redeploy the SSL proxy policy to ensure that the changes take effect on the site.

## Cloning SSL Forward Proxy Profiles

Cloning enables you to easily create a new SSL forward proxy profile based on an existing one.

To clone an SSL forward proxy profile:

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears displaying the existing SSL forward proxy profiles.

2. Select the SSL forward proxy profile that you want to clone and select **More > Clone**. Alternatively, right-click a profile and select **Clone**.

The Clone SSL Proxy Profile page appears, showing the same fields that are presented when you create an SSL forward proxy profile.

3. Modify the SSL forward proxy profile fields as needed.

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

You are taken to the SSL Proxy Profiles page. A confirmation message appears, indicating the status of the clone operation.

## Deleting SSL Forward Proxy Profiles

To delete one or more SSL forward proxy profiles:

**NOTE:** If you try to delete an SSL forward proxy profile that is associated with an SSL proxy policy intent, a message is displayed indicating that the profile cannot be deleted.

1. Select **Configuration > SSL Proxy > Profiles**.

The SSL Proxy Profiles page appears, displaying the existing SSL forward proxy profiles.

2. Select one or more SSL forward proxy profiles that you want to delete and click the delete icon (X). Alternatively, right-click a profile and select **Delete SSL Proxy Profile**.

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

3. Click **Yes** to delete the selected SSL forward proxy profiles.

A confirmation message appears indicating the status of the delete operation.

**NOTE:** If the deleted SSL forward proxy profile is associated with an SSL proxy policy intent, you must redeploy the SSL proxy policy to ensure that the changes take effect on the site.

## RELATED DOCUMENTATION

[Creating SSL Forward Proxy Profiles | 533](#)[About the SSL Proxy Profiles Page | 531](#)

## Configuring and Deploying an SSL Forward Proxy Policy

The following is the workflow for configuring and deploying an intent-based SSL forward proxy policy in CSO:

1. Obtain the root certificate and private key from your trusted certificate authority (CA).
2. Combine the root certificate and private key into a single file.
3. Import the certificate and private key file (on the Import Certificate page); see [“Importing a Certificate” on page 268](#).
4. (Optional) Install the imported certificate on one or more sites (on the Install Certificate page); see [“Installing and Uninstalling Certificates” on page 270](#).
5. By default, Juniper Networks ships trusted certificates for sites that use HTTPS. These certificates are installed automatically by CSO when the site is successfully provisioned.  
  
If you want to use additional trusted certificates, import and install the certificates as explained in [Step 3](#) and [4](#).

6. Create an SSL proxy profile (on the Create SSL Proxy Profiles) page; see [“Creating SSL Forward Proxy Profiles” on page 533](#).

**NOTE:**

- Use the imported root certificate when you create the SSL proxy profile.
- For trusted certificates, specify that all trusted certificates on the device are used (select **All** in the **Trusted Certificate Authorities** field).

7. Create an SSL proxy policy intent that uses the SSL proxy profile that you created (on the SSL Proxy Policy page); see [“Creating SSL Proxy Policy Intents” on page 522](#).
8. Deploy the SSL proxy policy; see [“Deploying Policies” on page 548](#).

**NOTE:**

- Ensure that the root and trusted certificates are imported into CSO before the policy is deployed.
- If you have not installed the certificates referenced in the SSL proxy profile, then they are automatically installed when the SSL proxy policy is deployed.

9. For Internet access from an SRX Series device by using the SSL proxy, ensure that you import the root certificate (obtained in Step 1) into the browsers of the clients accessing the Internet.

**NOTE:** If you do not import the certificate, the traffic does not go through for clients in the LAN segments.

**RELATED DOCUMENTATION**

[SSL Forward Proxy Overview | 514](#)

[Understanding How SSL Proxy Policy Intents Are Applied | 529](#)

# Deploying Policies

## IN THIS CHAPTER

- [Deploying Policies Overview | 544](#)
- [About the Deployments Page | 545](#)
- [Using the Deployment Icon to Deploy Policies | 547](#)
- [Deploying Policies | 548](#)

## Deploying Policies Overview

When you finish creating and verifying your security configurations, you can deploy these configurations and keep them ready to be pushed to the security devices. CSO enables you to push security configurations to the devices all at once by providing a single interface that is intuitive.

The deployment workflow provides the ability to save and publish different services to be updated at a later time to the appropriate firewalls (during downtime). This enables administrators to review their firewall and NAT policies before updating the device. Administrators also save troubleshooting time, avoid errors, and save costs associated with errors. Verify and tweak your security configurations before updating them to the device. This approach helps you keep the configurations ready and update these configurations to the devices during the maintenance window.

When you deploy policies, the process takes into account the priority and precedence values set on the policy and the order of rules on the device. Rules are published in the order of their priority groups.

If you change the priority or precedence of a published policy, the policy must be republished for the changes to take effect. Sometimes, changing priority or precedence in one policy can affect other policies in the same priority group. However, such dependent policies do not need to be republished in order for their changes in priority or precedence to take effect. It will be enough if the policy which is updated is republished.

There are three ways in which you can view and deploy your security configurations:

- Click on the deployment icon present in the CSO Customer Portal banner and use the deployment panel that appears, to deploy policies. See [“Using the Deployment Icon to Deploy Policies” on page 547](#).

**NOTE:** The deployment icon is highlighted in orange if there are undeployed configurations.

- Use the **Deployments** page. See [“About the Deployments Page” on page 545](#).
- Select a firewall, NAT or SD-WAN policy from its respective landing pages and click **Deploy**. For more information, see [“Deploying Policies” on page 548](#).

RELATED DOCUMENTATION

[Using the Deployment Icon to Deploy Policies | 547](#)

[About the Deployments Page | 545](#)

[Deploying Policies | 548](#)

# About the Deployments Page

To access this page, click **Configuration > Deployments**.

Use this page to deploy or schedule the deployment of undeployed SD-WAN, NAT, and firewall policies. Undeployed policies refer to newly created firewall policy rules or NAT policies. These changes do not come into effect until the policies are deployed. The **Deploy** page provides scheduling options for you to deploy these policies.

## Tasks You Can Perform

You can perform the following task from this page:

- Deploy a policy. See [“Deploying Policies” on page 548](#).

## Field Descriptions

[Table 194 on page 546](#) provides guidelines on using the fields on the **Deployments** page.

Table 194: Fields on the Deployments Page

Field	Description
Awaiting Deployment	<p>The <b>Awaiting Deployment</b> tab displays all the policies that are awaiting deployment. The following fields provide more information about the undeployed policies:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the policy that needs to be deployed.</li> <li>• <b>Deployment Type</b>—Type of the policy that needs to be deployed.</li> <li>• <b>Summary</b>—Description of the policy.</li> <li>• <b>Owner</b>—The tenant who has created the policy.</li> <li>• <b>Last updated</b>—The last time the policy was updated.</li> </ul> <p>If you want to deploy a policy, select the policy and click <b>Deploy</b>. The policy is deployed and will no longer appear in the <b>Awaiting Deployment</b> tab.</p> <p>If you want to refresh the <b>Awaiting Deployment</b> tab, click the refresh icon provided below the details table.</p>
Scheduled	<p>The <b>Scheduled</b> tab displays all the policies that have been scheduled for deployment on a certain date and time. The following fields provide more information about scheduled policies:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the policy.</li> <li>• <b>Deployment Type</b>—Type of the policy that needs to be deployed.</li> <li>• <b>Summary</b>—Description of the policy.</li> <li>• <b>Schedule</b>—The date and time at which the policy is scheduled to be deployed.</li> <li>• <b>Status</b>—Displays whether the scheduled policy has been deployed or not.</li> <li>• <b>Next Run</b>—Date and time when the scheduled deployments will be run.</li> </ul> <p>If you want to deploy a scheduled policy immediately, select the policy and click <b>Deploy Now</b>. If you want to modify the deployment schedule of a policy, select the policy and click the edit icon (pencil icon). The <b>Deploy</b> page appears displaying the current scheduling information. See <a href="#">“Deploying Policies” on page 548</a>, to update the schedule.</p>
History	<p>The <b>History</b> tab displays all the policies that have been deployed. The following fields provide more information about deployed policies:</p> <ul style="list-style-type: none"> <li>• <b>Name</b>—Name of the deployed policy.</li> <li>• <b>Deployment Type</b>—Type of the deployed policy.</li> <li>• <b>Summary</b>—Description of the policy.</li> <li>• <b>Status</b>—Displays the status of the deployed policy.</li> <li>• <b>Job Details</b>—Details of the job.</li> <li>• <b>Deployed On</b>—Date and time the policy was deployed.</li> </ul> <p>If you want to redeploy a policy, select the policy and click <b>Re-Deploy</b>. The policy is redeployed and the <b>History</b> tab details changes to reflect this information.</p>



RELATED DOCUMENTATION

<a href="#">Deploying Policies Overview   544</a>
<a href="#">Using the Deployment Icon to Deploy Policies   547</a>
<a href="#">Deploying Policies   548</a>

## Using the Deployment Icon to Deploy Policies

CSO provides an option of viewing and deploying policies through the deployment panel, that appears when you click on the deployment icon. The deployment icon is highlighted in orange if there are undeployed policies.

To deploy policies through the deployment panel:

1. Click the deployment icon on the Customer Portal banner.  
The deployment panel appears. For information about the panel, see [Table 195 on page 547](#).
2. Hover over the policy you want to deploy. The **Deploy** option appears on the right side of the policy.
3. Click **Deploy** to deploy the policy. For more information, see [“Deploying Policies” on page 548](#).

[Table 195 on page 547](#) provides guidelines on using the fields on the deployment panel.

Table 195: Fields on the Deployment Panel

Field	Description
Awaiting Deployment	The <b>Awaiting Deployment</b> tab displays all the policies that are awaiting deployment.
In Progress	The <b>In Progress</b> tab displays all the policies that are currently being deployed.

RELATED DOCUMENTATION

<a href="#">Deploying Policies Overview   544</a>
<a href="#">About the Deployments Page   545</a>
<a href="#">Deploying Policies   548</a>

## Deploying Policies

You can deploy firewall, NAT, SD-WAN, and SSL proxy policies added by various services immediately or schedule the deployment for a later date and time.

To configure a deployment:

1. You can initiate the deployment of a policy in the following ways:
  - Select a policy from the **Awaiting Deployment** tab on the **Deployments** page and click **Deploy**.
  - Select a policy from the **Scheduled** tab on the **Deployments** page and click **Deploy**.
  - Select a policy from the **Scheduled** tab on the **History** page and click **Re-Deploy**.
  - Use the deployment icon on the Customer Portal banner. For more information about deploying policies using the deployment icon, see [“Using the Deployment Icon to Deploy Policies” on page 547](#).

**NOTE:** The deployment icon is highlighted in orange if there are undeployed policies.

- Select **Configuration > Firewall > Firewall Policy**. The **Firewall Policy** page appears, displaying the intents associated with the policy. Click **Deploy**.
  - Select **Configuration > NAT > NAT Policies** and select the NAT policy you want to deploy. Click **Deploy**.
  - Select **Configuration > SSL Proxy > Policy**. The **SSL Proxy Policy** page appears, displaying the intents associated with the policy. Click **Deploy**.
  - Select an SD-WAN policy intent on the **SD-WAN Policy** page and click **Deploy**.
2. The **Deploy** page appears. In **Choose Deployment Time** options, select **Run Now** to deploy the policy immediately.  
  
Select **Schedule at a later time** to deploy the policy at a later date and time. For scheduling options, see [Table 196 on page 548](#).

3. Click **Deploy**.

[Table 196 on page 548](#) provides guidelines on using the fields on the **Deploy** page.

Table 196: Fields on the Deploy Page

Field	Description
<b>Summary</b>	
Policies	The summary of the policy that is to be deployed.

Table 196: Fields on the Deploy Page *(continued)*

Field	Description
<b>Choose Deployment Time</b>	
Type	<ul style="list-style-type: none"><li>• Select <b>Run now</b> if you want to deploy the policy immediately.</li><li>• Select <b>Schedule at a later time</b> if you want to schedule the deployment for a later date and time.<ul style="list-style-type: none"><li>• Click on the calendar icon to choose the date for the deployment in MM/DD/YYYY format.</li><li>• Enter the time for the deployment in HH:MM:SS format. 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.</li></ul></li></ul>

RELATED DOCUMENTATION

<a href="#">Deploying Policies Overview   544</a>
<a href="#">Using the Deployment Icon to Deploy Policies   547</a>
<a href="#">About the Deployments Page   545</a>

# 5

PART

## Managing Network Services and Shared Objects

---

Configuring Network Services in a Distributed Deployment | **551**

Managing Shared Objects | **570**

---

# Configuring Network Services in a Distributed Deployment

## IN THIS CHAPTER

- [Network Service Overview | 551](#)
- [About the Network Services Page | 552](#)
- [About the Service Overview Page | 554](#)
- [About the Service Instances Page | 556](#)
- [Configuring VNF Properties | 558](#)
- [vSRX VNF Configuration Settings | 558](#)
- [LxCIPtable VNF Configuration Settings | 564](#)
- [Cisco CSR-1000v VNF Configuration Settings | 566](#)
- [Riverbed Steelhead VNF Configuration Settings | 568](#)

## Network Service 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   552
About the Service Overview Page   554
About the Service Instances Page   556

## About the Network Services Page

To access this page, click **Configuration > Network Services**.

You can use the Network 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 Service Overview” on page 551](#).

### Tasks You Can Perform

You can perform the following tasks from this page:

- Quickly view important data about network services and about instances of those services deployed at customers’ sites in the widgets that appear at the top of the page. See [Table 197 on page 552](#).
- 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 556](#).

### Field Descriptions

[Table 197 on page 552](#) shows the descriptions of the widgets that appear at the top of the Network Services page.

Table 197: Widgets on the Network Services Page

Widget	Description
Top Network Services Instantiated	View the numbers of instances of the three services that are most used by tenants in the network.  This view helps you identify trends for network services, especially when you introduce a new service.
Services with Critical Alerts	View the top three network services receiving the maximum number of critical alerts.

Table 197: Widgets on the Network Services Page (*continued*)

Widget	Description
Top Services by POP CPU Usage	View the top three network services using the largest percentage of CPU from the assigned CPU cores.

Table 198 on page 553 shows the descriptions of the fields on the Network Services page.

Table 198: Fields on the Network Services Page

Field	Description
Name	View the name of the service.  Click the name to view full information about a service.
Tenants	View the names of the tenants that have access to the network service.
Sites	View the total number of sites at which the service is deployed for the tenant.  Example: 2
Instances	View the total number of occurrences of the service that administrative users have activated for the tenant.  Example: 1
Last Update	View the date on which the network service designer last modified the service.

Table 199 on page 553 shows the descriptions of the fields on the Detail for *network service name* page.

Table 199: Fields on the Network Service Detail Page

Field	Description
<i>General</i>	
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.  Example: 1.1
State	View the status of the network service.  Example: Published

Table 199: Fields on the Network Service Detail Page *(continued)*

Field	Description
Performance Goals	View performance parameters of the network service that include bandwidth, number of sessions, latency, and license cost.

## RELATED DOCUMENTATION

[Network Service Overview | 551](#)

[About the Service Overview Page | 554](#)

[About the Service Instances Page | 556](#)

## About the Service Overview Page

To access this page, click **Service > 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 200 on page 555](#).
- View resources required for the service and its performance specification. See *Service Requirements* and *Service Performance* in [Table 200 on page 555](#).
- View the service chain, with its constituent VNFs. See *Service Configuration* in [Table 200 on page 555](#).
- Configure VNFs. Click a VNF in the service chain graphic. See [“vSRX VNF Configuration Settings” on page 558](#).

### Field Descriptions

[Table 200 on page 555](#) provides guidelines on using the fields on the Service Overview page.



Table 200: Fields on the Service Overview Page

Field	Description
<i>General Information</i>	
Description	View a summary about the service's capabilities.  The network service designer provides this summary.
State	View the state of the network service: <ul style="list-style-type: none"> <li>• Discontinued—Service is no longer available for customers.</li> <li>• Published—Service designer has published service to network catalog, and it is available for customers.</li> </ul>
Tenants	View the number of tenants using this service.
<i>Service Requirements</i>	
CPU	View the number of CPUs that the service needs (cores).
Memory	View the amount of RAM that the service needs in gigabytes (GB).
<i>Service Performance</i>	
Sessions	View the number of sessions concurrently supported by one instance of the service.
Bandwidth	View the data rate for the service in megabytes per second (Mbps) or gigabytes per second (Gbps).
Latency	View the time a packet takes to traverse the service in milliseconds (ms) or nanoseconds (ns).
License cost	Specify the license cost for the network service in USD.
<i>Service Configuration (graphic of the service chain)</i>	
I	View the ingress point—the point at which packets enter the service.
E	View the egress point—the point at which packets exit the service.

Table 200: Fields on the Service Overview Page (continued)

Field	Description
One or more VNFs	<p>Click to view settings for the VNF. See <a href="#">“vSRX VNF Configuration Settings” on page 558</a>.</p> <p>The service designer can configure the VNF settings in Network Service Designer and the administrative user can configure the VNF settings in Customer Portal.</p> <p><b>BEST PRACTICE:</b> The network service designer configures settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and the administrative user configures settings for the service, such as policies. The service designer can also configure a few example settings for the service. These example settings should be generic and not network-specific.</p>

## RELATED DOCUMENTATION

[Network Service Overview | 551](#)

[About the Network Services Page | 552](#)

[About the Service Instances Page | 556](#)

## About the Service Instances Page

To access this page, click **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 202 on page 557](#).
- 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 558](#).

## Field Descriptions

Table 201 on page 557 shows the descriptions of the fields on the Service Instances page.

**Table 201: Fields on the Service Instances Page**

Field	Description
Name	View the name of the occurrence of a service at a specific tenant site.
Tenant	View the name of the tenant.
Status	View the state of the service at the customer site: <ul style="list-style-type: none"> <li>Created—Administrative user for the tenant has enabled this service instance, which is active.</li> <li>Blank—Administrative user for the tenant has disabled this service instance.</li> </ul>
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 202 on page 557 shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

**Table 202: Fields on the Service Instance Details Page**

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

## RELATED DOCUMENTATION

[Network Service Overview | 551](#)

[About the Network Services Page | 552](#)

[About the Service Overview Page | 554](#)

## 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 **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](#) | 556

## vSRX VNF Configuration Settings

You can configure the vSRX VNF from **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.

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

- [Table 203 on page 559](#) 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 204 on page 561](#) shows the firewall settings you can configure.

**Table 203: Fields for the vSRX Base Settings**

Field	Description
Host Name	<p>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.</p> <p>Example: vm-vsrx</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
Loopback Address	<p>Specify an IPv4 loopback address for the management interface of the VM.</p> <p>Example: 192.0.2.25</p>
DNS Servers	<p>Specify the fully qualified domain names (FQDNs) or IP addresses of one or more DNS name servers.</p> <p>Example: 192.0.2.35</p>
NTP Servers	<p>Specify the FQDNs or IP addresses of one or more NTP servers.</p> <p>Example: 192.0.2.45</p>
Syslog Servers	<p>Specify the FQDNs or IP addresses of one or more system log servers.</p> <p>Example: 192.0.2.55</p>

Table 203: Fields for the vSRX Base Settings (*continued*)

Field	Description
Enable Re-filter	<p>Select <b>True</b> to enable a stateless firewall filter that protects the Routing Engine from denial-of-service (DoS) attacks or <b>False</b> to allow DoS attacks.</p> <p>Example: True</p>
Enable Default Screens	<p>For a cloud site, select <b>True</b> to enable the default screens security profile for the destination zone or <b>False</b> to disable default screening.</p> <p>Example: False</p> <p>You cannot configure this setting for an on-premise site.</p>
Time Zone	<p>Specify the time zone for the VM.</p> <p>Example: UTC</p>
Right Interface	<p>Specify the identifier of the VM interface that transmits data.</p> <p>Example: ge-0/0/1</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
Left Interface	<p>Specify the identifier of the VM interface that receives data.</p> <p>Example: ge-0/0/0</p> <p>For an on-premise site, the vSRX application resides on the CPE device, and you cannot configure this setting.</p>
SNMP Prefix List	<p>If you set the Enable Re-filter field to <b>True</b>, specify the routes that the Junos Space Virtual Appliance uses for SNMP operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.0/24</p>
Ping Prefix List	<p>If you set the Enable Re-filter field to <b>True</b>, specify the routes that the Junos Space Virtual Appliance uses for ping operations when it discovers the vSRX VNF.</p> <p>Example: 10.0.2.1/24</p>
Space Servers	<p>If you set the Enable Re-filter field to <b>True</b>, specify the IP addresses of the VMs that contain the Junos Space Virtual Appliances.</p> <p>Example: 10.0.2.50</p>

Table 204: Fields for the vSRX Firewall Settings

Field	Description
Policy Name	<p>Specify the name of the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols.</p> <p>Example: policy-1</p>
Source Zone	<p>Select the security zone from which packets originate.</p> <ul style="list-style-type: none"> <li>• <b>left</b>—Interface that transmits data to the host</li> <li>• <b>right</b>—Interface that receives data transmitted from the host</li> </ul> <p>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 <i>context</i>.</p> <p>Example: left</p>
Destination Zone	<p>Select the security zone to which packets are delivered.</p> <ul style="list-style-type: none"> <li>• <b>left</b>—Interface that transmits data to the host</li> <li>• <b>right</b>—Interface that receives data transmitted from the host</li> </ul> <p>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 <i>context</i>.</p> <p>Example: right</p>
Source Address	<p>Specify the source IP address prefixes that the network service uses as match criteria for incoming traffic.</p> <p>To add source addresses:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Source Address</b> column. The source-address page appears.</li> <li>2. Select <b>any</b> to match any source IP address of packets or <b>ipp</b> to match a specific prefix in the source IP address for which the application enforces the policy.</li> <li>3. If you select <b>ipp</b>, specify a prefix.</li> <li>4. Click <b>OK</b>.</li> </ol> <p>Example: 10.0.2.30</p>

Table 204: Fields for the vSRX Firewall Settings (continued)

Field	Description
Destination Address	<p>Specify the destination IP address prefixes that the network service uses as match criteria for outgoing traffic.</p> <p>To add a destination address:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Destination Address</b> column. The destination-address page appears.</li> <li>2. Select <b>any</b> to match any source IP address of packets or <b>ipp</b> to match a specific prefix in the source IP address for which the application enforces the policy.</li> <li>3. If you select <b>ipp</b>, specify a prefix.</li> <li>4. Click <b>OK</b>.</li> </ol> <p>Example: 192.0.2.0/24</p>
Action	<p>Select <b>permit</b> to transmit packets that match the rule or <b>deny</b> to drop packets that match the rule.</p> <p>Example: permit</p>



Table 204: Fields for the vSRX Firewall Settings (continued)

Field	Description
Application	<p>Specify the applications to which the policy applies. The applications are based on protocols and ports.</p> <p>To specify applications:</p> <ol style="list-style-type: none"><li>Click the <b>Application</b> column. The application page appears.</li><li>In the allowed_apps field, select <b>any</b> to match any application or <b>app</b> to choose specific applications. If you select <b>app</b>, press and hold the Ctrl key and click the required applications from the drop-down list.<ul style="list-style-type: none"><li>junos-tcp-any</li><li>junos-udp-any</li><li>junos-ftp</li><li>junos-http</li><li>junos-https</li><li>junos-icmp-all</li><li>junos-icmp-ping</li><li>junos-telnet</li><li>junos-tftp</li></ul></li><li>Click <b>OK</b>.</li></ol> <p>Example:</p> <ul style="list-style-type: none"><li>junos-tcp-any</li><li>junos-udp-any</li></ul>

RELATED DOCUMENTATION

<a href="#">About the Network Services Page   552</a>
<a href="#">About the Service Overview Page   554</a>
<a href="#">About the Service Instances Page   556</a>
<a href="#">Configuring VNF Properties   558</a>

## LxCIPtable VNF Configuration Settings

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 205 on page 564](#) 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 206 on page 564](#) shows the firewall settings you can configure.
- [Table 207 on page 566](#) shows the Network Address Translation (NAT) settings you can configure.

**Table 205: Fields for the LxCIP Base Settings**

Field	Description
Loopback Address	Specify a loopback IP address.  Example: 192.0.2.10
Operation	Select <b>add</b> to apply the policies to a specific route or <b>del</b> 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
Next Hop	Specify the IP address of a Contrail gateway network to which the VM connects.  Example: 192.0.2.20

**Table 206: Fields for the LxCIP Firewall Policy Settings**

Field	Description
<i>Firewall Policies</i>	
Prevent SSH Brute	Select <b>True</b> to prevent SSH brute attacks or <b>False</b> to allow SSH brute attacks.  Example: False

Table 206: Fields for the LxCIP Firewall Policy Settings (*continued*)

Field	Description
Prevent Ping Flood	<p>Select <b>True</b> to prevent ping flood attacks or <b>False</b> to allow ping flood attacks.</p> <p>Example: False</p>
<i>Forwarding Rule Settings</i>	
Destination Address	<p>Specify the destination IP address prefix that the network service uses as a match criterion for outgoing traffic.</p> <p>Example: 192.0.2.25/24</p>
Operation	<p>Select the operation, which applies to a chain of rules of the same type, from the drop-down list. The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>append</b>—Append the rule to a rule chain.</li> <li>• <b>insert-before</b>—Insert the rule before a rule with the same name.</li> <li>• <b>delete</b>—Replace an existing rule with this name.</li> </ul> <p>Example: append</p>
Source Address	<p>Specify the source IP address prefix that the network service uses as a match criterion for outgoing traffic.</p> <p>Example: 192.0.2.20/24</p>
Name	<p>Specify the name for the rule. The field has no limit on the number of characters and accepts letters, numbers, and symbols.</p> <p>Example: vsrx-fw-policy</p>
Action	<p>Select the action for the rule, which applies to all traffic that matches the specified criteria.</p> <ul style="list-style-type: none"> <li>• <b>accept</b>—Transmit packets that match the policy parameters.</li> <li>• <b>drop</b>—Drop packets that match the policy parameters.</li> <li>• <b>reject</b>—Reject packets that match the policy parameters.</li> </ul> <p>Example: accept</p>
Service	<p>Specify the service that you want the rule to match.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• http</li> <li>• smtp</li> </ul>

Table 206: Fields for the LxCIP Firewall Policy Settings (*continued*)

Field	Description
Type	<p>Select the type of packet that the rule matches.</p> <ul style="list-style-type: none"> <li>• <b>input</b>—Packets that the network service receives that are addressed to this VM</li> <li>• <b>forward</b>—Packets that the network service receives that are addressed to other VMs</li> <li>• <b>output</b>—Packets that the network service transmits</li> </ul> <p>The application creates a chain of all rules with a particular type.</p> <p>Example: input</p>

Table 207: Fields for the LxCIP NAT Policy Settings

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

## RELATED DOCUMENTATION

| [Managing a Single Site](#) | 139

## Cisco CSR-1000v VNF Configuration Settings

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 208 on page 567](#) 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 209 on page 567](#) shows the firewall settings you can configure.

**Table 208: 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 209: 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 209: Fields for the CSR-1000v Firewall Settings (*continued*)

Field	Description
Left to Right Allowed Apps	<p>Select the applications from the drop-down list for which the policy is enforced in outgoing packets. The following applications are available:</p> <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> <li>• telnet</li> <li>• ftp</li> <li>• tcp</li> <li>• udp</li> <li>• icmp</li> </ul> <p>Example: http, https</p>
Right to Left Allowed Apps	<p>Select the application from the drop-down list for which the policy is enforced for incoming packets. The following applications are available:</p> <ul style="list-style-type: none"> <li>• http</li> <li>• https</li> <li>• telnet</li> <li>• ftp</li> <li>• tcp</li> <li>• udp</li> <li>• icmp</li> </ul> <p>Example: ftp, udp</p>

## RELATED DOCUMENTATION

[Managing a Single Site](#) | 139

## 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

| [Managing a Single Site](#) | 139

# Managing Shared Objects

## IN THIS CHAPTER

- [Addresses and Address Groups Overview | 571](#)
- [About the Addresses Page | 571](#)
- [Creating Addresses or Address Groups | 573](#)
- [Editing, Cloning, and Deleting Addresses and Address Groups | 575](#)
- [Services and Service Groups Overview | 577](#)
- [About the Services Page | 578](#)
- [Creating Services and Service Groups | 579](#)
- [Creating Protocols | 581](#)
- [Editing and Deleting Protocols | 584](#)
- [Editing, Cloning, and Deleting Services and Service Groups | 586](#)
- [Application Signatures Overview | 588](#)
- [About the Application Signatures Page | 589](#)
- [Understanding Custom Application Signatures | 590](#)
- [Adding Application Signatures | 592](#)
- [Editing, Cloning, and Deleting Application Signatures | 597](#)
- [Adding Application Signature Groups | 599](#)
- [Editing, Cloning, and Deleting Application Signature Groups | 600](#)
- [About the Departments Page | 601](#)
- [Adding a Department | 602](#)
- [Deleting a Department | 603](#)



## Addresses and Address Groups Overview

An address specifies an IP address or a hostname. You can create addresses that can be used across all policies. Addresses are used in firewall and NAT services and apply to the corresponding policies. If you know only the hostname, you enter it into the **Hostname** field and use the address resolution option to resolve it to an IP address. You can also resolve an IP address to the corresponding hostname.

After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple addresses.

Contrail Service Orchestration (CSO) manages its address book at the global level, assigning objects to devices that are required to create policies. An address book is a collection of addresses and address groups that are available in a security zone. If the device is capable of using a global address book, CSO pushes address objects used in the policies to the global address book of the device.

### RELATED DOCUMENTATION

---

[About the Addresses Page | 571](#)

---

[Creating Addresses or Address Groups | 573](#)

---

[Editing, Cloning, and Deleting Addresses and Address Groups | 575](#)

## About the Addresses Page

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

Use this page to create, edit, and delete addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create an address or address group. See [“Creating Addresses or Address Groups” on page 573](#).
- Modify, clone, or delete an address or address group. See [“Editing, Cloning, and Deleting Addresses and Address Groups” on page 575](#).

- View the configured parameters of an address or address group. Click the details icon that appears when you hover over the name of an address or address group or select **More > Detailed View**.
- Show or hide columns about the address or address group. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for an address or address group. Click the Search icon in the top right corner of the page to search for an address or address group.

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

The search results are displayed on the same page.

Field Descriptions

Table 210 on page 572 provides guidelines on using the fields on the Addresses page.

Table 210: Fields on the Addresses Page

Field	Description
Name	View the name of the address or address group.
Type	View the type of the address or address group.
Hostname	View the hostname of the address.
IP Address	View the IP address associated with the address.
Description	View the description provided about the address or address group when it was created.

RELATED DOCUMENTATION

Addresses and Address Groups Overview   571
Creating Addresses or Address Groups   573
Editing, Cloning, and Deleting Addresses and Address Groups   575

## Creating Addresses or Address Groups

Use the **Addresses** page to create addresses and address groups. Addresses and address groups are used in firewall and NAT services. After you create an address, you can combine it with other addresses to form an address group. Address groups are useful when you want to apply the same policy to multiple services.

To create an address or address group:

1. Select **Configure > Shared Objects > Addresses**.

The **Addresses** page appears.

2. Click on the add icon (+).

The **Create Addresses** page appears.

3. Complete the configuration according to the guidelines provided in [Table 211 on page 573](#) and [Table 212 on page 575](#).

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

A new address or address group with your configurations is created. You can use this object in firewall or NAT policies.

**Table 211: Fields on the Create Addresses Page**

Field	Description
Object Type	Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group. <a href="#">Table 212 on page 575</a> describes address group configuration parameters.
Name	Enter a unique name for the address. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your address; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.

Table 211: Fields on the Create Addresses Page (*continued*)

Field	Description
Type	<p>Select a type of address and fill in the corresponding fields. Available types are:</p> <ul style="list-style-type: none"> <li>• <b>Host</b> <ul style="list-style-type: none"> <li>• <b>Host IP</b>—Enter the IPv4 or IPv6 host IP address. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2. If you do not know the IP address, you can enter the hostname and click <b>Look up hostname</b>.</li> <li>• <b>Hostname</b>—Enter the hostname. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed. If you do not know the host name, you can enter the IP address and click <b>Look up IP address</b>. For example, enter www.company.com and click <b>Look up IP address</b>. Hostname lookup is supported for IPv4 and IPv6 addresses.</li> </ul> </li> <li>• <b>Range</b> <ul style="list-style-type: none"> <li>• <b>Start Address</b>—Enter a starting IPv4 or IPv6 address for the address range. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2.</li> <li>• <b>End Address</b>—Enter an ending IPv4 or IPv6 address for the address range. The range is validated after you enter the address.</li> </ul> <p><b>NOTE:</b> An address range is configured on a managed device as an address set with one or more network address objects covering the specified address range.</p> </li> <li>• <b>Network</b> <ul style="list-style-type: none"> <li>• <b>Network</b>—Enter the network IP address. For example: 192.0.2.0. IPv6 is also supported. For example: 2001:db8:4136:e378:8000:63bf:3fff:fdd2.</li> <li>• <b>Subnet Mask</b>—Enter the subnet mask for the network range. For example, IPv4 netmask: 192.0.2.0/24. The subnet mask is validated as you enter it. You must enter the correct subnet mask in accordance with the network value. For example, IPv6 netmask: 2001:db8:4136:e378:8000:63bf:3fff:fdd2.</li> </ul> </li> <li>• <b>Wildcard</b> <ul style="list-style-type: none"> <li>• <b>Network</b>—Enter the network IPv4 or IPv6 address. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2.</li> <li>• <b>Wildcard Mask</b>—Enter the wildcard mask for the network range. For example: 0.0.0.255.</li> </ul> </li> <li>• <b>DNS Host</b> <ul style="list-style-type: none"> <li>• <b>DNS Name</b>—Enter the DNS name. For example: company.com. Only alphanumeric characters, dashes, and periods are accepted. This name cannot exceed 69 characters in length, and must end with an alphanumeric character.</li> </ul> </li> </ul>

Table 212: Address Group Settings

Field	Description
Object Type	Select Address or Address Group. If you select Address Group, then the screen changes so you can select the addresses you want to include in your address group. <a href="#">Table 211 on page 573</a> describes address group configuration parameters.
Name	Enter a unique name for the address group. It must begin with an alphanumeric character and cannot exceed 63 characters. Dashes and underscores are allowed.
Description	Enter a description for your address group; maximum length is 1,024 characters. You should make this description as useful as possible for all administrators.
Addresses	Select the check box beside each address you want to include in the address group. Click the greater-than icon (>) to move the selected address or addresses from the <b>Available</b> column to the <b>Selected</b> column. Note that you can use the fields at the top of each column to search for addresses.

#### RELATED DOCUMENTATION

[Addresses and Address Groups Overview | 571](#)

[About the Addresses Page | 571](#)

[Editing, Cloning, and Deleting Addresses and Address Groups | 575](#)

## Editing, Cloning, and Deleting Addresses and Address Groups

### IN THIS SECTION

- [Editing Addresses and Address Groups | 576](#)
- [Cloning Addresses and Address Groups | 576](#)
- [Deleting Addresses and Address Groups | 577](#)

You can edit, clone, and delete addresses and address groups from the **Addresses** page.

## Editing Addresses and Address Groups

To modify the parameters configured for an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

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

The **Edit** page appears, showing the same options as displayed when you create a new address or address group.

3. Modify the parameters according to the guidelines provided in [“Creating Addresses or Address Groups” on page 573](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

When you click **OK**, the modified address or address group is displayed on the **Addresses** page.

**NOTE:** When you edit an address that is deployed as part of a policy, you will need to redeploy that policy in order for the changes to take effect. See [“Deploying Policies” on page 548](#) for more information.

## Cloning Addresses and Address Groups

To clone an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

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

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

3. Modify the configured parameters of the address or address group, as required.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you select **OK**, the cloned address or address group is saved.

## Deleting Addresses and Address Groups

**NOTE:** Only addresses or address groups that have not been referenced in any policy can be deleted. If you try to delete such an address or address group, an error message will be displayed.

To delete an address or address group:

1. Select **Configuration > Shared Objects > Addresses**.

The **Addresses** page appears.

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

An alert message appears verifying that you want to delete your selection.

3. Click **Yes** to delete the address or address group. If you do not want to delete, click **Cancel** instead.

If you select **Yes**, the selected address or address group is deleted, unless it is referenced in a policy.

## RELATED DOCUMENTATION

---

[Addresses and Address Groups Overview | 571](#)

---

[About the Addresses Page | 571](#)

---

[Creating Addresses or Address Groups | 573](#)

## Services and Service Groups Overview

A service refers to an application on a device. For example, Domain Name Service (DNS). Services are based on protocols and ports used by an application, and when added to a policy, a configured service can be applied across all devices. Services are candidates for firewall policy end-points. The protocols used to create a service include: TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6. Contrail Service Orchestration (CSO) also includes predefined, commonly used services, and you cannot modify or delete them.

Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services, as this enables you create fewer policies.

RELATED DOCUMENTATION

<a href="#">About the Services Page   578</a>
<a href="#">Creating Services and Service Groups   579</a>
<a href="#">Editing, Cloning, and Deleting Services and Service Groups   586</a>

## About the Services Page

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

Use the **Services** page to create, modify, clone and delete service or service groups. You can also create and manage protocols, that you use to create services.

A service refers to an application on a device, such as Domain Name Service (DNS). Services are based on protocols and ports used by an application. When added to a policy, a configured service can be applied across all devices. The protocols available to create a service include: TCP, UDP, SUN-RPC, MS-RPC, ICMP, ICMPv6, and so on.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a service or service group. See [“Creating Services and Service Groups” on page 579](#).
- Modify, clone or delete a service or service group. See [“Editing, Cloning, and Deleting Services and Service Groups” on page 586](#).
- View the configured parameters of a service or service group. Click the details icon that appears when you hover over the name of a service or service group, or click **More > Detailed View**. See *Viewing Object Details*.
- Show or hide columns about the services or service groups. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search a specific service or service group. Click the Search icon in the top right corner of the page to search for a service or service group.

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

The search results are displayed on the same page.

### Field Descriptions

[Table 213 on page 579](#) provides guidelines on using the fields on the **Services** page.



Table 213: Fields on the Service Page

Field	Description
Name	Name of the service or service group.
Type	Specifies whether the object is a service or service group.
Description	Description about the service or service group.
Predefined or Custom	List of predefined services and service groups, and a list of custom services or service groups that you created.

## RELATED DOCUMENTATION

[Services and Service Groups Overview | 577](#)

[Creating Services and Service Groups | 579](#)

[Editing, Cloning, and Deleting Services and Service Groups | 586](#)

## Creating Services and Service Groups

Use the **Create Service** page to create a service. You can create services based on protocols and ports used by an application. The protocols used to create a service include: TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6. Once you create a service, you can combine it with other services to form a service group. Service groups are useful when you want to apply the same policy to multiple services.

You can also create or modify protocols that you base your services on, from the **Services** page.

To configure a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Click the add icon (+) to create service or service group.

The **Create Services** page appears.

3. Complete the configuration of a service according to the guidelines provided in [Table 214 on page 580](#).

If you want to configure a service group, see [Table 215 on page 580](#).

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

A new service or service group with the configuration you provided is created. You can use this service or service group as an endpoint in firewall policies.

[Table 214 on page 580](#) provides guidelines on using the fields to create a service.

**Table 214: Service Settings**

Field	Description
Object Type	Select <b>Service</b> or <b>Service Group</b> . If you select <b>Service Group</b> , then the page changes so you can select the services you want to include in your service group.
Name	Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your service. You should make this description as useful as possible for all administrators.
Protocols	<p>Select the protocol you want to associate with the service. You can use existing protocols that are listed in the <b>Protocols</b> table. You can also create a new protocol, or edit existing protocols:</p> <ul style="list-style-type: none"> <li>• To create a new protocol, click on the add icon (+). See <a href="#">“Creating Protocols” on page 581</a>.</li> <li>• To edit an existing protocol, click on the edit icon (pencil symbol). See <a href="#">“Editing and Deleting Protocols” on page 584</a>.</li> </ul>

[Table 215 on page 580](#) provides guidelines on using the fields to create a service group.

**Table 215: Service Group Settings**

Field	Description
Object Type	Select <b>Service</b> or <b>Service Group</b> . If you select <b>Service Group</b> , then the screen changes so you can select the services you want to include in your service group.
Name	Enter a unique name for the service. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your service group. You should make this description as useful as possible for all administrators.

Table 215: Service Group Settings (continued)

Field	Description
Services	Select the service you want to include in the service group and click the greater-than icon (>) to move the selected service or services from the <b>Available</b> column to the <b>Selected</b> column. You can use the search field at the top of each column to search for listed services.

## RELATED DOCUMENTATION

- [Services and Service Groups Overview | 577](#)
- [About the Services Page | 578](#)
- [Editing, Cloning, and Deleting Services and Service Groups | 586](#)
- [Creating Protocols | 581](#)
- [Editing and Deleting Protocols | 584](#)

## Creating Protocols

Use the **Create Protocol** page to create TCP, UDP, MS-RPC, SUN-RPC, ICMP, and ICMPv6 protocols, that can be used in services. A service refers to an application on a device. Services are based on protocols and ports used by an application.

To create a protocol:

1. Select **Configuration > Shared Objects > Services**.  
The **Services** page appears.
2. Click the add icon (+) to create service or service group.  
The **Create Services** page appears.
3. Click the add icon (+) that appears about the **Protocols** table.  
The **Create Protocol** page appears.
4. Complete the configuration of the protocol according to the guidelines provided in [Table 216 on page 582](#) and [Table 217 on page 582](#).
5. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new protocol with the configuration you provided is created. You can use this protocol to create services.

[Table 216 on page 582](#) provides guidelines on using the fields to create a protocol.

**Table 216: Fields on Create Protocol Page Settings**

Field	Description
<b>General Information</b>	
Name	Enter a unique name for the protocol. It must begin with an alphanumeric character and cannot exceed 63 characters; dashes and underscores are allowed.
Description	Enter a description for your protocol. It cannot exceed 1,024 characters.
Type	Select the type of the protocol you want to create and fill in the corresponding fields. The available types of protocols are: TCP, UDP, ICMP, SUN-RPC, MS-RPC, ICMPv6, and so on. If you select TCP, continue with this table. See <a href="#">Table 217 on page 582</a> for the other protocol types.
Destination Port	Enter a destination port number for TCP. The range is from 0 to 65,535.
<b>Advanced Settings</b>	
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds or 2,160 minutes.
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter the source port or port range for the protocol.

[Table 217 on page 582](#) includes the settings and guidelines for the various protocol types.

**Table 217: Create Protocol Type Settings**

Field	Description
<b>UDP</b>	
Destination Port	Enter a destination port number for UDP. This is a value or value range from 0 through 65,535.
<b>Advanced Settings</b>	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.

Table 217: Create Protocol Type Settings (*continued*)

Field	Description
ALG	Select an ALG (Application Layer Gateway) service option if applicable.
Source Ports and Port Ranges	Enter a source port or port range for UDP. This is a value or value range from 0 through 65,535.
<b>ICMP</b>	
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ICMP Type	Enter a value from 0 through 225 for the ICMP message type. For example, enter 1 for host unreachable. You can find these values in RFC 792.
ICMP Code	Enter a value from 0 through 225 for the ICMP code. For example, enter 0 for echo reply. You can find these values in RFC 792.
<b>SUN-RPC</b>	
Destination Port (available if Enable ALG is selected)	Enter a destination port for SUN-RPC. This is a value or value range from 0 through 65,535.
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port in the field that becomes available.
RPC Program Number	Enter a value or value range for the RPC (remote procedure call) service. For example, enter 100,017 for remote execution. You can find these values in RFC 5531.
Protocol Type	Select TCP or UDP for the protocol type.
<b>MS-RPC</b>	
Destination Port (available if Enable ALG is selected)	Enter a destination port for MS-RPC. This is a value or value range from 0 through 65,535.
Enable Inactivity Timeout	Enabled by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
Enable ALG	Not selected by default. If you enable ALG for this protocol, you must enter a destination port number in the field that becomes available.

Table 217: Create Protocol Type Settings (continued)

Field	Description
UUID	Enter the corresponding UUID value for the MS-RPC service. For predefined values, refer to MS-RPC UUID Mappings.
Protocol Type	Select TCP or UDP for the protocol type.
<b>ICMPv6</b>	
Enable Inactivity Timeout	Selected by default. Enter a timeout value for this protocol in seconds or minutes. The maximum values are 129,600 seconds and 2,160 minutes.
ICMP Type	Enter a value from 0 through 225 for the ICMPv6 message type. You can find these values in RFC 4443.
ICMP Code	Enter a value from 0 through 225 for the ICMPv6 code. You can find these values in RFC 4443.
Destination Port	Use other to create protocols that do not match the provided type categories. Enter a destination port for the other protocol. This is a value or value range from 0 through 65,535.

## RELATED DOCUMENTATION

- [Editing and Deleting Protocols | 584](#)
- [About the Services Page | 578](#)
- [Creating Services and Service Groups | 579](#)

## Editing and Deleting Protocols

### IN THIS SECTION

- [Editing Protocols | 585](#)
- [Deleting Protocols | 585](#)

You can edit and delete protocols through the **Services** page.

## Editing Protocols

To modify the parameters configured for a protocol:

1. Select **Configuration > Shared Objects > Services** .

The **Services** page appears.

2. Select the service to which the protocol you want to edit is associated, and click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Service**.

The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.

3. Select the protocol that you want to edit, and then click on the edit icon (pencil symbol) on the right top corner of the **Protocols** table, or right-click and select **Edit Protocol**.

The **Edit Protocol** page appears, showing the same fields as those seen when you create a new protocol.

4. Modify the parameters of the protocol according to the guidelines provided in [“Creating Protocols” on page 581](#).

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

If you click **OK**, the modified protocol appears in the **Protocols** table.

## Deleting Protocols

To delete a protocol:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

2. Select the service to which the protocol you want to delete is associated, and click on the edit icon (pencil symbol) on the right top corner of the table, or right-click and select **Edit Service**.

The **Edit Service** page appears, listing the protocols associated with the service in **Protocols** table.

3. Select the protocol you want to delete and then click the delete icon (X).

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

4. Click **Yes** to delete the protocol. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected protocol is deleted.

## RELATED DOCUMENTATION

Services and Service Groups Overview	577
About the Services Page	578
Creating Services and Service Groups	579
Editing, Cloning, and Deleting Services and Service Groups	586
Creating Protocols	581

# Editing, Cloning, and Deleting Services and Service Groups

## IN THIS SECTION

- Editing Services and Service Groups | 586
- Cloning Services or Service Groups | 587
- Deleting Services and Service Groups | 587

You can edit, clone, and delete services and service groups from the **Services** page.

## Editing Services and Service Groups

To modify the parameters configured for a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

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

The **Edit Service** page appears, displaying the same options that are displayed when creating a new service or service group.



3. Modify the parameters according to the guidelines provided in [“Creating Services and Service Groups” on page 579](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, you will see the modified service or service group in the **Services** page.

## Cloning Services or Service Groups

To clone a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

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

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

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

If you click **OK**, the cloned service or service group will appear beneath the selected service or service group.

## Deleting Services and Service Groups

To delete a service or service group:

1. Select **Configuration > Shared Objects > Services**.

The **Services** page appears.

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

An alert message appears, verifying that you want to delete the service or service group.

3. Click **Yes** to delete the service or service group. If you do not want to delete, click **Cancel** instead.

If you click **Yes**, the selected service or service group is deleted.

## RELATED DOCUMENTATION

---

[Services and Service Groups Overview | 577](#)

---

[About the Services Page | 578](#)

---

[Creating Services and Service Groups | 579](#)

---

## 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 | 589](#)

---

[Adding Application Signatures | 592](#)

---

[Editing, Cloning, and Deleting Application Signatures | 597](#)

---

[Adding Application Signature Groups | 599](#)

---

[Editing, Cloning, and Deleting Application Signature Groups | 600](#)

---

[Signature Database Overview | 262](#)

---

# 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:

- Add an application signature. See [“Adding Application Signatures” on page 592](#).
- Modify, clone, or delete an application signature. See [“Editing, Cloning, and Deleting Application Signatures” on page 597](#).
- Add an application signature group. See [“Adding Application Signature Groups” on page 599](#).
- Modify, clone, or delete an application signature group. See [“Editing, Cloning, and Deleting Application Signature Groups” on page 600](#).
- 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**.
- Show or hide columns in the **Application Signatures**. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for a specific application signature or application signature group. Click the Search icon in the top right corner of the page to search for an application signature or application signature group.
- 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 218 on page 589](#) provides guidelines on using the fields on the **Application Signatures** page.

**Table 218: Fields on the Application Signatures Page**

Field	Description
Name	Name of the application signature or application signature group.

Table 218: Fields on the Application Signatures Page (*continued*)

Field	Description
Object Type	Signature type—either application signature or application signature group.
Category	UTM category of the application signature. For example, the value of <b>Category</b> can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Subcategory	UTM subcategory of the application signature. For example, the value of <b>Subcategory</b> 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 <b>Risk</b> 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 | 588](#)

[Adding Application Signatures | 592](#)

[Editing, Cloning, and Deleting Application Signatures | 597](#)

[Adding Application Signature Groups | 599](#)

[Editing, Cloning, and Deleting Application Signature Groups | 600](#)

[Signature Database Overview | 262](#)

[About the Signature Database Page | 263](#)

## Understanding Custom Application Signatures

Application identification supports user-defined custom application signatures to detect applications as they pass through the device. Custom application signatures are unique to your environment and are not part of the predefined application package. You use this custom application signature in SD-WAN policies to steer, and block traffic when a threat is detected.

Custom application signatures are required to:

- Control traffic particular to an environment.
- Bring visibility to unknown or unclassified applications.
- Identify Layer 7 applications or temporary applications, and to achieve further granularity of known applications.
- Perform QoS for your specific application.

CSO supports the following custom application signatures:

- **ICMP-Based Mapping**—The Internet Control Message Protocol (ICMP) mapping technique maps standard ICMP message types and optional codes to a unique application name. This mapping technique lets you differentiate between various types of ICMP messages.
- **IP Address-Based Mapping**—Layer 3 and Layer 4 address mapping defines an application by the IP address and optional port range of the traffic.

To ensure adequate security, use address mapping when the configuration of your private network predicts application traffic to or from trusted servers. Address mapping provides efficiency and accuracy in handling traffic from a known application.

With Layer 3 and Layer 4 address-based custom applications, you can match the IP address and port range to destination IP address and port range. When IP address and port range are configured, they must match the destination tuples (IP address and port range) of the packet.

For example, consider a Session Initiation Protocol (SIP) server that initiates sessions from its known port 5060. Because all traffic from this IP address and port is generated by only the SIP application, the SIP application can be mapped to an IP address of the server and port 5060 for application identification. In this way, all traffic with this IP address and port is identified as SIP application traffic.

- **IP Protocol-Based Mapping**—Standard IP protocol numbers can map an application to IP traffic. As with address mapping, to ensure adequate security, use IP protocol mapping only in your private network for trusted servers.
- **Layer 7-Based Signatures**—Layer 7 custom signatures define an application running over TCP or UDP or Layer 7 applications. Layer 7-based custom application signatures are required for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. The custom signature is cacheable for Layer 7 signatures only. You can create multiple signatures and each signature can contain multiple members (maximum 15 members).

Layer 7-based custom application signatures detect applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS). Application identification can extract the server name information or the server certification from the TLS or SSL sessions. It can also detect patterns in TCP or UDP payload in Layer 7 applications.

RELATED DOCUMENTATION

<a href="#">Adding Application Signatures   592</a>
<a href="#">Editing, Cloning, and Deleting Application Signatures   597</a>

## Adding Application Signatures

You can add custom application signatures for applications that are not part of the Juniper Networks predefined application database. When you add custom application signatures, make sure that your application signatures are unique, by providing a unique and relevant name.

You can add custom application signatures by specifying a name, protocol, port number where the application runs, and match criteria.

To create a custom application signature:

1. Select **Configuration > Shared Objects > Application Signatures**.
2. Click **Create > Signature**.
3. Complete the configuration according to the guidelines provided in [Table 219 on page 592](#).
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

A new application signature with your configurations is created. You use this application signature while creating SD-WAN policy intents.

[Table 219 on page 592](#) provides guidelines on using the fields on the **Create Application Signature** page.

Table 219: Fields on the Create Application Signature Page

Field	Description
Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the application signature.

Table 219: Fields on the Create Application Signature Page (*continued*)

Field	Description
Order	<p>Enter the order for the custom application signature. A lower order value has higher priority. This option is used when multiple custom application signatures of the same type match the same traffic. However, you cannot use this option to prioritize among different type of applications such as TCP stream-based applications against TCP port-based applications or IP address-based applications against port-based applications.</p> <p>Range is 1-50000.</p>
Priority	Specify the application signature priority (high or low) over other application signatures.
<b>Select one or more Application Identification match criteria</b>	<p>Select one or more applications matching criteria from the following list:</p> <ul style="list-style-type: none"> <li>• ICMP Mapping</li> <li>• IP Protocol Mapping</li> <li>• Address Mapping</li> <li>• L7 Signature</li> </ul>
<i>ICMP Mapping</i>	<p>Specify the Internet Control Message Protocol (ICMP) value for an application while configuring custom application signatures for application identification.</p> <p>The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name. The ICMP code and type provide additional specification, for packet matching in an application definition.</p>
ICMP Type	<p>Enter an ICMP value for the application. The ICMP mapping technique maps standard ICMP message types and optional codes to a unique application name.</p> <p>Range is 0-254.</p>
ICMP Code	<p>Enter an ICMP code for the application. The field provides further information (such as RFCs) about the ICMP type field.</p> <p>Range is 0-254.</p>
<i>IP Protocol Mapping</i>	Specify the IP protocol value for an application to match. This parameter is used to identify an application based on IP and is intended only for IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.

Table 219: Fields on the Create Application Signature Page (*continued*)

Field	Description
IP Protocol	<p>Enter an IP Protocol number for the application. Standard IP protocol numbers map an application to IP traffic. To ensure adequate security, use IP protocol mapping only in your private network for trusted servers.</p> <p>Range is 0-254.</p> <p>You can find a complete list of industry standard protocol numbers at the <a href="#">IANA website</a>.</p> <p><b>NOTE:</b> You cannot use IP protocol numbers 1(ICMP), 6(TCP ) and 17(UDP) for custom application signature creation. Instead, we recommend you to use L7 signature policies for these protocols.</p>
<i>Address Mapping</i>	<p>Layer 3 and Layer 4 address mapping defines an application by matching the destination IP address or port range (optional) of the traffic. Use the address mapping option to configure custom applications signatures when the configuration of your private network predicts application traffic to or from trusted servers.</p> <p>Address mapping provides efficiency and accuracy while handling traffic from a known application.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• You must specify either IP address or TCP/UDP port range for address mapping.</li> <li>• If both IP address and TCP/UDP ports are configured, both should match destination tuples (IP address and port range) of the packet.</li> </ul>
Name	<p>Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed; maximum length is 63 characters.</p>
Dst. IP Address	<p>Enter an IPv4 or IPv6 address for the application.</p>
CIDR	<p>Enter a CIDR value for the IP Address that you assign to the application.</p> <p>Range for IPv4 address is 1-32.</p> <p>Range for IPv6 address is 1-128.</p>
Dst. TCP Port range (Optional)	<p>Enter space-separated list of ports or port ranges to match a TCP destination port for Layer 3 and Layer 4 address-based custom applications.</p> <p>The range is 0-65535.</p> <p>Example: 80-82 443.</p>



Table 219: Fields on the Create Application Signature Page (*continued*)

Field	Description
Dst. UDP port range (Optional)	Enter space-separated list of ports or port ranges ranges to match an UDP destination port for Layer 3 and Layer 4 address-based custom applications. The range is 0-65535.  Example: 160-162 260.
<i>L7 Signature</i>	Specify the Layer 7-based custom application signatures that are required to identify the multiple applications running on the same L7 protocols.
Cacheable	Select True to enable caching of application identification results on the device.  Set this option to <b>True</b> only when L7 signatures are configured alone in a custom signature. This option is not supported for address-based, IP protocol-based, and ICMP-based custom application signatures.
Name	Displays the name of the L7 signature.
Port range	Displays the port range for the application.
Over Protocol	Displays the L7 application protocol that matches the signature..
Members	Displays the member name for L7 signature.
<i>Add L7 Signature</i>	Configure a custom signature based on L7 applications. You create Layer 7-based custom application signatures for the identification of multiple applications running on the same L7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol.
Over Protocol	Displays the signature to match the application protocol.  Example: HTTP.
Signature Name	Enter a unique name that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Port Range	Enter the port range for the application.  Range is 0-65535  Example: 80-82,443

Table 219: Fields on the Create Application Signature Page (*continued*)

Field	Description
Member No.	Enter the member name for a custom application signature. Custom signatures can contain multiple members that define attributes for an application. (The supported member name range is m01–m15.)
Direction	<p>Select the direction of the packet flow to which the signature must be matched.</p> <ul style="list-style-type: none"> <li>any—The direction of packet flow can either be from client-side to server-side or from server-side to client-side.</li> <li>client-to-server—The direction of packet flow is from client-side to server-side.</li> <li>server-to-client—The direction of packet flow is from server-side to client-side.</li> </ul>
Pattern	Enter the deterministic finite automaton (DFA) pattern matched on the context. The DFA pattern specifies the pattern to be matched for the signature. Maximum length is 128.
Context ( <i>Over HTTP</i> )	<p>Select the service-specific context from the following list:</p> <ul style="list-style-type: none"> <li>http-get-url-parsed-param-parsed</li> <li>http-header-content-type</li> <li>http-header-cookie</li> <li>http-header-host</li> <li>http-header-user-agent</li> <li>http-post-url-parsed-param-parsed</li> <li>http-post-variable-parsed</li> <li>http-url-parsed</li> <li>http-url-parsed-param-parsed</li> </ul> <p>For possible combinations of context and direction for L7 application creation, refer <a href="#">context (Application Identification)</a>.</p>
Context ( <i>Over SSL</i> )	Select the service-specific context as <b>ssl-server-name</b> .
Context ( <i>Over TCP</i> )	Select the service-specific context as <b>stream</b> .
Context ( <i>Over UDP</i> )	Select the service-specific context as <b>stream</b> .

## RELATED DOCUMENTATION

[Understanding Custom Application Signatures | 590](#)
[Editing, Cloning, and Deleting Application Signatures | 597](#)

---

[Creating SD-WAN Policy Intents | 412](#)

---

[Adding SLA-Based Steering Profiles | 424](#)

---

[Adding Path-Based Steering Profiles | 435](#)

---

## Editing, Cloning, and Deleting Application Signatures

### IN THIS SECTION

- [Editing Application Signatures | 597](#)
- [Cloning Application Signatures | 598](#)
- [Deleting Application Signatures | 598](#)

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

### Editing Application Signatures

To modify the parameters configured for a cloned user-created (custom) application signature:

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

The **Application Signatures** page appears.

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

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

3. Modify the parameters according to the guidelines provided in *Adding Application Signatures*.
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

The modified application signature appears on the **Application Signatures** page.

## Cloning Application Signatures

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

To clone a custom application signature:

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

The **Application Signatures** page appears.

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

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

3. Modify the fields as required. Refer to the guidelines provided in *Adding Application Signatures*.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

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

## Deleting Application Signatures

To delete a cloned user-created (custom) application signature:

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

The **Application Signatures** page appears.

2. Select the application signature you want to delete and then click the delete icon.

An alert message appears to verify that you want to delete the selected application signature.

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

The deleted application signature is removed from the **Application Signatures** page.

## RELATED DOCUMENTATION

[Adding Application Signatures | 592](#)

[Editing, Cloning, and Deleting Application Signatures | 597](#)

# Adding Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you add custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

To add 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 220 on page 599](#).
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 220 on page 599](#) provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 220: 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.
Group Members	Click the add icon (+) to add signatures to your application group. On the <b>Add Application Signatures</b> page, select the check boxes next to the signatures you want to add to the group.

## RELATED DOCUMENTATION

- [Application Signatures Overview | 588](#)
- [About the Application Signatures Page | 589](#)
- [Editing, Cloning, and Deleting Application Signature Groups | 600](#)
- [Signature Database Overview | 262](#)
- [About the Signature Database Page | 263](#)

## Editing, Cloning, and Deleting Application Signature Groups

### IN THIS SECTION

- [Editing Application Signature Groups | 600](#)
- [Cloning Application Signature Groups | 600](#)
- [Deleting Application Signature Groups | 601](#)

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

### Editing Application Signature Groups

To modify the parameters configured for an application signature group:

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

The **Application Signatures** page appears.

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

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

3. Modify the parameters according to the guidelines provided in [“Adding Application Signature Groups” on page 599](#).
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 | 588](#)

[About the Application Signatures Page | 589](#)

[Adding Application Signature Groups | 599](#)

[Signature Database Overview | 262](#)

## About the Departments Page

To access this page, click **Configuration > Network Services > Shared Objects > Departments**.

You can use the Departments page to add, view, or delete departments. A department is a grouping of LAN segments within a site. You use departments to apply specific policies to LAN segments that are members of a department.

Tasks You Can Perform

You can perform the following tasks from this page:

- Add a Department. See [“Adding a Department” on page 602](#).
- Delete a department. See [“Deleting a Department” on page 603](#).

Field Descriptions

[Table 221 on page 602](#) shows the descriptions of the fields on the **Departments** page.

Table 221: Fields on the Departments Page

Field	Description
Name	Displays the name of the department.
Site/LAN Segments	Displays the sites and LAN segments that are associated with the department.
VPN	Displays the VPN to which the department is assigned.
Data Center	Displays whether the department is a data center department or not.
Description	Displays the description of the department.
UUID	Displays the Universally Unique Identifier (UUID) of the department.
Network UUID	Displays an internal UUID used by Contrail Service Orchestration (CSO).

RELATED DOCUMENTATION

<a href="#">Adding a Department   602</a>
<a href="#">Deleting a Department   603</a>

Adding a Department

You can add departments from the **Configuration > Shared Objects > Departments** page.



To add a department:

1. Click the add icon (+) on the **Departments** page.  
The **Add Department** page appears.
2. Complete the configuration settings according to the guidelines provided in [Table 222 on page 603](#).
3. Click **OK**.

You are taken to the **Departments** page where the department that you added is displayed.

Table 222: Fields on the Add Department Page

Field	Description
Name	Enter a unique name for the department, which can contain alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.
Description	Enter a description of the department.
VPN	The default VPN to which the department is assigned is displayed. <b>NOTE:</b> This field is displayed only if network segmentation is disabled for the tenant.
Data Center Department	Select whether the department is a data center department (Yes) or not (No).  A data center department can be attached (by using LAN segments) only to enterprise hubs.

RELATED DOCUMENTATION

<a href="#">About the Departments Page   601</a>
<a href="#">Deleting a Department   603</a>

## Deleting a Department

You can delete departments by clicking the delete icon (X) on the **Departments** page. You can delete only one department at a time. You cannot delete a department that is associated with one or more LAN segments. Before you delete the department, you must reassign the LAN segments assigned to that department.

To delete a department:

1. Click **Configuration > Shared Objects > Departments**.

The Departments page appears.

2. Select the department that you want to delete.

3. Click the delete icon (X).

The Delete Department page appears.

4. Click **OK** to confirm the deletion.

The department is deleted and you are returned to the Departments page

#### RELATED DOCUMENTATION

[About the Departments Page | 601](#)

[Adding a Department | 602](#)



## Monitoring Jobs and Audit Logs

---

[Managing Jobs](#) | **606**

[Managing Audit Logs](#) | **612**

---

# Managing Jobs

## IN THIS CHAPTER

- [About the Jobs Page | 606](#)
- [Editing and Deleting Scheduled Jobs | 608](#)
- [Viewing Job Details | 610](#)
- [Retrying a Failed Job on Devices | 611](#)

## About the Jobs Page

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

A job is an action that is performed on any object that is managed by CSO, such as a device, tenant, site, or user. You can monitor the status of jobs that have run or are scheduled to run in CSO. You can run the job immediately or schedule it for a later date and time. You can view the status of the job whether it is completed or failed. You can retry tssm.ztp type jobs that are failed.

Use this page to view the list of all jobs and the jobs that are scheduled to be executed. You can view general information about the jobs and the overall progress and status of the jobs. You can also edit and delete scheduled jobs.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a job. See [“Viewing Job Details” on page 610](#).
- Retry a job. See [“Retrying a Failed Job on Devices” on page 611](#).
- Edit and delete scheduled jobs. See [“Editing and Deleting Scheduled Jobs” on page 608](#).

### Field Descriptions

[Table 223 on page 607](#) provides guidelines on using the fields on the Jobs page.

Table 223: Fields on the Jobs Page

Field	Description
Job Name	View the name of the job. CSO automatically generates the job name.  Example: MSEC_DOWNLOAD_IPS/APPLICATION_SIGNATURES_08_Jul_17_124229_024
Resource Name	View the resource name of the job.  Example: Download IPS/Application Signatures
Status	View the status of the job to know whether the job succeeded, failed, or in progress.  Example: Success
Owner	View the name of the owner who created the job.  Example: cspadmin
Number of Tasks	View the number of tasks associated with the job.  Example: 2  For example, the tasks <b>site.ucpe-32</b> and <b>customer.sdwan</b> are associated with the job.
Job ID	When a job is initiated from a object in CSO, CSO assigns a unique ID to that job, which serves to identify the job (along with the job type) on the Jobs page. The following is a list of some of the job types supported in CSO: <ul style="list-style-type: none"> <li>• Configure Sites</li> <li>• Download Signature</li> <li>• Create Sites</li> <li>• Remove Site</li> </ul>
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 224 on page 608 provides guidelines on using the fields on the Scheduled Jobs page.

Table 224: 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 default status is scheduled.
Record Type	View the job type.  Example: tssm onboard tenant
Owner	View the name of the owner who scheduled the job.  Example: cspadmin
Next Run Time	View the time when the job is scheduled to run next.

## RELATED DOCUMENTATION

[Editing and Deleting Scheduled Jobs | 608](#)

## Editing and Deleting Scheduled Jobs

### IN THIS SECTION

- [Editing Scheduled Jobs | 609](#)
- [Deleting Scheduled Jobs | 609](#)

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

## Editing Scheduled Jobs

You can modify the date and time of deployment of scheduled jobs.

To modify a scheduled job:

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

The Jobs page displays all scheduled jobs.

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

The Edit Schedule page appears. This page displays the option that you have selected initially.

3. Modify the deployment type.

To execute the job immediately, select the **Run now** option.

To reschedule the job for a later date and time, select the **Schedule at a later time** option and select the date and time of deployment.

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

A success message is displayed indicating that the scheduled job is modified.

## Deleting Scheduled Jobs

You can delete one or more scheduled jobs.

To delete a scheduled job:

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

The Jobs page displays all scheduled jobs.

2. Select the job that you want to delete and then click the delete icon (X). You can select one or more jobs

The Confirm Delete page appears.

3. Click **Yes** to confirm.

A success message is displayed indicating that the scheduled job is deleted.

## RELATED DOCUMENTATION

[About the Jobs Page | 606](#)[Viewing Job Details | 610](#)

## Viewing Job Details

You can use the Detail for *Job-Name* page to view all the parameters of a job. This page has the following two tabs:

- **Details**—Displays the overall progress of the job and lists general information about the job (for example, the Job ID, Request ID, Created By, and so on). For more information about the field description on this page, see [“About the Jobs Page” on page 606](#).
- **Tasks**—Displays the number of tasks associated with the job. A green check mark (success ) or a red cross mark (failed) is displayed next to each task indicating the status of the task. You can click the Detailed View icon to view the summary of the task.

To view details of a job:

- Right-click the job name that you want to see the detailed view for and select **Detail View**.
- Select the job and click **More > Detail View**.
- Alternatively, hover over the job name and click the Detailed View icon that appears before it.

The Detail for *Job-Name* page appears, showing the details of the job and the number of tasks associated with the job. Click **View Logs** to view the status of the jobs. See [“About the Jobs Page” on page 606](#) for a description of each fields on this page.

## RELATED DOCUMENTATION

[About the Jobs Page | 606](#)



## 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.

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*

*Editing and Deleting Scheduled Jobs*

# Managing Audit Logs

## IN THIS CHAPTER

- [Audit Logs Overview | 612](#)
- [About the Audit Logs Page | 613](#)
- [Viewing the Details of an Audit Log | 614](#)
- [Exporting Audit Logs | 617](#)
- [Purging Audit Logs \(After Archiving or Without Archiving\) | 618](#)

## Audit Logs Overview

An audit log is a record of a sequence of activities that have affected a specific operation or procedure. Audit logs are useful for tracing events and for maintaining historical data.

Audit logs contain information about tasks initiated by using the Contrail Service Orchestration (CSO) GUI or APIs. In addition to providing information about the resources that were accessed, audit log entries usually include details about user-initiated tasks, such as the name, role, and IP address of the user who initiated a task, the status of the task, and date and time of execution.

**NOTE:** Device-driven tasks (that is, tasks not initiated by the user) are not recorded in audit logs.

Administrators can use audit logs to review events. For example, administrators can identify the user accounts associated with an event, determine the chronological sequence of events. For audit log entries that have an associated job, you can click the hyperlinked job ID to go to the Jobs page, where you can view the details of the job.

## RELATED DOCUMENTATION

[About the Audit Logs Page | 613](#)

[Exporting Audit Logs | 617](#)

## About the Audit Logs Page

To access this page, select **Administration > Audit Logs**.

Use the Audit Logs page to view tasks that you have initiated either by using the Contrail Service Orchestration (CSO) GUI or APIs. You can also export audit logs as a comma-separated values (CSV) file and purge audit logs after archiving them or without archiving them.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View the details of various user-initiated tasks by selecting **More > Details**. You can also mouse over the audit log and click on the **Detailed View** icon. See [“Viewing the Details of an Audit Log” on page 614](#).
- Export audit logs as a CSV file—See [“Exporting Audit Logs” on page 617](#).
- Purge audit logs—See [“Purging Audit Logs \(After Archiving or Without Archiving\)” on page 618](#).
- Search for audit logs by using keywords—Click the search icon and enter the search term in the text box and press Enter. The search results are displayed on the same page.
- Sort and filter audit logs:

**NOTE:** Sorting and filtering is applicable only to some fields.

- Click a column name to sort the audit logs based on the column name.
- Click the filter icon and select whether you want to show or hide column filters or apply a quick filter. For example, you can use audit log filtering to track user accounts that were added on a specific date, track configuration changes across a particular type of device, view services that were provisioned on specific devices, monitor user login and logout activities over time, and so on.
- Show or hide columns—Click the **Show Hide Columns** icon at the top right corner of the page and select the columns that you displayed on the Audit Logs page.

[Table 225 on page 613](#) provides description of the fields on the Audit Logs page.

Table 225: Fields on the Audit Logs Page

Field	Description
Username	Displays the username of the user who initiated the task.

Table 225: Fields on the Audit Logs Page (*continued*)

Field	Description
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
Object Name	Displays the name of the object on which the task was initiated. An object can be a tenant, site, device, device image, template, and so on.
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Description	Displays details about the task.
Status	<p>Displays the status of the task that triggered the audit log:</p> <ul style="list-style-type: none"> <li>• Success—Job or task was completed successfully.</li> <li>• Failure—Job or task failed and was terminated.</li> <li>• Job Scheduled—Job is scheduled but has not yet started.</li> <li>• Recurring Job Scheduled—Recurring job is scheduled.</li> </ul>
End Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
Job ID	<p>For tasks that have associated jobs, displays the ID of the job associated with the task.</p> <p>You can click the job ID to go to the Jobs page, where you can view the status of the job.</p>

## RELATED DOCUMENTATION

[About the Jobs Page](#) | 606

## Viewing the Details of an Audit Log

Use the Audit Log Details pane to view details of an audit log.

To view the details of an audit log:

1. Select **Administration** > **Audit Logs**.

The Audit Logs page appears displaying the audit logs.

- 2. Select the audit log for which you want to view details and click **More > Details**. Alternatively, you can mouse over the audit log, and click on the **Detailed View** icon.

The Audit Log Details pane appears on the right side of the Audit Logs page. [Table 226 on page 615](#) provides descriptions the fields on the Audit Log Details pane.

- 3. Click the close icon (X) to close the Audit Log Details pane.

You are returned to the Audit Logs page.

[Table 226 on page 615](#) provides descriptions the fields on the Audit Log Details pane.

Table 226: Fields on the Audit Log Details Pane

Field	Description
<b>Details</b>	
<b>User</b>	
Username	Displays the username of the user who initiated the task.
User IP	Displays the IP address of the client from which the user initiated the task. For tasks that do not have an associated user IP address, this field is blank.
<b>Task</b>	
Task	Displays the name of the task that triggered the audit log. For example, tenant.create, device.create, site.configure, site.provision, tenant.update, and so on.
Status	Displays the status of the task that triggered the audit log: <ul style="list-style-type: none"><li>• Success—Job or task was completed successfully.</li><li>• Failure—Job or task failed and was terminated.</li><li>• Job Scheduled—Job is scheduled but has not yet started.</li><li>• Recurring Job Scheduled—Recurring job is scheduled.</li></ul>
Description	Displays details about the task.
<b>Affected Objects</b>	

Table 226: Fields on the Audit Log Details Pane (*continued*)

Field	Description
Object Name	<p>Displays the name of the affected object on which the task was initiated. An affected object can be a tenant, site, device, device image, template, and so on.. Click the hyperlinked object name to view details of the object:</p> <ul style="list-style-type: none"> <li>• If the affected object is a site, the Sites page appears. See <a href="#">“About the Sites Page” on page 40.</a></li> <li>• If the affected object is a device, the Tenant Devices page appears. See <a href="#">“About the Devices Page” on page 210.</a></li> <li>• If the affected object is a tenant, clicking on the tenant name displays an error message as you do not have permission to view this page.</li> </ul> <p><b>NOTE:</b> If the object is deleted or if you do not have permissions to view it, an error message is displayed.</p>
Object UUID	Displays the Universally Unique Identifier (UUID) of the affected object.
<b>Log Info</b>	
Audit Log ID	Displays the automatically-generated unique ID of the audit log associated with the task.
Job ID	<p>For tasks that have associated jobs, displays the ID of the job associated with the task.</p> <p>You can click the job ID to go to the Jobs page, where you can view the status of the job.</p>
End Time	Displays the date and time at which the execution of the task was completed. This timestamp is stored in UTC time in the database, but is mapped to the local time zone of the client computer.
<b>Raw Audit Log</b>	
Microservice	Displays the name of the microservice that initiated the execution of the task.
Raw Audit Log	Displays all the fields of the audit log that are stored in the database. The raw audit log typically contains additional details or parameters associated with the audit log.

## RELATED DOCUMENTATION

[Audit Logs Overview](#) | 612

## Exporting Audit Logs

You can export audit logs as a comma-separated values (CSV) file that can be opened or edited using an application such as Microsoft Excel. You can view and analyze the exported audit logs, as needed.

To export the audit logs:

1. Select **Administration > Audit Logs**.

The Audit Logs page appears displaying the audit logs.

2. Click **Export**.

The Export Audit Logs page appears.

3. Specify the time period for which you want to export the audit logs according to the guidelines provided in [Table 227 on page 617](#).

**NOTE:** You can export audit logs for a maximum of 30 days prior to the current date and time. For example, if the current date is May 31, 2018, you can export the audit logs starting from May 1, 2018.

4. Click **OK** to export the audit logs.

Depending on the settings of the browser that you are using, the CSV file containing the audit logs for the specified time period is either downloaded directly, or you are asked to open or save the file.

You are returned to the Audit Logs page.

After the file is downloaded, you can open the CSV file in an application such as Microsoft Excel and view and analyze the logs as required.

**Table 227: Fields on the Export Audit Logs Page**

Field	Description
Start Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when the audit logs should be exported.
End Date and Time	Specify the date and time (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) up to when the audit logs should be exported.

RELATED DOCUMENTATION

<a href="#">Audit Logs Overview   612</a>
<a href="#">About the Audit Logs Page   613</a>
<a href="#">Viewing the Details of an Audit Log   614</a>

Purging Audit Logs (After Archiving or Without Archiving)

You can manage the volume of audit log data stored by purging log files from the CSO database without archiving them or by purging log files after archiving them. You can purge audit logs immediately or schedule the purging for a later date and schedule the purging on a recurring basis.

To purge audit logs after archiving or without archiving them:

1. Select **Administration > Audit Logs**.  
The Audit Logs page appears displaying the audit logs.
2. Click **Purge**.  
The Purge Audit Logs page appears.
3. Complete the configuration according to the guidelines provided in [Table 228 on page 618](#).

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

4. Click **OK**.  
You are returned to the Audit Logs page and one of the following operations occur:
  - If you triggered a purge of the audit logs without archiving, a job to purge the audit logs is created.
  - If you triggered a purge of the audit logs after archiving, a job is created to archive the audit logs and then purge the audit logs after archiving.After the audit logs are purged successfully, the Audit Logs page refreshes automatically and displays only the audit logs that were not purged.

Table 228: Purge Audit Logs Settings

Field	Description
Purge Options	



Table 228: Purge Audit Logs Settings (*continued*)

Field	Description
<b>Purge Logs</b>	<p>Select one of the following options to purge audit logs:</p> <ul style="list-style-type: none"> <li>• Purge audit logs that were generated before a specified date and time—If you select this option, you must enter a date and time in the <b>Before</b> field.</li> <li>• Purge generated audit logs that are older than a specified number of days—If you select this option, you must specify the number of days in the <b>Older than</b> field.</li> </ul>
<b>Before</b>	<p>To purge audit logs before a specified date and time, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format)</p> <p>You specify the time in the local time zone of the client computer.</p>
<b>Older than</b>	<p>To purge generated audit logs older than a specified number of days, enter the number of days (from 1 through 90)</p>
<b>Archive Logs Before Purging</b>	<p>To archive audit logs <i>before</i> purging them, select this check box. By default, this check box is cleared, which means that audit logs are purged without archiving them.</p> <p><b>CAUTION:</b> If you choose not to archive the audit logs before purging, the audit logs are deleted from the CSO database and cannot be recovered.</p>
<b>Archive Mode</b>	<p>Specify whether you want to archive the log files locally (<b>local</b>) or on a remote server (<b>remote</b>).</p> <p>If you archive the logs on a remote server, which is the default option, you must enter access and login details for the remote server.</p> <p><b>NOTE:</b></p> <ul style="list-style-type: none"> <li>• Archived log files are saved in a single file in compressed comma-separated values (CSV) format (extension .zip).</li> <li>• When you archive data locally, the archived log files are saved on the central microservices virtual machine (VM).</li> </ul>
<b>Username</b>	Enter a valid username to access the remote server.
<b>Password</b>	Enter a valid password to access the remote server on which the audit logs will be archived.
<b>Confirm Password</b>	For confirmation, re-enter the password to access the remote server.
<b>Remote Server IP Address</b>	Enter the IPv4 address of the remote server; for example, 192.0.2.10.

Table 228: Purge Audit Logs Settings (*continued*)

Field	Description
<b>Remote Server Path</b>	Enter the directory path on the remote server on which to store the archived log files. The directory that you specify must already exist on the remote server.
<b>Schedule Purge</b>	
<b>Type</b>	<p>Specify whether the audit logs should be purged immediately (<b>Run now</b>) or schedule the purge for later (<b>Schedule at a later time</b>).</p> <p>If you schedule the purge for later, enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) that you want the purge to occur.</p> <p>You specify the time in the local time zone of the client computer.</p>
<b>Recurrence</b>	<p>To specify whether the purge operation should occur on a recurring basis, select this check box.</p> <p><b>NOTE:</b> This option is enabled only if you choose to archive and purge audit logs older than a specified number of days.</p>
<b>Repeat</b>	Specify the periodicity of the recurrence. Currently, a weekly periodicity is the only option supported.
<b>On</b>	For purges that recur every week, specify one or more days on which you want the purge to recur.
<b>Time</b>	<p>Enter the time (in HH:MM:SS 24-hour or AM/PM format) that you want the recurring purge to occur. By default, the purge recurs at 12.00 AM.</p> <p>You specify the time in the local time zone of the client computer.</p>
<b>Ends</b>	<p>Specify whether the recurring purge ends or not:</p> <ul style="list-style-type: none"> <li>• Select <b>Never</b> to continue (without an end date) the recurring purge operation at the specified recurrence interval.</li> <li>• Select <b>On</b> and enter the date (in MM/DD/YYYY format) and time (in HH:MM:SS 24-hour or AM/PM format) on which to stop the recurring purge operation.</li> </ul> <p>You specify the time in the local time zone of the client computer.</p>

## RELATED DOCUMENTATION



# 7

PART

## Monitoring Alarms, Events, and Threats

---

Monitoring Security Alerts and Alarms | **623**

Monitoring Security and Device Events | **635**

Monitoring SD-WAN Events | **667**

Monitoring Applications | **670**

Monitoring Threats | **688**

---

# Monitoring Security Alerts and Alarms

## IN THIS CHAPTER

- [About the Monitor Overview Page | 623](#)
- [Alerts Overview | 625](#)
- [About the Generated Alerts Page | 625](#)
- [About the Alert Definitions Page | 627](#)
- [Managing Security Alerts Definitions | 628](#)
- [Creating Security Alert Definitions | 629](#)
- [Editing, Cloning, and Deleting Security Alert Definitions | 631](#)
- [About the Alarms Page | 633](#)

## 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, network services, 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.

You can also view the visual representation of the hub and link failure on this page.

- **Hub Failure** —The hub and the link connected to the hub appear in red color.
- **Link Failure** — The link connected to the hub appears in red color. However, the hub remains active and appears in green color.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View on-premise spoke site details.
- View on-premise hub site details.

- View cloud spoke sites.
- View provider hub sites.
- View multiple sites.

Field Descriptions

Table 229 on page 624 shows the descriptions of the fields on the Monitor Overview page.

Table 229: Fields on the Monitor Overview Page

Field	Description
Sites	<p>View the sites at which the service is deployed.</p> <p>Click the <b>Sites</b> drop-down list and select <b>Show sites</b></p>
Connections	<p>View the connections in the network.</p> <p>Click the <b>Connections</b> drop-down list and select <b>Show connections</b>.</p>
Only the node with alerts	<p>View the nodes with issues with the service.</p> <p>Click the drop-down list located next to the <b>Only the nodes with alerts</b> check box and select the type of alerts.</p> <ul style="list-style-type: none"><li>• Critical—Issues that prevent the node from working and require action from the operator. The nodes with critical alerts are displayed in red.</li><li>• 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.</li><li>• 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.</li></ul> <p><b>NOTE:</b> The nodes without any alerts are displayed in blue.</p>

RELATED DOCUMENTATION

<a href="#">Managing Security Alerts Definitions   628</a>
<a href="#">Creating Security Alert Definitions   629</a>

## Alerts Overview

Alerts and notifications are used to notify administrators about significant events within the system. Notifications can also be sent through e-mail. You will be notified when a predefined network traffic condition is met. The alert trigger threshold is the number of network traffic events crossing a predefined threshold within a period of time.

Alerts and notifications provide options for:

- Defining alert criteria based on a set of predefined filters. You can use the filters defined in the advanced search to create an alert. You can also save filters and add them to security alert definitions.
- Generating an alert message and notifying you when alert criteria are met.
- Searching for specific alerts on the Generated Alerts page based on alert ID, description, or alert type.
- Supporting event-based alerts.

For example, If you are an administrator, you can define a condition such that if the number of firewall-deny events crosses a predefined threshold in a given time range for a specific device, you will receive an e-mail alert.

**NOTE:** If a threshold is crossed and remains so for a long duration, new alerts are not generated. Alerts are generated again when the number of logs matching the alert criteria drops below the threshold and crosses the threshold again.

### RELATED DOCUMENTATION

---

[About the Generated Alerts Page | 625](#)

---

[About the Alert Definitions Page | 627](#)

---

[Managing Security Alerts Definitions | 628](#)

## 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 CSO 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 > Jump to Events and Logs**. The corresponding events that triggered the alert are displayed.
- Select the generated alert and then right-click or click **More > Detail View**. The Alert Detail page appears displaying all the details of the alert.
- Select the generated alert and then right-click or click **More > Clear All Selections**.

## Field Descriptions

[Table 230 on page 626](#) provides guidelines on using the fields on the Generated Alerts page.

**Table 230: Fields on the Generated Alerts Page**

Field	Description
Severity	View the severity of the alert.
Time	View the date and time when the alert was generated.
Site	View the name of the tenant site.
Source	View the source of the alert. The source identifies whether an alert is a security alert or an SD-WAN alert.
Description	View the description of the alert.
Alert Type	View the type of alert.
ID	View the alert ID. Alert ID is a unique identification for each alert. For example, b4a3c027-7157-4861-8e3c-c872721cff2d.
Service Instance	View the service instance associated with the alert..
Object Type	View the object type.
Alert Name	View the name of the alert.
Tenant	View the name of the tenant.



## RELATED DOCUMENTATION

[Managing Security Alerts Definitions](#) | 628

## About the Alert Definitions Page

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

Use the Alert Definitions page to view alert definitions for SD-WAN and manage alert definitions for security. An alert definition consists of data criterion for triggering alerts about issues in the SD-WAN environment. Alert definitions also define the necessary action required to resolve issues based on the severity of the alert. An alert is triggered when the event threshold exceeds the data criteria that is defined. You can create an alert definition to monitor your data in real time and identify issues and attacks before they impact your network.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View SD-WAN alert definitions. The SD-WAN alert definitions are loading by default when the Alert Definitions page is loaded. See [Table 231 on page 627](#) for descriptions of the fields on the SD-WAN alert definitions pane.
- Manage Security alert definitions. See [“Managing Security Alerts Definitions” on page 628](#).
- Show or hide columns that contain information about SD-WAN alert definitions. Click the **Show Hide columns** icon in the top right corner of the page and select columns that you want to view on the page.
- Search for alert definitions using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

### Field Descriptions

[Table 231 on page 627](#) describes the fields on the SD-WAN Alert Definitions pane.

Table 231: Fields on the SD-WAN Alert Definitions Pane

Field	Description
Rule Priority	View the priority of the alert definition. A value of one (1) indicates highest priority.
Alert Description	View the description of the alert.

Table 231: Fields on the SD-WAN Alert Definitions Pane (*continued*)

Field	Description
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

[Managing Security Alerts Definitions | 628](#)
[About the Generated Alerts Page | 625](#)

## Managing Security Alerts Definitions

Use the Security pane to generate alerts that warn you of problems in your monitored environment. An alert definition consists of data criteria for triggering an alert. An alert is triggered when the event threshold exceeds the data criteria that is defined.

### Tasks You Can Perform

You can perform the following tasks from this pane:

- Create security alert definition. See [“Creating Security Alert Definitions” on page 629](#).
- Edit, clone, and delete security alert definition. See [“Editing, Cloning, and Deleting Security Alert Definitions” on page 631](#).

### Field Descriptions

[Table 232 on page 628](#) provides guidelines on using the fields on the Security alert definitions pane.

Table 232: Fields on the Security Alert Definitions Pane

Field	Description
Alert Name	View the name of the alert.

Table 232: Fields on the Security Alert Definitions Pane (*continued*)

Field	Description
Alert Description	View the description for the alert.
Filter	View filter values of the alert.
Recipients	View recipients' e-mail addresses where alert notifications are sent.
Status	View the status of the alert.
Alert Type	View the type of alert.  Example: Event-based

## RELATED DOCUMENTATION

[Alerts Overview | 625](#)
[Creating Security Alert Definitions | 629](#)

## Creating Security Alert Definitions

You can create an alert definition to monitor your data in real time. You can identify issues and attacks before they impact your network.

For example, if you are an administrator, you can define a condition such that if the number of firewall deny events crosses a predefined threshold in a given time frame for a specific device, you receive an e-mail alert.

To create a security alert definition:

1. Select **Monitor > Alerts & Alarms > Alert Definitions > Security**.

The Security alert definitions page appears.

2. Click the create icon (+) or add icon (+).

The Create an Alert Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 233 on page 630](#).
4. Click **OK**. If you want to discard the changes, click **Cancel** instead.

A new alert definition with the configured alert triggering condition is created. You can view the generated alerts from the alert definition to troubleshoot the issues with your system.

**Table 233: Fields on the Security Alert Definitions Page**

Field	Description
<b>General</b>	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.
Alert Description	Enter a description for the alerts; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system-based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: info, minor, major, critical.
<b>Trigger</b>	
Use Data Criteria from Filters	<p>Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer.</p> <p>To add saved filters:</p> <ul style="list-style-type: none"> <li>• Click the <b>Use data criteria</b> from filters link. The Add Saved Filters page appears.</li> <li>• Select the filters to be added.</li> <li>• Click <b>OK</b>.</li> </ul>
Add Data Criteria	Specifies the data criteria based on the Time Span period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.
<b>Recipient(s)</b>	
E-mail Address(es)	Specify the e-mail addresses for the recipients of the alert notification.
Custom Message	Enter a custom string for identifying the type of alert in the alert notification e-mail.

## RELATED DOCUMENTATION

[Managing Security Alerts Definitions | 628](#)

[Editing, Cloning, and Deleting Security Alert Definitions | 631](#)

## Editing, Cloning, and Deleting Security Alert Definitions

### IN THIS SECTION

- [Editing Security Alert Definitions | 631](#)
- [Cloning Security Alert Definitions | 631](#)
- [Deleting Security Alert Definitions | 632](#)

You can edit, clone, and delete security alert definitions.

### Editing Security Alert Definitions

To edit the security alert definition:

1. Select **Monitor > Alerts & Alarms > Alert Definitions > Security**.

The Security Alerts Definition page appears.

2. Select the check box of the security alert definition that you want to modify, and click the edit icon.

The Edit Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Update the configuration as needed.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

### Cloning Security Alert Definitions

You can clone an alert definition when you want to quickly create a copy of an alert definition and modify its parameters including the name of the alert.

To clone an alert definition:

1. Select **Monitor > Alerts & Alarms > Alert Definitions > Security**.

The Security Alert Definitions page appears.

2. Select the alert definition that you want to clone, and click **More > Clone** at the top right corner of the page.

The Clone Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Click **OK** to save the configuration.

A new alert definition is created.

## Deleting Security Alert Definitions

You can click the delete icon (X) to delete one or more alert definitions.

To delete the alert definition:

1. Select **Monitor > Alerts & Alarms > Alert Definitions > Security**.

The Security Alerts Definition page appears.

2. Select the alert definition that you want to delete and click the delete icon (X icon).

The Confirm Delete page appears.

3. Click **Yes** to delete the alert definition or **No** to cancel the deletion.

If you click **Yes**, then the alert definition is deleted from the main page.

## RELATED DOCUMENTATION

[Managing Security Alerts Definitions | 628](#)

[Creating Security Alert Definitions | 629](#)

## About the Alarms Page

To access this page, select **Monitor > Alerts & Alarms > Alarms**.

Use the Alarms page to view system-generated alarms. Alarms notify you of conditions that might prevent the device from operating normally. Alarm conditions for a system are preset and are based on the fault monitoring and performance monitoring (FMPM) being performed on a device. For example, conditions such as hardware issues, drop in throughput and latency of data, temperature variations, and capacity optimization issues automatically trigger an alarm.

The difference between alerts and alarms lies in the type of events that are being monitored. An alert is used to notify administrators about significant events within the system. For example, when a predefined network traffic condition is met. For more information about alerts, see [“Alerts Overview” on page 625](#).

### Tasks You Can Perform

You can perform the following tasks from this page:

- View alarm activity within a specific time range:
  - Select either 2 hours (2h), 4 hours (4h), 8 hours (8h), 16 hours (16h), 24 hours (24h), or 1 week (1w), or Custom as the time range to view alarm activity. By default, alarm activity is displayed for a time range of 1 week.

If you click Custom, the Custom Time Range Selection page appears.

You must specify the **From** date and time, and **To** date and time (in MM/DD/YYYY and HH:MM:SS formats).
- View details of an alarm—Select a generated alarm on the page and right-click to select **Detail View** or click **More > Detail View** to view more details (such as alarm type, severity, and so on) of the alarm.
- Delete an alarm—Select an alarm that you want to delete and click the **Delete** icon. The selected alarm is deleted from the page.
- Apply a filter to view specific alarms—Click the **Filter** icon and select the filter criteria from the list of available options, to view only specific alarms. You can filter the alarms based on severity (critical, major, minor, normal), tenant name, site name, and source of the alarm.
- Show or hide columns on the page—Click the **Show or Hide Columns** icon to select or clear columns that you want to display or hide on the page.
- Select the number of alarms that you want to view on the page—From the **Details** list, select either **20**, **50** or **100** as the number of alarms that you want to view on the page.

Field Descriptions

Table 234 on page 634 describes the fields on the Alarms page.

Table 234: Fields on the Alarms Page

Field	Description
Severity	Severity of the alarm.
Time	Date and time when the alarm was generated.
Tenant	Name of the tenant.
Site	Name of the tenant site for which the alarm was generated.
Source	Source from where the alarm originated.
Description	Description of the alarm.
UUID	Universally Unique Identifier (UUID) of the alarm.  You can use the UUID to identify an alarm on the <b>Monitor &gt; Logs</b> page.
Link Name	Name of the link that generated the alarm.
Service Instance	Service instance associated with the alarm.
Object Type	Type of device from which the alarm originated.  Example: Hub



# Monitoring Security and Device Events

## IN THIS CHAPTER

- [About the All Security Events Page | 635](#)
- [About the Firewall Events Page | 640](#)
- [About the Web Filtering Events Page | 643](#)
- [About the IPsec VPNs Events Page | 646](#)
- [About the Content Filtering Events Page | 648](#)
- [About the Antispam Events Page | 650](#)
- [About the Antivirus Events Page | 652](#)
- [About the IPS Events Page | 655](#)
- [About the Device Events Page | 658](#)
- [About the Screen Events Page | 662](#)

## About the All Security Events Page

To access this page, click **Monitoring > Security Events > All Events**.

Use this page to get an overall, high-level view of your network environment. You can view abnormal events, attacks, viruses, or worms when log data is correlated and analyzed.

This page provides administrators with an advanced filtering mechanism and provides visibility into actual events collected by the Log Collector. Using the time-range slider, you can instantly focus on areas of unusual activity by dragging the time slider to the area of interest to you. The slider and the Custom button under Time Range remain at the top of each tab. Users select the time range, and then they can decide how to view the data, using the summary view or detail view tabs.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all events in your network. See [“Summary View” on page 636](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 636](#).

### Summary View

You can view a brief summary of all the events in your network. At the center of the page is critical information, including total number of events, viruses found, total number of interfaces that are down, number of attacks, CPU spikes, and system reboots. This data is refreshed automatically based on the selected time range. At the bottom of the page is a swim lane view of different events that are happening at a specific time. The events include firewall, web filtering, VPN, content filtering, antispam, antivirus, and IPS. Each event is color-coded, with darker shades representing a higher level of activity. Each tab provides deep information like type, and number of events occurring at that specific time.

[Table 235 on page 636](#) describes the widgets on the All Events Summary View page.

**Table 235: Widgets on the All Events Summary View Page**

Field	Description
Total Events	View the total number of all the events that includes firewall, web filtering, IPS, IPSec VPNs, content filtering, antispam, and antivirus events.
Virus Instances	View the total number of virtual instances running in the system.
Attacks	View the total number of attacks on the firewall.
Interface Down	View the total number of interfaces that are down.
CPU Spikes	View the total number of times a CPU utilization spike has occurred.
Reboots	View the total number of system reboots.
Sessions	View the total number of sessions established through firewall.

### Detail View

Click **Detail View** for comprehensive details of events in a tabular format that includes sortable columns. You can sort the events using the Group By option. For example, you can sort the events based on severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

### Advanced Search

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

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

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

- Specific events originating from or landing within United States

Source Country = United States OR Destination Country = United States AND Event Name = IDP\_ATTACK\_LOG\_EVENT, IDP\_ATTACK\_LOG\_EVENT\_LS, IDP\_APPDDOS\_APP\_ATTACK\_EVENT\_LS, IDP\_APPDDOS\_APP\_STATE\_EVENT, IDP\_APPDDOS\_APP\_STATE\_EVENT\_LS, AV\_VIRUS\_DETECTED\_MT, AV\_VIRUS\_DETECTED, ANTISPAM\_SPAM\_DETECTED\_MT, ANTISPAM\_SPAM\_DETECTED\_MT\_LS, FWAUTH\_FTP\_USER\_AUTH\_FAIL, FWAUTH\_FTP\_USER\_AUTH\_FAIL\_LS, FWAUTH\_HTTP\_USER\_AUTH\_FAIL, FWAUTH\_HTTP\_USER\_AUTH\_FAIL\_LS, FWAUTH\_TELNET\_USER\_AUTH\_FAIL, FWAUTH\_TELNET\_USER\_AUTH\_FAIL\_LS, FWAUTH\_WEBAUTH\_FAIL, FWAUTH\_WEBAUTH\_FAIL\_LS

- User wants to filter all RT flow sessions originating from IP addresses 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 IP addresses with or without specific destination IP addresses.

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

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

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

[Table 236 on page 638](#) describes the fields on the All Events Detail View Page.

Table 236: Fields on the All Events Detail View Page

Field	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Site	View the name of the tenant site.
Source Country	View the source country name.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack Name	View the attack name of the log: 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.
Action	View the action taken for the event: warning, allow, and 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 hostname in the log.

Table 236: Fields on the All Events Detail View Page (*continued*)

Field	Description
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role name associated with the log.
Reason	View the reason for the log generation. For example, a connection tear down may have an associated reason such as “authentication failed”.
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	View the name of the All events profile that triggered the event.

## RELATED DOCUMENTATION

---

[About the Firewall Events Page | 640](#)

---

[About the Web Filtering Events Page | 643](#)

---

[About the IPsec VPNs Events Page | 646](#)

---

[About the Content Filtering Events Page | 648](#)

---

[About the Antispam Events Page | 650](#)

---

[About the Antivirus Events Page | 652](#)

---

[About the IPS Events Page | 655](#)

---

## About the Firewall Events Page

To access this page, click **Monitor > Security Events > Firewall**.

Use the Firewall Events page to view information about security events based on firewall policies. Analyzing firewall logs yields useful security management information, such as attempts to breach your network and observing the inherent characteristics of your traffic in real-time. Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the firewall events in your network. See [“Summary View” on page 640](#)
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 641](#).

### Summary View

The data presented in the line graph (also known as swim lanes) is refreshed automatically based on the selected time range. The line graph shows light blue lanes that represent all firewall events and dark blue lanes represent blocked firewall events.

Below the swim lanes are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices.

[Table 237 on page 641](#) describes the widgets on the Summary View page.

**Table 237: Widgets on the Summary View Page**

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Users	View then top users of the network traffic; sorted by event count.
Top Reporting Devices	View the top reporting devices in the network; sorted by event count.

## Detail View

Detail view includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected

[Table 238 on page 641](#) provides guidelines on using the fields on the Detail View page.

**Table 238: Fields on the Detail View Page**

Field	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Policy Name	View the policy name in the log.

Table 238: Fields on the Detail View Page (*continued*)

Field	Description
User Name	View the username of the log.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Application	View the application name from which the events or logs are generated.
Hostname	View the hostname in the log.
Service Name	The name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the user traffic received from the zone.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role names associated with the event.
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.
Rule Name	View the rule name of the log.



## RELATED DOCUMENTATION

<a href="#">About the All Security Events Page   635</a>
<a href="#">About the Web Filtering Events Page   643</a>
<a href="#">About the IPsec VPNs Events Page   646</a>
<a href="#">About the Content Filtering Events Page   648</a>
<a href="#">About the Antispam Events Page   650</a>
<a href="#">About the Antivirus Events Page   652</a>
<a href="#">About the IPS Events Page   655</a>

## About the Web Filtering Events Page

To access this page, click **Monitor > Security Events > Web Filtering**.

Use the Web Filtering page to view information about security events based on Web filtering policies. Web filtering allows you to permit or block access to specific websites by URL or by URL category using cloud-based lookups, a local database, or an external Websense server. Analyzing Web filtering logs yields useful security management information such as users detected accessing restricted URLs and actions taken by the system. Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the Web filtering events in your network. See [“Summary View” on page 643](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 644](#).

### Summary View

The top of the page has a swim lane graph of all the Web filtering events against the blocked events.

Below the swim lanes are widgets displaying critical information such as top sources, top destinations, top users, and top reporting devices.

You can use the widgets at the bottom of the page to view critical information such as top URLs blocked, top matched profiles, top sources, and top destinations.

[Table 239 on page 644](#) describes the widgets on the Summary View page.

**Table 239: Widgets on the Summary View Page**

Widget	Description
Top URLs blocked	View the URL names that are blocked; sorted by event count.
Top Matched Profiles	View the web filtering profile names; sorted by event count.
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.

## Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 240 on page 644](#) provides guidelines on using the fields on the Detail View page.

**Table 240: Fields on the Detail View Page**

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.

Table 240: Fields on the Detail View Page (*continued*)

Fields	Description
Description	View the description of the log.
UTM category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
Path Name	View the path name of the log.
Profile Name	View the name of the Web filtering profile that triggered the event.

## RELATED DOCUMENTATION

[About the All Security Events Page | 635](#)
[About the Firewall Events Page | 640](#)
[About the IPsec VPNs Events Page | 646](#)
[About the Content Filtering Events Page | 648](#)
[About the Antispam Events Page | 650](#)
[About the Antivirus Events Page | 652](#)
[About the IPS Events Page | 655](#)

## About the IPsec VPNs Events Page

To access this page, click **Monitor > Security Events > IPsec VPNs**.

Use this page to view information about security events based on IPsec VPN policies. The event viewer provides a view of all IPsec VPN events.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the IPsec VPN events in your network. See [“Summary View” on page 646](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 647](#).

### Summary View

The top of the page has a swim lane graph of all the VPN events. You can use the widgets at the bottom of the page to view critical information such as top sources, top destinations, and top reporting devices.

[Table 241 on page 646](#) describes the widgets on the Summary View page.

**Table 241: Widgets on the Summary View Page**

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Reporting Devices	View the top reporting device IP addresses; sorted by event count.

## Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, log source, host name, source country, and so on.

[Table 242 on page 647](#) provides guidelines on using the fields on the Detail View page.

**Table 242: Fields on the Detail View Page**

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Destination Country	View the destination country name from where the event occurred.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Rule Name	View the name of the antivirus profile that triggered the event.

## RELATED DOCUMENTATION

[About the All Security Events Page | 635](#)

[About the Firewall Events Page | 640](#)

[About the Web Filtering Events Page | 643](#)

[About the Content Filtering Events Page | 648](#)

[About the Antispam Events Page | 650](#)

[About the Antivirus Events Page | 652](#)

[About the IPS Events Page | 655](#)

# About the Content Filtering Events Page

To access this page, click **Monitor > Security Events > Content Filtering**.

Use this page to view information about security events based on content filtering policies. The event viewer provides a view of all content filtering events and how the events are handled by content filter. This page can be used to view traffic on the network in real time or as a debugging tool to view how content filtering is operating.

Content filtering provides basic data loss prevention functionality. Content filtering screens traffic based on MIME type, file extension, protocol commands, and embedded object type. It either permits or blocks specific commands or extensions on a protocol-by-protocol basis.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the content filtering events in your network. See [“Summary View” on page 648](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 649](#).

## Summary View

The top of the page has a swim lane graph of all the content filtering events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources.

[Table 243 on page 648](#) describes the widgets on the Summary View page.

Table 243: Widgets on the Summary View Page

Widget	Description
Top Blocked Protocol commands	View the top command names or file extensions blocked on a protocol-by-protocol basis.
Top Reasons	View the top reasons for blocking the content. For example: Inappropriate or harmful communication.

Table 243: Widgets on the Summary View Page (*continued*)

Widget	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.

## Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 244 on page 649](#) provides guidelines on using the fields on the Detail View page.

Table 244: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access

Table 244: Fields on the Detail View Page (continued)

Fields	Description
Profile Name	View the name of the content filtering profile that triggered the event.

RELATED DOCUMENTATION

<a href="#">About the All Security Events Page   635</a>
<a href="#">About the Firewall Events Page   640</a>
<a href="#">About the Web Filtering Events Page   643</a>
<a href="#">About the IPsec VPNs Events Page   646</a>
<a href="#">About the Antispam Events Page   650</a>
<a href="#">About the Antivirus Events Page   652</a>
<a href="#">About the IPS Events Page   655</a>

## About the Antispam Events Page

To access this page, click **Monitor > Security Events > Antispam**.

Use this page to view information about security events based on antispam policies. The event viewer provides a view of all antispam events and the action taken by the antispam scanner.

The antispam scanner inspects and block spam by scanning inbound and outbound SMTP e-mail traffic. The filtering can be server-based using an external spam block list server or local-based using local lists (blocklists and allowlists) for matching.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the antispam events in your network. See [“Summary View” on page 651](#).



- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 651](#).

### Summary View

The top of the page has a swim lane graph of all antispam events. You can use the widget at the bottom of the page to view source IP addresses of the network traffic, sorted by event count.

### Detail View

You can aggregate the events using the Group by option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 245 on page 651](#) provides guidelines on using the fields on the Detail View page.

**Table 245: Fields on the Detail View Page**

Fields	Description
Time	View the time when the event occurred.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Argument	View the type of traffic. For example, FTP and HTTP.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.

Table 245: Fields on the Detail View Page (*continued*)

Fields	Description
Reason	View the reason for the log generation. For example, unrestricted access
Profile Name	View the name of the content filtering profile that triggered the event.

## RELATED DOCUMENTATION

[About the All Security Events Page | 635](#)

[About the Firewall Events Page | 640](#)

[About the Web Filtering Events Page | 643](#)

[About the IPsec VPNs Events Page | 646](#)

[About the Content Filtering Events Page | 648](#)

[About the Antivirus Events Page | 652](#)

[About the IPS Events Page | 655](#)

## About the Antivirus Events Page

To access this page, click **Monitor > Security Events > Antivirus**.

Use this page to view information about security events based on antivirus policies. The event viewer provides a view of all antivirus events and the action taken by the virus scanner.

The antivirus scanner inspects files transmitted over several protocols to determine if the files exchanged are malicious (for example, viruses, Trojans, rootkits, and worms).

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the Custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the antivirus events in your network. See [“Summary View” on page 653](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See “[Detail View](#)” on page 653.

Summary View

The top of the page has a swim lane graph of all the antivirus events against the blocked events. You can use the widgets at the bottom of the page to view critical information such as top blocked protocol commands, top reasons, and top sources.

[Table 246 on page 653](#) provides guidelines on using the widgets on the Detail View page.

Table 246: Widgets on the Summary Page

Field	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by event count.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by event count.
Top Reporting/Attacked Devices	View the top reporting/attacked device IP addresses; sorted by event count.
Top Viruses	View the top virus names detected; sorted by event count.
Top Source Countries	View the top source country names where the events originated; sorted by event count.
Top Destination Countries	View the top destination country names where the events occurred; sorted by event count.

Detail View

You can aggregate the events using the Group By option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 247 on page 653](#) provides guidelines on using the fields on the Detail View page.

Table 247: Fields on the Detail View Page

Fields	Description
Time	View the time when the event occurred.

Table 247: Fields on the Detail View Page (*continued*)

Fields	Description
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred (IPv4 or IPv6).
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event (IPv4 or IPv6).
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
UTM Category or Virus Name	View the UTM category of the log: enhanced, local, and redirect.
URL	View the accessed URL name that triggered the event.
Action	View the action taken for the event: warning, allow, and block.
Log Source	View the IP address of the log source (IPv4 or IPv6).
Host Name	View the hostname in the log.
Source Zone	View the user traffic received from the zone.
Roles	View the role names associated with the event.
Reason	View the reason for the log generation. For example, unrestricted access.
Profile Name	View the name of the antivirus profile that triggered the event.

## RELATED DOCUMENTATION

[About the All Security Events Page | 635](#)
[About the Firewall Events Page | 640](#)

[About the Web Filtering Events Page | 643](#)

[About the IPsec VPNs Events Page | 646](#)

[About the Content Filtering Events Page | 648](#)

[About the Antispam Events Page | 650](#)

[About the IPS Events Page | 655](#)

## About the IPS Events Page

To access this page, click **Monitor > Security Events > IPS**.

Use the IPS Events page to view information about security events based on IPS policies. Analyzing IPS logs yields useful security management information, such as abnormal events, attacks, viruses, or worms.

Using the time-range slider, you can quickly focus on the area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the custom button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the all the IPS events in your network. See [“Summary View” on page 655](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 656](#).

### Summary View

The data presented in the area graph is refreshed automatically based on the selected time range. You can use widgets to view critical information such as IPS severities, top sources, top destinations, top reporting devices, top IPS attacks, top source countries, and top destination countries.

[Table 248 on page 655](#) provides guidelines on using the widgets on the Detail View page.

**Table 248: Widgets on the Summary Page**

Field	Description
IPS Severities	View the top IPS severities of the events based on the severity level: high, medium, low.

Table 248: Widgets on the Summary Page (continued)

Field	Description
Top Sources	View the top source IP addresses of the network traffic; sorted by the number of event occurrences.
Top Destinations	View the top destination IP addresses of the network traffic; sorted by the number of event occurrences.
Top Reporting/Attacked Devices	View the top devices that are attacked by IPS events; sorted by the number of times users are active on the network.
Top IPS attacks	View the top IPS attacks in the network traffic; sorted by the times devices are attacked.
Top Source Countries	View the top source countries from where the event source originated; sorted by the number of IP addresses.
Top Destination Countries	View the top source countries from where the event source originated; sorted by the number of IP addresses.

## Detail View

You can sort the events using the Group By option. For example, you can sort the events based on severity. The table includes information such as the rule that caused the event, severity for the event, event ID, traffic information, and how and when the event was detected.

[Table 249 on page 656](#) provides guidelines on using the fields on the Detail View page.

Table 249: Fields on the Detail View Page

Column	Description
Time	View the time when the log was received.
Event Name	View the event name of the log.
Source Country	View the source country name from where the event originated.
Source IP	View the source IP address from where the event occurred.
Destination Country	View the destination country name from where the event occurred.
Destination IP	View the destination IP address of the event.

Table 249: Fields on the Detail View Page (*continued*)

Column	Description
Source Port	View the source port of the event.
Destination Port	View the destination port of the event.
Description	View the description of the log.
Attack name	View the attack name of the log: Trojan, worm, virus, and so on.
Threat Severity	View the threat severity of the event.
Policy Name	View the policy name in the log.
Action	View the action taken for the event: warning, allow, and 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 name in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
NAT Source Port	View the translated source port.
NAT Destination Port	View the translated destination port
NAT Source IP	View the NAT source IP address of the log.
NAT Destination IP	View the NAT destination IP address of the log.
Rule Name	View the name of the rule.

## RELATED DOCUMENTATION

<a href="#">About the All Security Events Page   635</a>
<a href="#">About the Firewall Events Page   640</a>
<a href="#">About the Web Filtering Events Page   643</a>
<a href="#">About the IPsec VPNs Events Page   646</a>
<a href="#">About the Content Filtering Events Page   648</a>
<a href="#">About the Antispam Events Page   650</a>
<a href="#">About the Antivirus Events Page   652</a>

## About the Device Events Page

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

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

You can view comprehensive details of device events in a tabular format that includes sortable columns and a line graph (also known as swim lanes). The data presented in the line graph is refreshed automatically based on the selected time range. The line graph shows light blue areas that represent all device events and dark blue areas represent blocked device events

### Tasks You Can Perform

You can perform the following tasks from this page:

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

### Advanced Search

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

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

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



- Specific events originating from or landing within United States

Source Country = United States OR Destination Country = United States AND Event Name = IDP\_ATTACK\_LOG\_EVENT, IDP\_ATTACK\_LOG\_EVENT\_LS, IDP\_APPDDOS\_APP\_ATTACK\_EVENT\_LS, IDP\_APPDDOS\_APP\_STATE\_EVENT, IDP\_APPDDOS\_APP\_STATE\_EVENT\_LS, AV\_VIRUS\_DETECTED\_MT, AV\_VIRUS\_DETECTED, ANTISPAM\_SPAM\_DETECTED\_MT, ANTISPAM\_SPAM\_DETECTED\_MT\_LS, FWAUTH\_FTP\_USER\_AUTH\_FAIL, FWAUTH\_FTP\_USER\_AUTH\_FAIL\_LS, FWAUTH\_HTTP\_USER\_AUTH\_FAIL, FWAUTH\_HTTP\_USER\_AUTH\_FAIL\_LS, FWAUTH\_TELNET\_USER\_AUTH\_FAIL, FWAUTH\_TELNET\_USER\_AUTH\_FAIL\_LS, FWAUTH\_WEBAUTH\_FAIL, FWAUTH\_WEBAUTH\_FAIL\_LS

- User wants to filter all RT flow sessions originating from IPs in specific countries and landing on IPs in specific countries

Event Name = RT\_FLOW\_SESSION\_CREATE, RT\_FLOW\_SESSION\_CLOSE AND Source IP = 177.1.1.1, 220.194.0.150, 14.1.1.2, 196.194.56.4 AND Destination IP = 255.255.255.255, 10.207.99.75, 10.207.99.72, 223.165.27.13 AND Source Country = Brazil, United States, China, Russia, Algeria AND Destination Country = Germany, India, United States

- Traffic between zone pairs for policy – IDP2

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

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

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

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

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

## Field Descriptions

[Table 250 on page 659](#) provides guidelines on using the fields on the Device Events page.

**Table 250: 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.
Site	View the name of the tenant site.

Table 250: Fields on the Device Events Detailed View Page (*continued*)

Field	Description
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 hostname in the log.
Service Name	View the name of the application service. For example, FTP, HTTP, SSH, and so on.

Table 250: Fields on the Device Events Detailed View Page (*continued*)

Field	Description
Nested Application	View the nested application in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role name associated with the log.
Reason	View the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
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.

## RELATED DOCUMENTATION

| [About the All Security Events Page](#) | 635

## About the Screen Events Page

To access this page, click **Monitor > Security Events > Screen**.

Use this page to view information about screen events that occur as a result of the screen options configured on SRX Series or vSRX security devices. Screen options are a detection and defense mechanism configured to filter the connection attempts bound towards a security zone. Screen options are used to prevent attacks, such as IP address sweeps, port scans, denial of service (DOS) attacks, Internet Control Message Protocol (ICMP), UDP, and SYN (Synchronize) floods.

You can view information related to screen events, including ICMP screening, IP screening, TCP screening, and UDP screening.

Using the time-range slider, you can quickly focus on the time and area of activity that you are most interested in. Once the time range is selected, all of the data presented in your view is refreshed automatically. You can also use the **Custom** button to set a custom time range.

There are two ways to view your data. You can select either the **Summary View** tab or the **Detail View** tab.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View a brief summary of all the screen events in your network. See [“Summary View” on page 662](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 663](#).

### Summary View

The top of the page has a swim lane graph of all the screen events. You can use the widgets at the bottom of the page to view critical information such as, top sources, top source countries, top destinations, and top destination countries.

[Table 251 on page 663](#) describes the widgets on the Detail View page.

Table 251: Widgets on the Summary Page

Field	Description
Top Sources	Top five source IP addresses with highest network traffic.
Top Destinations	Top five destination IP addresses with highest network traffic.
Top Source Countries	Top five countries from which the traffic that triggered the highest number of events originated and the number of events per country.
Top Destination Countries	Top five countries to which the traffic that triggered the highest number events was sent and the number of events per country.

## Detail View

You can group the events using the **Group By** option. For example, you can group the events based on source country. The table includes information such as the event name, UTM category, source IP address, source country, and so on.

[Table 252 on page 663](#) describes the fields on the Detail View page.

Table 252: Fields on the Detail View Page

Fields	Description
Log Generated Time	Time when the event occurred.
Log Received Time	Time the log was received at the log collector.
Site	Name of the tenant site from which the event originated.
Event Name	Name of the device event in the log.
Source Country	Country from which the traffic that triggered the event originated.
Source IP	Source IP address for the traffic that triggered the event (IPv4 or IPv6).
Destination Country	Country to which the traffic that triggered the event was sent.
Destination IP	Destination IP address for the traffic that triggered the event (IPv4 or IPv6).
Source Port	Source TCP/UDP port number of the traffic that triggered the event.
Destination Port	Destination TCP/UDP port number of the traffic that triggered the event.

Table 252: Fields on the Detail View Page (*continued*)

Fields	Description
Attack Name	Name of the attack in the log for threat event. For example, trojan, worm, virus, and so on.
Description	Brief description of the event.
Threat Severity	Level of severity of the threat. For example, minor, major, critical, and so on.
Policy Name	Name of the policy which generates the log. The policy is configured on the SRX Series or vSRX device.
Virus Name	This field is not applicable for screen events.
URL	Accessed URL that triggered the event.
Event Category	Event category in the log. For example, screen.
User Name	User name identified by the SRX Series or vSRX device, if user identity is enabled on the device.
Argument	Type of traffic. For example, FTP and HTTP.
Action	Action taken for the event. For example, warning, allow, and block.
Log Source	IP address of the device where the log is received (IPv4 or IPv6).
Application	Name of the application associated with the traffic that triggered the event.
Host Name	Hostname of the device where the log was generated.
Service Name	Name of the application service used for the traffic that triggered the event. For example, FTP, HTTP, SSH, and so on.
Nested Application	Nested application associated with the traffic that triggered the event.
Source Zone	Source security zone of the traffic that triggered the event.
Destination Zone	Destination security zone of the traffic that triggered the event.
Protocol ID	Protocol ID of the traffic that triggered the event.
Roles	Roles of the user as defined in the Active Directory, if available.

Table 252: Fields on the Detail View Page (*continued*)

Fields	Description
Reason	Reason for the log generation. For example, unrestricted access.
NAT Source Port	Translated source port.
NAT Destination Port	Translated destination port.
NAT Source Rule Name	NAT source rule name configured on the SRX Series or vSRX device.
NAT Destination Rule Name	NAT destination rule name configured on the SRX Series or vSRX device.
NAT Source IP	Translated source IP address for the traffic that triggered the event (IPv4 or IPv6).
NAT Destination IP	Translated destination IP address for the traffic that triggered the event (IPv4 or IPv6).
Traffic Session ID	Traffic session ID of the log.
Path Name	This field is not applicable for screen events.
Logical System Name	Name of the logical system which received the log.
Rule Name	Name of the rule which generates the log. This rule is configured on the SRX Series or vSRX device.
Profile Name	Name of the profile which filters the traffic that triggered the event.
Client Host Name	Hostname of the client associated with the traffic that triggered the event. For example, if a specific computer is infected, the name of that computer is displayed.
Malware info	Information about the malware causing the event.

## RELATED DOCUMENTATION

[About the All Security Events Page | 635](#)
[About the Firewall Events Page | 640](#)
[About the Web Filtering Events Page | 643](#)

[About the IPsec VPNs Events Page | 646](#)

---

[About the Content Filtering Events Page | 648](#)

---

[About the Antispam Events Page | 650](#)

---

[About the Antivirus Events Page | 652](#)

---

[About the IPS Events Page | 655](#)



# Monitoring SD-WAN Events

## IN THIS CHAPTER

- [SD-WAN Events Overview | 667](#)
- [About the SD-WAN Events Page | 668](#)

## SD-WAN Events Overview

Service-level agreements (SLAs) define the expected class of service (CoS) for all applications and application groups in a site. The network operator needs tools to measure and monitor the performance metrics for all applications to determine the quality of the network and adherence to an assured CoS. To ensure compliance with SLAs, the network operator also needs tools to take remedial action when network performance deteriorates and SLAs are not being met. SD-WAN link-switch events enable the network to switch WAN links to meet the site's SLA requirements when the network-designated WAN link is unable to meet the site's SLA requirements.

Because SLA parameters override the path preference, in dynamic SD-WAN policies, the SD-WAN network chooses the best possible WAN link for traffic management. The WAN link is chosen is based on the SLA parameters defined in the SLA profile. If multiple links match the SLA profile, the least loaded link is chosen. When a policy intent is deployed on a site, if the WAN link chosen by the SD-WAN network is unable to meet the SLA requirements in runtime, then the site switches WAN links to meet the SLA requirements. This link switching is called an SD-WAN event. Link switching also takes into account the priority defined in the SLA profile and SLA profiles with higher priority are given precedence while finding alternate WAN links. The ability of a site to switch WAN links ensures that SLA requirements are met and instances of not meeting the SLA requirements are minimized.

In static policies, link switching cannot occur even if the designated WAN link is unable to meet the SLA requirements, because path preference is defined.

## RELATED DOCUMENTATION

[About the SD-WAN Events Page | 668](#)

[SLA Profiles and SD-WAN Policies Overview | 406](#)

# About the SD-WAN Events Page

To access this page, click **Monitor > Link Switch Events** in the Customer Portal.

You can use the SD-WAN Events page to view information about SD-WAN events. An SD-WAN event is triggered when the SLA requirements for a site are not met on its network-designated WAN link and the site switches WAN links to meet the SLA requirements.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View a graphical representation of SD-WAN events in a specified time range (Time Range widget)  
The x-axis represents the defined time and the y-axis represents number of SD-WAN events.  
Use the slider to decrease or increase the time range within which you want to view SD-WAN events. You can also select from pre-defined time ranges such as 2h, 4h, 8h, 16h, 24h, or Custom.  
If you select Custom, you must specify the dates and times (in MM/DD/YYYY and HH:MM:SS 24-hour or AM/PM formats) from when and up to when you want the SD-WAN events displayed.
- View the SD-WAN events that occurred and information related to the events; see [Table 253 on page 669](#).
- Show or hide the columns displayed on the page—Click the Show Hide Columns icon at the top right corner of the page and select the columns that you want displayed in the grid.
- Sort and filter SD-WAN events:

**NOTE:** Sorting and filtering is applicable only to some fields.

- Click a column name to sort the SD-WAN events based on the column name.
- Click the filter icon (funnel) to toggle the filtering. You can enter the filter parameters in one or more fields and press Enter to display the filtered results.
- Search for SD-WAN events 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 253 on page 669](#) describes the fields on the SD-WAN Events page.

Table 253: Fields on the SD-WAN Events Page

Field	Description
Time Range	<p>View a graphical representation of SD-WAN events against a defined time range. The x-axis represents the defined time and the y-axis represents SD-WAN events.</p> <p>Use the slider to decrease or increase the time range within which you want to view SD-WAN events. You can also choose from pre-defined time ranges such as 2h, 4h, 8h, 16h, 24h, or 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.</p>
SLA Violation Time	Date and time at which the SLA violation occurred.
Link Switch Time	Date and time at which the link was switched.
Site	Name of the site for which the link was switched.
Connected To	Displays the name of the destination spoke or hub site to which the traffic is being sent.
SLA Profile	Name of the SLA-based steering profile associated with the site.
Reason	<p>Indicates the reason for the link switch.</p> <p>Mouse over the reason to view details of the SLA metrics violated.</p>
Apps	Name of the applications for which the SLA violation occurred.
Department	Name of the department for which the SLA violation occurred.
Source Tunnel	Overlay tunnel of the device <i>from</i> which the link switch took place.
Destination Tunnel	Overlay tunnel of the device <i>to</i> which the link switch took place.
Duration (Sec)	<p>Duration (in seconds) for which the SLA requirement for a site was not met before the site switched WAN links.</p> <p>A duration of 0 indicates that the site switched WAN links before it failed to meet the SLA requirements, and the SLA requirements were met immediately on the new WAN link with no loss in meeting SLA requirements.</p>

## RELATED DOCUMENTATION

[SD-WAN Events Overview](#) | 667

# Monitoring Applications

## IN THIS CHAPTER

- [About the SLA Performance of a Single Tenant Page | 670](#)
- [Viewing the SLA Performance of a Site | 673](#)
- [Viewing the SLA Performance of an Application or Application Group | 677](#)
- [Application Visibility Overview | 679](#)
- [About the Application Visibility Page | 679](#)
- [About the User Visibility Page | 683](#)
- [Viewing Application or User Visibility Data for Specific Sites | 686](#)

## About the SLA Performance of a Single Tenant Page

To access this page, select **Monitor > Application SLA Performance > *Tenant-Name* SLA Performance** in the Customer Portal.

You can use the *Tenant-Name* SLA Performance page to view performance reports for all sites in a tenant. You can view the SLA performance of all sites that have met and all the sites that have not met the defined SLA target values for the specified time range. You can customize your view and also the time range for which you want to view the SLA performance.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View the SLA performance for all sites in the tenant that have met the defined SLA target values, without switching WAN links, for the specified time range.
- View the SLA performance for all sites in the tenant that have met the defined SLA target values, after switching WAN links, for the specified time range.
- View the SLA performance for all sites in a tenant that have not met the defined SLA target values for the specified time range.
- View the SLA performance for all sites in a tenant in grid or card views.

Select card view or grid view at the top right of the page. By default, card view is selected.

- Customize the time range to view the SLA performance for all sites in a tenant.
- View the SLA performance for multiple departments within a single tenant.

Select the specific department for which you want to view the SLA performance from the drop-down list at the top right of the page.

## Field Descriptions

Table 254 on page 671 describes the fields on the *Tenant-Name* SLA Performance page.

**Table 254: Fields on the SLA Performance of a Single Tenant Page**

Field	Description
Time range	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, <b>Previous 1 day</b> is selected.
View	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.
Sites Not Meeting SLAs	<p>The sites that did not meet the defined SLA target values in the selected time range.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See <a href="#">“Viewing the SLA Performance of a Site” on page 673</a>.</p>
Sites Meeting SLAs With Switch	<p>The sites that switched WAN links to meet the defined SLA target values in the selected time range.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See <a href="#">“Viewing the SLA Performance of a Site” on page 673</a>.</p>
Sites Meeting SLAs Without Switch	<p>The sites that met the defined SLA target values in the selected time range without switching WAN links.</p> <p>Click each site to view more information about the SLA performance of the applications and application groups in the site. See <a href="#">“Viewing the SLA Performance of a Site” on page 673</a>.</p>

Table 255 on page 672 describes the fields in the card and grid views.

**Table 255: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views**

Field	View	Description
Name	Card and Grid	View the name of the site.
SLA not met (Time)	Card and Grid	View the average time (in %) during which all the sites in a tenant did not meet the defined SLA target values.
Profiles	Card	View the time (in %) during which defined SLA target values were not met for each SLA profile. The top two profiles with highest priority and the percentage of time during which SLA target values were not met are listed. The remaining profiles and their combined sum of time (in %) for which SLA target values were not met are listed under <b>Others</b> . The SLA profile priority is indicated inside a circle. You can define priority of the SLA profile when you create an SLA profile.  Hover over the profile priority to view the SLA profile name.
Profile SLA Not Met	Grid	
App - Groups	Card and Grid	View the total number of applications and application groups in the site.
Switch Events	Card and Grid	View the number of times the site switched WAN links over the number of designated WAN links. A switch event, also called SD-WAN event, occurs when a site switches WAN links to meet the SLA requirements.
Switch Events Per Profile	Card and Grid	View the number of times the site switched WAN links for each profile. You can view the switch events for the top two SLA profiles in the decreasing order of switch events for each profile.

## RELATED DOCUMENTATION

[Viewing the SLA Performance of a Site | 673](#)

[Viewing the SLA Performance of an Application or Application Group | 677](#)

[SD-WAN Events Overview | 667](#)

[Adding SLA-Based Steering Profiles | 424](#)

[Adding Path-Based Steering Profiles | 435](#)

## Viewing the SLA Performance of a Site

### IN THIS SECTION

- [SLA Not Met by SLA Profiles | 673](#)
- [Applications SLA Performance by Throughput | 674](#)
- [SLA Performance for ALL | 676](#)

You can use the **Monitor > Applications > Tenant\_name SLA Performance > Site\_name SLA Performance** page in the Customer Portal to view the 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 sections:

### SLA Not Met by SLA Profiles

You can use the **SLA Not Met by SLA Profiles** section on the **Site\_name SLA Performance** page to view the SLA profiles for which SLA requirements were not met and the time at which they were not met. The y-axis represents the SLA profiles and the x-axis represents the specified time range. The **SLA Not Met by SLA Profiles** section can be viewed and remains the same in both graph and grid views.

To view a graphical representation of SLA profiles for which SLA target values were not met:

1. Select the time range for which you want to view the SLA profiles for which SLA target values were not met. You can choose from Previous 1 hour, Previous 1 day, Previous 1 week, Previous 1 month, and Custom. For custom time, you must enter from and to dates in MM/DD/YYYY format and the time in HH:MM:SS format. By default, Previous 1 day is selected.

The graphical representation of SLA profiles for which SLA target values were not met is displayed for the selected time range.

2. (Optional) You can use the sliders at the sides of the graph to further customize the time range.

The graphical representation of SLA profiles for which SLA target values were not met is refreshed and displayed for the customized time range. The graphical representation of SLA performance data in the subsequent sections on the page is also refreshed and displayed for the customized time range.

## Applications SLA Performance by Throughput

You can use the **Applications SLA Performance by Throughput** section on the **Site\_name SLA Performance** page to view average throughput performance of all applications and application groups in a site. You can also customize your view by selecting graph or grid views. In the graph view, you can further select scatter plot or tree map.

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 and 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 677](#).
5. 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 256 on page 675](#) describes the fields on the Applications SLA Performance by Throughput grid view.

**Table 256: Fields on the Applications SLA Performance by Throughput Grid View**

Field	Description
Name	View name of the application or application group.
SLA Profile	View the SLA profile associated with the application or application group.
Type	View the type—application or application group
Category	View the category of the application or application group. The value of Category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on.
Sessions	View 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 information about the application or application group. See [“Viewing the SLA Performance of an Application or Application Group” on page 677](#).

## 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* page.

## RELATED DOCUMENTATION

[About the SLA Performance of a Single Tenant Page](#) | 670

## Viewing the SLA Performance of an Application or Application Group

You can use the **Monitor > Applications > Tenant-Name SLA Performance > Site-Name SLA Performance** page in the Customer Portal to view the SLA performance for 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 257 on page 677](#) describes the fields on the application or application group SLA Performance details page.

**Table 257: 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 throughput performance (in %) above or below the configured target throughput. The average throughput (in Mbps) is displayed within parentheses.
SLA Metrics by Throughput	View a graphical representation of the SLA metrics by throughput during the specified time range for that application or application group. The y-axis represents the throughput (in Mbps). The x-axis represents the specified time range. Hover over the graph to view the throughput value and time at any specified point. You can also view the sessions consumed by the WAN links for the application or application group time range.

Table 257: Fields on the Application or Application Group Details Page (*continued*)

Field	Description
Global SLA Profile Performance	<p>View the performance for all the SLA parameters of the SLA profile associated with the application or application group. The SLA performance is represented by a color-coded donut chart. The section in blue in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were met. The section in red in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were not met.</p> <p>Click the red colored section of the donut chart to view more information about when SLA requirements for the SLA profile were not met. The <b>SLA Profile Performance</b> page appears. The SLA Profile Performance page displays the following fields:</p> <ul style="list-style-type: none"> <li>• SLA Profile—SLA profile associated with the application or application group</li> <li>• Target—Target throughput configured in the SLA profile</li> <li>• SLAs Not Met—Percentage of time SLA requirements were not met for the SLA profile</li> <li>• Sessions—Number of sessions consumed by the application or application group</li> <li>• Start Time—Time at which the WAN links associated with the application or application groups started to fail meeting the SLA requirements</li> <li>• End Time—Time at which SLA profile requirements started to be met again</li> <li>• Avg Val—Average throughput (in Mbps) when the SLA requirements started to fail</li> <li>• Duration—Total duration (in seconds) during which SLA requirements were not met</li> <li>• From—Source WAN link</li> <li>• To—Destination WAN link</li> </ul>

## RELATED DOCUMENTATION

[About the SLA Performance of a Single Tenant Page | 670](#)

[Viewing the SLA Performance of a Site | 673](#)

## Application Visibility Overview

You can use the **Application Visibility** page to view information about bandwidth consumption, session establishment, and the risks associated with your applications.

Analyzing your network applications yields useful security management information, such as abnormal applications that can lead to data loss, heavy bandwidth usage, time-consuming applications, and personal applications that can elevate business risks.

### RELATED DOCUMENTATION

[About the Application Visibility Page | 679](#)

[Viewing Application or User Visibility Data for Specific Sites | 686](#)

## About the Application Visibility Page

To access this page, select **Monitor > Applications > Visibility**.

There are two ways in which you can view your application visibility data—**Chart View** or **Grid View**. By default, the data is displayed in **Chart View**.

### Tasks You Can Perform

You can perform the following tasks from this page:

- View application visibility data in **Chart View**. See [“Chart View” on page 679](#).
- View application visibility data in **Grid View**. See [“Grid View” on page 681](#).
- Select a device to which the application visibility settings are applicable. See [“Viewing Application or User Visibility Data for Specific Sites” on page 686](#).

### Chart View

Click the **Chart View** link for a brief summary of the top 50 applications consuming the maximum bandwidth in your network. The data can be presented graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time range. You can also use the **Custom** button to set a custom time range.

You can hover over your applications to view critical information such as total number of sessions, total number of blocks, category, bandwidth consumed, risk levels, and characteristics. You can also view the top five users accessing your application.

[Table 258 on page 680](#) provides guidelines on using the fields on the **Chart View** of the **Application Visibility** page.

**Table 258: Fields on the Chart View**

Field	Description
All Devices	Displays application visibility data for all the sites managed by CSO. Click <b>Edit</b> to select individual devices for which you want to view the data.
Show By	<p>Select from the following options to view a user's data:</p> <ul style="list-style-type: none"> <li>• Bandwidth—Shows data based on the amount of bandwidth the application has consumed for a particular time range.</li> <li>• Number of Sessions—Shows data based on the number of sessions consumed by the application.</li> </ul>
Time Span	<p>Select the required time range to view a user's data.</p> <p>Use the custom option to choose the time range if you want to view data for more than one day. The time range is from 00:00 through 23:59.</p>
Select graph	<p>Select from the following graphical representations to view an application's data:</p> <ul style="list-style-type: none"> <li>• Bubble Graph</li> <li>• Heat Map</li> <li>• Zoomable Bubble Graph</li> </ul> <p>By default, data is shown in the Bubble Graph format.</p>
Group By	<p>Select from the following options to view the application's data:</p> <ul style="list-style-type: none"> <li>• Risk—Grouped by critical, high, unsafe, and so on.</li> <li>• Category—Grouped by categories such as web, infrastructure, and so on.</li> </ul>
Number of Sessions	Displays the total number of application sessions.
Number of Blocks	Displays the total number of times the application was blocked.
Bandwidth	Displays the bandwidth usage of the application.
Risk Level	Displays the risk associated with the application. For example, critical, high, unsafe, and so on.
Category	Displays the category of the application. For example, web, infrastructure, and so on.

Table 258: Fields on the Chart View *(continued)*

Field	Description
Characteristics	Displays the characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling, and so on.

## Grid View

Click the **Grid View** link to obtain comprehensive details about applications. You can view top users by volume, top applications by volume, top category by volume, top characteristics by volume, and sessions by risk. You can also view the data in a tabular format that includes sortable columns. You can sort the applications in ascending or descending order based on application name, risk level, and so on.

[Table 259 on page 681](#) describes the widgets in this view. Use these widgets to get an overall, high-level view of your applications, users, and the content traversing your network.

[Table 259 on page 681](#) provides guidelines on using the fields on the **Grid View** of the **Application Visibility** page.

Table 259: Widgets on the Grid View

Field	Description
Top Users By Volume	Top users of the application; sorted by bandwidth consumption.
Top Apps By Volume	Top applications using the network traffic, such as Amazon, Facebook, and so on, sorted by bandwidth consumption.
Top Category By Volume	The top category of the application, such as Web, infrastructure, and so on; sorted by bandwidth consumption.
Top Characteristics By Volume	Top behavioral characteristics of the application, such as whether it is highly prone to misuse, the top bandwidth consumer, and so on.
Sessions By Risk	Number of events or sessions received; grouped by risk.

[Table 260 on page 682](#) describes the fields in the table below the widgets. Users are displayed by usernames or IP addresses. When you click a link, the **User Visibility** page appears in a grid view, with the correct filter applied. Sessions are also displayed as links and when you click a link, the **All Events** page appears with all security events.

Table 260: Detailed View of Applications

Field	Description
Application Name	Name of the application, such as Amazon, Facebook, and so on.
Risk Level	Risk associated with the application: critical, high, unsafe, moderate, low, and unknown.
Users	Total number of users accessing the application.
Volume	Bandwidth used by the application.
Total Sessions	Total number of application sessions.
No of Rejects	Total number of sessions blocked.
Category	Category of the application, such as Web, infrastructure, and so on.
Sub Category	Subcategory of the application. For example, social networking, news, and advertisements.
Characteristics	Characteristics of the application. For example, prone to misuse, bandwidth consumer, capable of tunneling.

## RELATED DOCUMENTATION

[Application Visibility Overview | 679](#)
[Viewing Application or User Visibility Data for Specific Sites | 686](#)
[About the SLA Performance of a Single Tenant Page | 670](#)



# About the User Visibility Page

To access this page, select **Monitor > User Visibility**.

Use the User Visibility page to view information about devices (such as top 50 devices accessing high bandwidth-consuming applications and establishing higher number of sessions) on your network. Based on this information, network administrators can choose to rate-limit a device that is accessing applications which consume large bandwidth or create maximum traffic.

## Tasks You Can Perform

You can perform the following tasks from this page:

- View user visibility data in **Chart View**. See [“Chart View” on page 683](#).
- View user visibility data in **Grid View**. See [“Grid View” on page 685](#).
- Select one or more sites for which you want to view the user visibility data. See [“Viewing Application or User Visibility Data for Specific Sites” on page 686](#).

## Chart View

Click the **Chart View** tab to view the data graphically as a bubble graph, heat map, or a zoomable bubble graph. The data is refreshed automatically based on the selected time span.

You can hover over the chart to view critical information (such as the total number of sessions established and bandwidth consumed) about each user.

Users are represented by the IP address or usernames of their devices on the network.

You can also view the top five applications of each user, based on either their bandwidth consumption or number of sessions established.

[Table 261 on page 683](#) provides guidelines on using the fields on the **Chart View** tab of the **User Visibility** page.

Table 261: Fields on the Chart View

Field	Description
All Sites	<p>By default, the chart displays user visibility data for all the sites managed by CSO.</p> <p>Click <b>Edit</b> to select one or more sites for which you want to view the user visibility data.</p> <p>See <a href="#">“Viewing Application or User Visibility Data for Specific Sites” on page 686</a> for more information.</p>

Table 261: Fields on the Chart View *(continued)*

Field	Description
Show By	<p>Select the criterion to display information regarding the bandwidth consumed and number of sessions established by applications in the selected time span:</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth</b>—Displays users based on their bandwidth consumption. Users running applications that consume larger bandwidth are represented by larger bubbles or matrices.</li> <li>• <b>Number of Sessions</b>—Displays users based on the number of sessions established. Users running applications that have higher number of sessions established are represented by larger bubbles or matrices.</li> </ul>
Time Span	<p>Select the duration (last 15 minutes, last 30 minutes, last 45 minutes, last 1 hour, last 4 hours, last 8 hours, last 12 hours, last 1 day, or custom) for which you want to view the user visibility data.</p> <p>Select <b>Custom</b> to view data for more than one day.</p> <p>The <b>Custom Time</b> page appears.</p> <p>Specify the <b>From date</b> and <b>To date</b> (in MM/DD/YYYY format). The time span is from 00:00 through 23:59.</p>
Select Graph	<p>Select one of the following options to view data graphically:</p> <ul style="list-style-type: none"> <li>• Bubble Graph (default)</li> <li>• Heat Map</li> <li>• Zoomable Bubble Graph</li> </ul>

[Table 262 on page 684](#) describes the parameters that are displayed when you hover your cursor over the chart.

Table 262: Parameters on the Chart

Parameter	Description
Number of Sessions	Total number of application sessions established by the user (device).
Bandwidth	Total Bandwidth consumed by the user (device).
View All Applications	<p>Click the <i>View All Applications</i> link to view details (such as risk level and category) of all the applications on the network.</p> <p>The Application Visibility page in grid view appears. See <a href="#">“About the Application Visibility Page” on page 679</a> for more information.</p>

## Grid View

Click the **Grid View** tab to view high-level details of the users on your network. You can view widgets that provide information about top users by volume and top applications that create network traffic by volume. The data is also displayed in a tabular format with sortable columns.

[Table 259 on page 681](#) describes the widgets on the **Grid View** of the **User Visibility** page.

**Table 263: Widgets on the Grid View**

Field	Description
Top Users by Volume	Top users of applications, based on bandwidth consumption, for the selected time span.
Top Apps by Volume	Top applications accessed by users on the network, based on bandwidth consumption, for the selected time span.  For example: Amazon

[Table 264 on page 685](#) describes the fields in the table below the widgets.

The table includes sortable columns, with the users (devices) represented by usernames or IP addresses.

Click the Search icon to enter the search text that can include a specific application or user name, or IP address of a device on the network.

The search results are displayed. Click **Clear All** to clear the search results.

**Table 264: Detailed View of Users**

Field	Description
Applications	Name of the application accessed by a specific user (device).  For example: Google  <b>NOTE:</b> By default, this column lists only one application per user. If a user accesses more than one application, a +<integer>icon (for example: +2) appears to the right of the application name. The integer indicates the number of additional applications accessed by the user. Click the integer to view all applications accessed by a user.
User Name	IP address or username of the user (device) accessing the applications.
Volume	Bandwidth consumed by a user (who is represented by a user name or IP address).
Total Sessions	Total number of application sessions established by a specific user (device).

## Viewing Application or User Visibility Data for Specific Sites

### IN THIS SECTION

- [Viewing Application Visibility Data for Specific Sites | 686](#)
- [Viewing User Visibility Data for Specific Sites | 687](#)

You can select one or more sites for which you want to view application visibility or user visibility data (such as bandwidth consumption and number of sessions). By default, the application visibility and user visibility data is displayed for all sites in a tenant.

### Viewing Application Visibility Data for Specific Sites

To select the sites for which you want to view the application visibility data:

1. Select **Monitor > Application Visibility**.

The **Application Visibility** page appears.

2. Click the **Edit** link (next to the Show By field).

The **Select Sites** page appears.

3. From the Sites field:

- Click **Selective** to select the sites for which you want to view the application visibility data:

The available sites are displayed in the **Available** column.

- Click **All** to view application visibility data for all sites in the tenant.

If you click All, proceed to step [5](#).

4. Select the sites from the **Available** column and click the right arrow to move them to the **Selected** column.

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

You are returned to the Application Visibility page and the application visibility data is displayed for the sites that you selected.

To view application visibility data for other sites, repeat step [2](#).

## Viewing User Visibility Data for Specific Sites

To select the sites for which you want to view the user visibility data:

1. Select **Monitor > User Visibility**.

The **User Visibility** page appears.

2. Click the **Edit** link (next to the Show By field).

The **Select Sites** page appears.

3. From the Sites field:

- Click **Selective** to select the sites for which you want to view the user visibility data.

The available sites are displayed in the **Available** column.

- Click **All** to view user visibility data for all sites in the tenant.

If you click All, proceed to step [5](#).

4. Select the sites from the **Available** column and click the right arrow to move them to the **Selected** column.

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

You are returned to the User Visibility page and the user visibility data is displayed for the sites that you selected.

To view user visibility data for other sites, repeat step [2](#).

# Monitoring Threats

## IN THIS CHAPTER

- [About the Threats Map \(Live\) Page | 688](#)

## About the Threats Map (Live) Page

## IN THIS SECTION

- [Tasks You Can Perform | 689](#)
- [Field Descriptions | 690](#)
- [Threat Types | 691](#)

To access this page, select **Monitor > Threats Map (Live)** in Customer Portal.

Use this page to visualize incoming and outgoing threats between geographic regions. You can view blocked and allowed threat events based on feeds from intrusion prevention systems (IPS), antivirus, and antispam engines, unsuccessful login attempts, and screen options. You can also click a specific geographical location to view the event count and the top five inbound and outbound IP addresses.

The threat data is displayed starting from 12:00 AM (midnight) up to the current time (in your time zone) on that day and is updated every 30 seconds. The current date and time is displayed at the top right and a legend is displayed at the bottom left of the page.

If a threat occurs when you are viewing the page, an animation shows the country from which the threat originated (source) and the country in which the threat occurred (destination).

**NOTE:** For threats with unknown geographical IP addresses (private IP addresses), the animation shows the threat originating from the bottom center of the geographical map.

# Tasks You Can Perform

You can perform the following tasks from this page:

- Toggle between updating the data and allowing live updates—Click the **Pause** icon to stop the page from updating the threat map data and to stop animations. Click the **Play** icon to update the page data and resume animations.
- Zoom in and out of the page—Click the zoom in (+) and zoom out (–) icons to zoom in and out of the page.
- Pan the page—Click and drag the mouse to pan the page.
- View country-specific details:
  - Click a country on the threat map to view threat information specific to that country. A *Country-Name* pop-up appears displaying country-specific information.
  - Click the **View Details** link in the *Country-Name* pop-up to view additional details. The *Country-Name* (Details) panel appears.

For more information, see [Table 265 on page 689](#).

**Table 265: Country-Specific Threat Information**

Field	Description	Displayed In
<b><i>Number-of-threat-events</i></b> <b>Threat Events since 12:00 am</b>	Displays the total number of threat events (inbound and outbound) since midnight for that country.  Click the hyperlinked number to go to the All Events page, where you can view more information about the events.	<i>Country-Name</i> pop-up
<b>Inbound</b> <b><i>(Number-of-threat-events)</i></b>	Displays the total number of inbound threats for the country and the IP address and the number of events for that IP address for the top five inbound events.	<i>Country-Name</i> pop-up
<b>Outbound</b> <b><i>(Number-of-threat-events)</i></b>	Displays the total number of outbound threats for the country and the IP address and the number of events for that IP address for the top five outbound events.	<i>Country-Name</i> pop-up
<b><i>Number-of-threat-events</i></b> <b>Events since 12:00 am</b>	Displays the total number of threat events (inbound and outbound) since midnight for that country.  Click the hyperlinked number to go to the All Events page, where you can view more information about the events.	<i>Country-Name</i> (Details) panel

Table 265: Country-Specific Threat Information (*continued*)

Field	Description	Displayed In
<b>Number-of Inbound Events</b>	<p>Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> <li>• IPS Threats</li> <li>• Virus</li> <li>• Spam</li> <li>• Device Authentication</li> <li>• Screen</li> </ul> <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS Events page.</p> <p>Click the <b>Top 5 IP Addresses (Inbound)</b> to view the IP address and the number of events for that IP address for the top five inbound events.</p>	<i>Country-Name</i> (Details) panel
<b>Number-of Outbound Events</b>	<p>Displays the total number of outbound threats for the country and the number of outbound threat events for each of the following categories:</p> <ul style="list-style-type: none"> <li>• IPS Threats</li> <li>• Virus</li> <li>• Spam</li> <li>• Device Authentication</li> <li>• Screen</li> </ul> <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for screens takes you to the Screen Events page.</p> <p>Click the <b>Top 5 IP Addresses (Outbound)</b> to view the IP address and the number of events for that IP address for the top five outbound events.</p>	<i>Country-Name</i> (Details) panel

## Field Descriptions

Table 266 on page 691 displays the fields the Threats Map (Live) page.



Table 266: Fields on the Threats Map (Live) Page

Field	Description
<b>Total Threats Blocked &amp; Allowed</b>	Displays the total number of threats blocked and allowed. Click the hyperlinked number to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events.
<b>Threats Blocked &amp; Allowed</b>	<p>Displays the total number of threats blocked and allowed by the following categories:</p> <ul style="list-style-type: none"> <li>• IPS Threats</li> <li>• Virus</li> <li>• Spam</li> <li>• Device Authentication</li> <li>• Screen</li> </ul> <p>Click the hyperlinked number for a category to go to the page for that category, where you can view more information about that category. For example, clicking the hyperlinked number for IPS threats takes you to the IPS Events page (filtered view of the Detail View tab).</p>
<b>Top Target Devices</b>	Displays the top five targeted devices and the number of threats per device. Click the hyperlink for a device to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that device.
<b>Top Destination Countries</b>	Displays the top five destination countries and the number of threats per country. Click the hyperlink for a country to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that country.
<b>Top Source Countries</b>	<p>Displays the top five source countries and the number of threats per country. Click the hyperlink for a country to go to the All Events page (filtered view of the Detail View tab), where you can view more information about the IPS, virus, spam, device authentication, and screen events for that country.</p> <p><b>NOTE:</b> For threats with unknown geographical IP addresses (private IP addresses), the country name is displayed as <i>Undefined</i>. So, when you click the hyperlinked threat count and go to the All Events page, the filter query uses <b>Undefined</b> as the source country.</p>

## Threat Types

The Threats Map (Live) page displays blocked and allowed threat events based on feeds from IPS, antivirus, and antispam engines, unsuccessful login attempts, and screen options. [Table 267 on page 692](#) describes different types of threats blocked and allowed.

Table 267: Types of Threats

Attack	Description
IPS threat events	<p>Intrusion detection and prevention (IDP) attacks detected by the IDP module.</p> <p>The information reported about the attack (displayed on the IPS Events page) includes information about:</p> <ul style="list-style-type: none"> <li>• Source of attack</li> <li>• Destination of attack</li> <li>• Type of attack</li> <li>• Session information</li> <li>• Severity</li> <li>• Policy information that permitted the traffic.</li> <li>• Action: traffic permitted or dropped.</li> </ul>
Virus events	<p>Virus attacks detected by the antivirus engine.</p> <p>The information reported about the attack (displayed on the Antivirus Events page) includes information about:</p> <ul style="list-style-type: none"> <li>• Source of the infected file</li> <li>• Destination</li> <li>• Filename</li> <li>• URL used for accessing the file</li> </ul>
Spam events	<p>E-mail spam that is detected based on the blocklist spam e-mails.</p> <p>The information reported about the attack (displayed on the Antispam Events page) includes information about:</p> <ul style="list-style-type: none"> <li>• Source</li> <li>• Action: E-mail is rejected or allowed.</li> <li>• Reason for identifying as e-mail spam.</li> </ul>
Device authentications	<p>The firewall authentication messages generated due to unauthorized attempts to access the network. The reported information (displayed on the All Events page) contains the reason for authentication failure and the source of the request.</p>

Table 267: Types of Threats (continued)

Attack	Description
Screen events	<p>Events that are detected based on screen options.</p> <p>The information reported about the attack (displayed on the Screen Events page) includes information about:</p> <ul style="list-style-type: none"><li>• Internet Control Message Protocol (ICMP) screening</li><li>• IP screening</li><li>• TCP screening</li><li>• UDP screening</li></ul>

RELATED DOCUMENTATION

| [About the All Security Events Page](#) | 635

# 8

PART

## Managing Reports

---

[Security Reports](#) | **695**

[SD-WAN Reports](#) | **719**

---

# Security Reports

## IN THIS CHAPTER

- [Reports Overview | 695](#)
- [About the Security Report Definitions Page | 696](#)
- [Scheduling, Generating, Previewing, and Sharing Security Reports | 699](#)
- [About the Security Generated Reports Page | 702](#)
- [Creating Log Report Definition | 703](#)
- [Creating Bandwidth Report Definition | 707](#)
- [Creating ANR Report Definition | 709](#)
- [Editing, Deleting, and Cloning Log Report Definitions | 712](#)
- [Editing, Deleting, and Cloning Bandwidth Report Definitions | 714](#)
- [Editing, Deleting, and Cloning ANR Report Definitions | 716](#)

## Reports Overview

Reports are generated based on the summary of network activity (such as Virus Detected) and overall network status. To generate report definitions, you can use the predefined report definitions as is, or you can create custom report definitions that meet your needs for specific data.

Using report definitions, you can:

- Generate reports based on the defined filters.
- Generate reports based on the available predefined report definition.
- Generate reports with multiple sections, where each section has its own criteria.

The generated report contains a table of contents (TOC) with links to each section of the report. The designated recipients, whose e-mail addresses are included in the report definition, receive the report in PDF format.

You can generate two categories of reports:

Security reports—Provide information about network activity and network status.

SD-WAN reports—Provide information about SLA performance of all sites or specific sites in a tenant.

The following are the types of security reports:

- **Log Reports**—Enable you to analyze event history based on the data criteria (such as filters, aggregation criteria, time span, etc.) that you select.
- **Bandwidth Reports**—Enable you to analyze the bandwidth usage of an application or a user.
- **ANR Reports**—Enable you to analyze business risks in the network, based on application usage and resource usage.

The following are the types of SD-WAN reports:

- **SD-WAN Tenant Performance Reports**—Enable you to analyze tenant performance based on the parameters (top applications by bandwidth, top sites not meeting the SLA, top sites meeting the SLA with switching, sites meeting the SLA without switching, top sites by packet loss, and top sites by latency) that measure the SLA performance across all sites in a tenant.
- **SD-WAN Site Performance Reports**—Enable you to analyze site performance based on the parameters (top 10 applications, link utilization (by bandwidth) by applications, top profiles not meeting the SLA, and top SLA profiles switching links) that measure the SLA performance of specific sites in a tenant. You can select a maximum of five sites for which you want to generate the report.

## RELATED DOCUMENTATION

[About the Security Report Definitions Page | 696](#)

[About the SD-WAN Report Definitions Page | 719](#)

## About the Security Report Definitions Page

To access the Security Report Definitions page, click **Customer Portal > Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

The Security Report Definitions page displays a list of predefined and custom report definitions. To generate reports, you can use the predefined report definitions as is, or you can create custom report definitions.

**NOTE:** From CSO Release 4.1.0 onward, an Application and Network Risk (ANR) report is the only predefined report definition available on the Security Report Definitions page.

The ANR report provides information about data usage and network risks. The information is consolidated from various predefined report definitions available in the release prior to CSO Release 4.1.0.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create a report definition:
  - To create a log report definition, see [“Creating Log Report Definition” on page 703](#).
  - To create a bandwidth report definition, see [“Creating Bandwidth Report Definition” on page 707](#).
  - To create an application and network risk report definition, see [“Creating ANR Report Definition” on page 709](#)
- Edit, delete, or clone report definitions:
  - To edit, delete, or clone a log report definition, see [“Editing, Deleting, and Cloning Log Report Definitions” on page 712](#).
  - To edit, delete, or clone a bandwidth report definition, see [“Editing, Deleting, and Cloning Bandwidth Report Definitions” on page 714](#).
  - To edit, delete, or clone an application and network risk report definition, see [“Editing, Deleting, and Cloning ANR Report Definitions” on page 716](#).
- To schedule, generate reports, preview reports as PDF, and send the reports through e-mail, see [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).
- To view all the parameters of a report definition, right click the report definition that you want to see the detailed view for and select **Detailed View**, or select the report definition and click **More > Detailed View**. Alternatively, hover over the report definition name and click the Detailed View icon that appears before it.

The Report Definition Details page appears, displaying the same values that you specified for each parameter in the selected report definition.

### Field Descriptions

[Table 268 on page 698](#) describes the fields on the Security Report Definitions page.

Table 268: Fields on the Security Report Definitions Page

Field	Description
Name	Name of the report definition.
Description	Description of the report definition.  For example: Report of data usage by application and network risk.
Type	Type of report definition—ANR, Bandwidth, or Log.
Definition Type	Indicates whether the report definition is predefined (system-generated) or custom (user-created).
Report Content	Details of the sections in the report.  For example: Count, Time Duration.
Schedule	Indicates whether the report generation is scheduled at the current time (Now) or for a later date and time (Once).
Recipients	E-mail addresses of recipients to whom the generated report is sent.
Last Generated	Date and time when the report was last generated.
Job ID	Using the job ID, you can view the status of the task on the Jobs page.

## RELATED DOCUMENTATION

[Reports Overview | 695](#)
[Creating Log Report Definition | 703](#)
[Creating Bandwidth Report Definition | 707](#)
[Creating ANR Report Definition | 709](#)



## Scheduling, Generating, Previewing, and Sharing Security Reports

### IN THIS SECTION

- [Editing Report Generation Schedule | 699](#)
- [Generating Reports | 700](#)
- [Previewing Reports in PDF | 701](#)
- [Sharing Reports through E-mail | 701](#)

You can schedule report generation, generate reports, preview reports as PDF, and share the reports through e-mail.

To perform these actions on a report definition:

1. Select **Reports > Report Definitions**.

The Security Report Definitions page appears.

2. Select or right-click the report definition on which you want to perform an action and click **More**.

A list of actions that you can perform on the report definition is displayed.

3. Select the appropriate action from the list:

### Editing Report Generation Schedule

You can edit the report generation schedule of the selected report definition from the Security Report Definitions page:

1. Select the report definition for which you want to edit the report generation schedule.
2. Click **More > Edit Schedule**. Alternatively, right-click on the selected report definition and select **Edit Schedule**.

The Edit Report Schedule page appears.

3. Specify whether you want to generate the report at the current time or schedule it for a later date and time:
  - **Run now**—Select this option to schedule the report generation at the current time.

- Schedule at a later time—Select this option to schedule the report generation for a later date and time in MM/DD/YYYY and HH:MM:SS formats.

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

You are returned to the Security Report Definitions page on which a confirmation message, indicating that the report generation schedule is updated successfully, appears.

## Generating Reports

You can generate a report at the current time, with either saved settings or custom settings. You can select **Saved Settings** to generate a report based on the values specified in the report definition for the selected report or select **Custom Settings** to modify the values for the Number of Top Logs and the Time Span settings, and generate a report based on the modified values.

**NOTE:** The modified values are applicable only for the report that is being generated and are not saved in the report definition.

To generate a report:

1. From the Security Report Definitions page, select the report definition based on which you want to generate the report.
2. Click **Run Now** on the Security Report Definitions page. Alternatively, click **More > Run Now** or right-click on the report definition and click **Run Now**.

The Run Report page appears.

3. Do one of the following:
  - Select **Saved Settings** to generate a report based on the values already specified in the report definition.
  - Select **Custom Settings** to modify the values for the Number of Top Logs and Time Span settings, and generate a report based on the modified values.

**NOTE:** The values that you modify are applicable only for the report that is being generated and are not saved in the report definition.

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

The Run Report page appears indicating the progress of the report generation. After the report is generated, the **Download PDF Report** link appears on the Run Report page.

5. Click **Download PDF Report**.

Follow your browser instructions to view or save the report in PDF.

## Previewing Reports in PDF

You can preview and download the selected report in PDF:

1. Select the report definition based on which you want to generate the PDF of the report.
2. Click **More > Preview as PDF**. Alternatively, right-click on the report definition and select **Preview as PDF**.

The Preview as PDF page appears.

3. Click **Download PDF Report** to view the report in PDF. or click **Cancel** to cancel previewing the report.

You are returned to the Security Report Definitions page.

## Sharing Reports through E-mail

You can share the generated report through e-mail:

1. Select the report definition based on which the report is to be generated and shared through e-mail.
2. Click **More > Send Report**. Alternatively, right-click on the report definition and select **Send Report**.

The Edit Recipients page appears:

- **Recipients**—Enter or select one or more e-mail addresses of users to whom you want to send the report.

By default, you can search by first name and select registered users. You can also enter external e-mail addresses.

- **Subject**—Enter the subject line for the e-mail. The maximum length is 2048 characters.
- **Comments**—Enter the text to be included in the body of the e-mail.

The maximum length allowed is 2048 characters.

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

You are returned to the Security Report Definitions page.

RELATED DOCUMENTATION

| [About the Security Report Definitions Page](#) | 696

## About the Security Generated Reports Page

To access this page, click **Customer Portal > Reports > Generated Reports > Security**.

Use this page to view the list of reports that are generated from the Security Report Definitions page. You must click on the report to view the report in PDF format.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Delete the generated report.
- Open the generated report.

### Field Descriptions

[Table 269 on page 702](#) provides guidelines on using the fields on the Generated Reports page.

**Table 269: Fields on the Generated Reports Page**

Field	Description
Report PDF Name	View the name of the report (user created or predefined).
Generated Time	View the date and time when the report was generated.
Description	View the description of the report.
Definition Name	View the name of the report definition.
Generated By	View the name of who generated the report.
Recipients	View the recipients of the generated reports.

RELATED DOCUMENTATION

## Creating Log Report Definition

You can use the Create Log Report Definition page to create log report definitions and generate the corresponding log reports. Log reports are generated based on the data criteria, which are derived from one or more filters that you select. These reports help you to analyze business risks based on logs from services such as unified threat management (UTM) and firewalls.

To create a log report definition:

1. Select **Reports > Report Definitions > Security**.  
The Security Report Definitions page appears.
2. Click **Create > Log Report Definitions**.  
The Create Log Report Definition page appears.
3. Complete the configuration according to the guidelines provided in [Table 270 on page 703](#).

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

4. Click **OK** to save the log report definition.  
You are returned to the Security Report Definitions page on which a confirmation message, indicating that the report definition was successfully created, appears.  
You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).

Table 270: Fields on the Create Log Report Definition Page

Field	Description
<b>General</b>	
Report Name	Enter a unique name for the report definition. The name can be a string of alphanumeric characters, some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length is 63 characters.

Table 270: Fields on the Create Log Report Definition Page (*continued*)

Field	Description
Description	Enter a description for the report definition; the maximum length (including spaces) is 1024 characters.
<b>Content</b>	
Data Criteria	<p>Click <b>Filters</b> to select one or more filters.</p> <p>The <b>Use Data Criteria From Filter</b> page appears.</p> <p>The list of default and custom filters, which are saved from the Security Events page, is displayed in a tabular format. The table displays the Filter Name, Filter Description, Time Span, and Group By and Filter By criteria for each filter.</p> <p>Select one or more filters from the list as per your requirement, and click <b>OK</b>.</p> <p>You are returned to the Create Log Report Definition page.</p> <p>When you select one or more filters, new fields appear on the Create Log Report Definition page. The fields are populated with values from the filters. You can either retain the values or change the values if needed. See <a href="#">Table 271 on page 705</a> for an explanation of the fields.</p>
<b>Schedule</b>	
Schedule Report	<p>Click <b>Add Schedule</b> to schedule the report generation.</p> <p>The <b>Add Report Schedule</b> page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> <li>• <b>Run now</b>—Select this option to schedule the report generation at the current time, and click <b>OK</b>.</li> <li>• <b>Schedule at a later time</b>—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats) and click <b>OK</b>.</li> </ul> <p>You are returned to the Create Log Report Definition page on which the details of the report generation schedule appear.</p>
<b>E-Mail</b>	

Table 270: Fields on the Create Log Report Definition Page (continued)

Field	Description
E-Mail Recipients	<p>Click <b>Add Email Recipients</b> to add e-mail addresses of recipients to whom you want to send the log report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> <li>Recipients—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses (e-mail addresses that are not registered with CSO).</li> <li>Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> <li>Comment—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> </ul>

Table 271 on page 705 displays the additional fields that appear on the Create Log Report Definition page when you select one or more filters.

Table 271: Additional Fields on the Create Log Report Definition Page

Section	<p>Section number in the log report for a selected filter.</p> <p>Click <b>Delete Section</b> to remove the section and the corresponding filter.</p>
Section Title	<p>Name of the section in the log report.</p> <p>The section title is based on the selected filter.</p>
Section Description	<p>Description for the section in the log report.</p>
Group By	<p>Criteria, such as <b>Nested Application</b>, based on which logs are aggregated.</p> <p>You can select a maximum of two data criteria from the <b>Group By</b> drop-down list.</p>
Time Span (Last)	<p>Duration for which the report is to be generated.</p> <p>The default time span is 3 hours.</p> <p>You can specify the duration in minutes, hours, days, weeks, months, or specify a custom duration.</p>

Table 271: Additional Fields on the Create Log Report Definition Page (*continued*)

	<p>If you select <b>Custom</b>, the <b>Custom Time Range Selection</b> page appears. You must specify the <b>From</b> date and time, and <b>To</b> date and time (in MM/DD/YYYY and HH:MM:SS formats).</p>
<b>Filter By</b>	<p>Filter criteria (such as filtering applications based on http and https protocols) based on which the log report is to be generated.</p> <p>You can use AND, OR, Equal to (=), and Not Equal to (!=) logical operators as values to generate the report.</p> <p>For example: If you want to generate a report with the event category as antivirus and event name as AV_VIRUS_Detected_MT, then the value must be:</p> <p>Event Category = antivirus AND Event Name = AV_VIRUS_DETECTED_MT</p>
<b>Chart</b>	<p>Type of chart to graphically present data on the report.</p> <p>The available options are Bar (default), Comparison Bar, Timeline, Grid, Grouped Grid, Donut, and Bubble chart.</p>
<b>Number of Top Logs</b>	<p>Specify the number of events that you want to retrieve and display for each section in the report.</p> <p>Range: 1 through 20.</p> <p>Default: 10.</p>

## RELATED DOCUMENTATION

[About the Security Report Definitions Page | 696](#)
[Creating Bandwidth Report Definition | 707](#)
[Creating ANR Report Definition | 709](#)



# Creating Bandwidth Report Definition

You can use the Create Bandwidth Report Definition page to create bandwidth report definitions and generate the corresponding bandwidth reports. Bandwidth reports are used to analyze the bandwidth usage of an application or a user.

To create a bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Click **Create > Bandwidth Report Definitions**.

The Create Bandwidth Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 272 on page 707](#).

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

4. Click **OK** to save the bandwidth report definition.

The report definition is saved and you are returned to the Security Report Definitions page.

You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).

**Table 272: Fields on the Create Bandwidth Report Definition Page**

Field	Description
<b>General</b>	
Report Name	Enter a unique name for the report definition. The name can be a string of alphanumeric characters, some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the report definition; the maximum length (including spaces) is 1024 characters.
<b>Content</b>	

Table 272: Fields on the Create Bandwidth Report Definition Page (*continued*)

Field	Description
Number of Top Logs	<p>Specify the number of events that you want to retrieve and display for each section in the report.</p> <p>Range: 1 through 20.</p> <p>Default: 10.</p>
Time Span (Last)	<p>Specify the duration (Custom, last 3 hours, last 6 hours, last 12 hours, or last 24 hours) for which you want the report to be generated.</p> <p>If you select <b>Custom</b>, the <b>Custom Time Range Selection</b> page appears. You must specify the <b>From</b> date and time, and <b>To</b> date and time (in MM/DD/YYYY and HH:MM:SS formats).</p>
<b>Schedule</b>	
Add Schedule	<p>Click <b>Add Schedule</b> to schedule the report generation.</p> <p>The <b>Add Report Schedule</b> page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> <li>• Run now—Select this option to schedule the report generation at the current time, and click <b>OK</b>.</li> <li>• Schedule at a later time—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats), and click <b>OK</b>.</li> </ul> <p>You are returned to the Create Bandwidth Report Definition page on which the details of the report generation schedule appear.</p>
<b>E-Mail</b>	

Table 272: Fields on the Create Bandwidth Report Definition Page (*continued*)

Field	Description
Add E-Mail Recipients	<p>Click <b>Add Email Recipients</b> to add e-mail addresses of recipients to whom you want to send the Bandwidth report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> <li>• <b>Recipients</b>—Enter or select one or more e-mail addresses of users to whom you want to send the report. By default, you can search by first name and select registered users. You can also enter external e-mail addresses.</li> <li>• <b>Subject</b>—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> <li>• <b>Comment</b>—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> </ul>

## RELATED DOCUMENTATION

[About the Security Report Definitions Page | 696](#)

[Creating Log Report Definition | 703](#)

[Creating ANR Report Definition | 709](#)

## Creating ANR Report Definition

You can use the Create ANR Report Definition page to create Application and Network Risk (ANR) report definitions and generate the corresponding ANR reports. ANR reports help you to analyze business risks in a network, based on application usage and resource usage.

To create an ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Click **Create > ANR Report Definition**.

The Create ANR Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 273 on page 710](#).

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

4. Click **OK** to save the ANR report definition.

The report definition is saved and you are returned to the Security Report Definitions page.

You can perform various actions on the report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).

**Table 273: Fields on the Create ANR Report Definition Page**

Field	Description
<b>General</b>	
Report Name	Enter a unique name for the report definition. The name can be a string of alphanumeric characters, some special characters (colons, periods, dashes, and underscores); no spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the report definition; the maximum length (including spaces) is 1024 characters.
<b>Content</b>	
Number of Top Logs	Specify the number of events that you want to retrieve and display for each section in the report.  Range: 1 through 20.  Default: 10.
Time Span (Last)	Specify the duration (Custom, last 3 hours, last 6 hours, last 12 hours, or last 24 hours) for which you want the report to be generated.  If you select <b>Custom</b> , the <b>Custom Time Range Selection</b> page appears. You must specify the <b>From</b> date and time, and <b>To</b> date and time (in MM/DD/YYYY and HH:MM:SS formats).
<b>Schedule</b>	

Table 273: Fields on the Create ANR Report Definition Page (*continued*)

Field	Description
Schedule Report	<p>Click <b>Add Schedule</b> to schedule the report generation.</p> <p>The <b>Add Report Schedule</b> page appears.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time:</p> <ul style="list-style-type: none"> <li>• <b>Run now</b>—Select this option to schedule the report generation at the current time, and click <b>OK</b>.</li> <li>• <b>Schedule at a later time</b>—Select this option to schedule the report generation for a later date and time (in MM/DD/YYYY and HH:MM:SS formats), and click <b>OK</b>.</li> </ul> <p>You are returned to the Create ANR Report Definition page on which the details of the report generation schedule appear.</p>
<b>E-Mail</b>	
E-Mail Recipients	<p>Click <b>Add Email Recipients</b> to add e-mail addresses of recipients to whom you want to send the ANR report.</p> <p>The Add Recipients page appears.</p> <ul style="list-style-type: none"> <li>• <b>Recipients</b>—Enter or select one or more e-mail addresses of users to whom you want to send the report.</li> </ul> <p>By default, you can search by first name and select registered users. You can also enter external e-mail addresses.</p> <ul style="list-style-type: none"> <li>• <b>Subject</b>—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> <li>• <b>Comment</b>—Enter the text to be included in the body of the e-mail that is sent with the generated report.</li> </ul> <p>The maximum length is 2048 characters.</p>

## RELATED DOCUMENTATION

[About the Security Report Definitions Page | 696](#)

[Creating Bandwidth Report Definition | 707](#)

[Creating Log Report Definition | 703](#)

## Editing, Deleting, and Cloning Log Report Definitions

### IN THIS SECTION

- [Editing the Log Report Definition | 712](#)
- [Deleting Log Report Definitions | 712](#)
- [Cloning Log Report Definitions | 713](#)

You can edit, delete, and clone log report definitions.

### Editing the Log Report Definition

You can edit custom log report definitions from the Security Report Definitions page.

To edit the custom log report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the log report definition that you want to edit, and click the edit icon (pencil).

The **Edit Log Report Definition** page appears, displaying the same fields that are presented when you create a log report definition.

3. Modify the log report definition fields as needed.

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

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the report definition is updated, appears on top of the Security Report Definitions page.

### Deleting Log Report Definitions

You can use the Security Report Definitions page to delete one or more custom log report definitions.

To delete one or more log report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the log report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected log report definitions or click **No** to cancel the deletion.

You are returned to the Security Report Definitions page.

If you click Yes, the selected log report definitions are deleted. A confirmation message, indicating that the selected report definitions are deleted, appears on top of the Security Report Definitions page.

## Cloning Log Report Definitions

Cloning enables you to easily create a new log report definition based on an existing one.

**NOTE:** You can clone predefined and custom log report definitions.

To clone a log report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click on the log report definition that you want to clone and select **Clone**. Alternatively, select the log report definition and then select **More > Clone**.

The **Clone log Report Definition** page appears, displaying the same fields that are presented when you create a log report definition.

3. Modify the log Report Definition fields as needed.
4. Click **OK** to save your changes or click **Cancel** to discard the changes.

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the selected report definition was cloned successfully, appears on top of the Security Report Definitions page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).

## RELATED DOCUMENTATION

[Creating Log Report Definition | 703](#)

[About the Security Report Definitions Page | 696](#)

## Editing, Deleting, and Cloning Bandwidth Report Definitions

### IN THIS SECTION

- [Editing Bandwidth Report Definitions | 714](#)
- [Deleting Bandwidth Report Definitions | 715](#)
- [Cloning Bandwidth Report Definitions | 715](#)

You can edit, delete, and clone bandwidth report definitions.

### Editing Bandwidth Report Definitions

You can edit custom bandwidth report definitions from the Security Report Definitions page.

To edit the custom bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the bandwidth report definition that you want to edit, and click the edit icon (pencil).

The **Edit Bandwidth Report Definition** page appears, displaying the same fields that are presented when you create a bandwidth report definition.

3. Modify the bandwidth report definition fields as needed.

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

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the report definition is updated, appears on top of the Security Report Definitions page.



## Deleting Bandwidth Report Definitions

You can use the Security Report Definitions page to delete one or more custom bandwidth report definitions.

To delete one or more bandwidth report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the bandwidth report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected bandwidth report definitions or click **No** to cancel the deletion.

You are returned to the Security Report Definitions page.

If you click Yes, the selected bandwidth report definitions are deleted. A confirmation message, indicating that the selected report definitions are deleted, appears on top of the Security Report Definitions page.

## Cloning Bandwidth Report Definitions

Cloning enables you to easily create a new bandwidth report definition based on an existing one.

**NOTE:** You can clone predefined and custom bandwidth report definitions.

To clone a bandwidth report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click on the bandwidth report definition that you want to clone and select **Clone**. Alternatively, select the bandwidth report definition and then select **More > Clone**.

The **Clone Bandwidth Report Definition** page appears, displaying the same fields that are presented when you create a bandwidth report definition.

3. Modify the bandwidth report definition fields as needed.

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

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the selected report definition was cloned successfully, appears on top of the Security Report Definitions page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports”](#) on page 699.

## RELATED DOCUMENTATION

[About the Security Report Definitions Page](#) | 696

[Creating Bandwidth Report Definition](#) | 707

## Editing, Deleting, and Cloning ANR Report Definitions

### IN THIS SECTION

- [Editing ANR Report Definitions](#) | 716
- [Deleting ANR Report Definitions](#) | 717
- [Cloning ANR Report Definitions](#) | 717

You can edit, delete, and clone ANR report definitions.

### Editing ANR Report Definitions

You can edit custom ANR report definitions from the Security Report Definitions page.

To edit the custom ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The Security Report Definitions page appears.

2. Select the ANR report definition that you want to edit, and click the edit icon (pencil).

The **Edit ANR Report Definition** page appears, displaying the same fields that are presented when you create an ANR report definition.

3. Modify the ANR Report Definition fields as needed.
4. Click **OK** to save the changes or click **Cancel** to discard the changes.

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the report definition is updated, appears on top of the Security Report Definitions page.

## Deleting ANR Report Definitions

You can use the Security Report Definitions page to delete one or more custom ANR report definitions.

To delete one or more ANR report definitions:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Select the ANR report definitions that you want to delete, and click the delete icon. Alternatively, right click on the report definitions that you want to delete and select **Delete Report**.

The **Delete Report Definition** page appears.

3. Click **Yes** to delete the selected ANR report definitions or click **No** to cancel the deletion.

You are returned to the Security Report Definitions page.

If you click Yes, the selected ANR report definitions are deleted. A confirmation message, indicating that the selected report definitions are deleted, appears on top of the Security Report Definitions page.

## Cloning ANR Report Definitions

Cloning enables you to easily create a new ANR report definition based on an existing one.

**NOTE:** You can clone predefined and custom ANR report definitions.

To clone an ANR report definition:

1. Select **Reports > Report Definitions > Security**.

The **Security Report Definitions** page appears.

2. Right-click on the ANR report definition that you want to clone and select **Clone**. Alternatively, select the ANR report definition and then select **More > Clone**.

The **Clone ANR Report Definition** page appears, displaying the same fields that are presented when you create an ANR report definition..

3. Modify the ANR Report Definition fields as needed.
4. Click **OK** to save your changes or click **Cancel** to discard the changes.

You are returned to the Security Report Definitions page.

If you click OK, a confirmation message, indicating that the selected report definition was cloned successfully, appears on top of the Security Report Definitions page.

You can perform various actions on the cloned report definition. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#).

## RELATED DOCUMENTATION

---

[About the Security Report Definitions Page | 696](#)

[Creating ANR Report Definition | 709](#)

# SD-WAN Reports

## IN THIS CHAPTER

- [About the SD-WAN Report Definitions Page | 719](#)
- [Editing, Deleting, and Cloning SD-WAN Report Definitions | 721](#)
- [Creating SD-WAN Tenant Performance Report Definitions | 723](#)
- [Creating SD-WAN Site Performance Report Definitions | 727](#)
- [About the SD-WAN Generated Reports Page | 730](#)

## About the SD-WAN Report Definitions Page

To access this page, click **Customer Portal > Reports > Report Definitions > SD-WAN**.

Use this page to view and manage predefined and custom report definitions and generate reports based on the definitions. You can also preview a report in PDF and send reports to recipients. An SD-WAN report includes SLA performance of top applications by bandwidth, top sites not meeting SLA, top sites meeting SLA with switching, sites meeting SLA without switching, top sites by highest packet loss, top sites by highest latency, top sites by highest jitter, and current active tunnels. You can generate an SLA performance report for all sites in a tenant or for specific sites in a tenant.

You can perform various actions on reports such as run a report immediately, edit a schedule, edit e-mail recipients, preview a report in PDF, send reports, and clone reports, using this page.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Create SD-WAN tenant performance report definitions. See [“Creating SD-WAN Tenant Performance Report Definitions” on page 723](#)
- Create SD-WAN site performance report definitions. See [“Creating SD-WAN Site Performance Report Definitions” on page 727](#)

- Run a report immediately, edit a schedule, edit e-mail recipients, preview a report in PDF, send reports, and clone reports. See [“Scheduling, Generating, Previewing, and Sharing Security Reports” on page 699](#)
- View details about an SD-WAN report definition—Right-click a report definition and then select **Detailed View** or select **More > Detailed View**.

The Report Definition Details page appears, displaying fields such as Report Name, Description, Duration, Number of Top Logs, and Report Sections.

## Field Descriptions

[Table 274 on page 720](#) provides guidelines on using the fields on the SD-WAN Report Definitions page.

**Table 274: Fields on the SD-WAN Report Definitions Page**

Field	Description
Name	View the name of the SD-WAN report.
Description	View the description of the SD-WAN report definition.
Type	View the type of SD-WAN report. The report type can be SD-WAN tenant performance SD-WAN site performance.
Definition Type	View the type of SD-WAN report definition. The report definition type can be predefined or custom.
Schedule	View the report generation schedule, whether the report is scheduled to generate immediately or scheduled it for a later date and time.
Recipients	View the recipients of the generated reports.
Job ID	View the last generated job ID of the report.

## RELATED DOCUMENTATION

[Editing, Deleting, and Cloning SD-WAN Report Definitions | 721](#)

[Creating SD-WAN Tenant Performance Report Definitions | 723](#)

[Creating SD-WAN Site Performance Report Definitions | 727](#)

## Editing, Deleting, and Cloning SD-WAN Report Definitions

### IN THIS SECTION

- [Editing the SD-WAN Report Definition | 721](#)
- [Deleting SD-WAN Report Definitions | 722](#)
- [Cloning SD-WAN Report Definitions | 722](#)

You can edit, delete, and clone SD-WAN report definitions from the SD-WAN definitions page. This topic has the following sections:

### Editing the SD-WAN Report Definition

To edit the SD-WAN report definition:

**NOTE:** You cannot modify the predefined report definition.

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Select the check box of the SD-WAN custom report definition that you want to modify, and click the edit icon.

The Update SD-WAN Performance Report Definition page appears. The options available on the Create SD-WAN Performance Report Definition page are available for editing.

3. Update the configuration as needed.

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

The SD-WAN report definition information that you updated appears on the SD-WAN report definition page.

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

## Deleting SD-WAN Report Definitions

You can clear all unwanted report definitions that are not used anywhere in your network. Use the delete icon (X) in the top right corner of a page to delete one or more SD-WAN report definitions.

**NOTE:** You can delete only custom SD-WAN report definitions.

To delete an SD-WAN report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Select the SD-WAN report definition or right click on the report definition that you want to delete and click the delete icon (X).

The Confirm Delete page appears.

3. Click **Yes** to delete the SD-WAN report definition or **No** to cancel the deletion.

The SD-WAN report definition is deleted from the main page.

## Cloning SD-WAN Report Definitions

Cloning enables you to easily create a new SD-WAN report definition based on an existing one.

**NOTE:** You can clone predefined and custom SD-WAN report definitions.

To clone an SD-WAN report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Right-click on the SD-WAN report definition that you want to clone and select **Clone**. Alternatively, select the SD-WAN report definition and then select **More > Clone**.

The **Clone SD-WAN Performance Report Definition** page appears, displaying the same fields that are presented when you create an SD-WAN report definition.



3. Modify the SD-WAN Report Definition fields as needed.
4. Click **OK** to save your changes or click **Cancel** to discard the changes.

You are returned to the SD-WAN Report Definitions page.

If you click OK, a confirmation message, indicating that the selected report definition was cloned successfully, appears on top of the SD-WAN Report Definitions page.

## RELATED DOCUMENTATION

[About the SD-WAN Report Definitions Page | 719](#)

## Creating SD-WAN Tenant Performance Report Definitions

Use this page to create SD-WAN tenant performance report definitions for all sites in a tenant and generate reports based on the definitions. You can also schedule report generation and add one or more recipients to whom you want to send the reports.

The SD-WAN tenant performance report includes the following information:

- Top applications by bandwidth
- Top sites not meeting SLA
- Top sites meeting SLA with switching
- Sites meeting SLA without switching
- Top sites by current active tunnels
- Top sites by highest packet loss
- Top sites by highest latency
- Top sites by highest jitter

**NOTE:** Only users with the Tenant Administrator role can create SD-WAN tenant performance report definitions.

To create an SD-WAN tenant report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Click **Add > Tenant Performance**.

The Add SD-WAN Tenant Performance Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 275 on page 724](#).

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

4. Click **OK** to save the report definition.

An SD-WAN tenant performance report definition is created and listed on the report definitions page.

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

**Table 275: Fields on the Create Tenant Performance Report Definition**

Field	Description
<b>General</b>	
Report Name	Enter a unique string of alphanumeric characters and some special characters (: . -). No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.
<b>Content</b>	
Time Span	Specify the duration (custom, last 24 hours, last 7 days, or last 30 days) for which the report is generated. When you select the custom option, you must specify start ( <b>From</b> ) and end ( <b>To</b> ) of the time span (in MM/DD/YYYY and HH:MM:SS formats).
<b>NOTE:</b> The <b>From</b> and <b>To</b> fields are listed only when you select the <b>Custom</b> duration.	
From	Specify the start date and time from which the report should be generated.
To	Specify the end date and time up to which the report should be generated.
Number of Top Logs	Enter the number of SLA events (1 through 20) that you want to retrieve and display for each section in the report.

Table 275: Fields on the Create Tenant Performance Report Definition (*continued*)

Field	Description
Report Content	<p>Select the content that you want to view in the report.</p> <ul style="list-style-type: none"> <li>• <b>Top Applications By Bandwidth</b>—Displays a report on top applications by bandwidth.</li> <li>• <b>Top Sites Not Meeting SLA</b>—Displays a report on top sites not meeting the SLA performance.</li> <li>• <b>Top Sites Meeting SLA with Switching</b>—Displays a report on top sites meeting SLA performance with link switching.</li> <li>• <b>Sites Meeting SLA without Switching</b>—Displays report on sites meeting SLA performance without switching.</li> <li>• <b>Current Active Tunnels</b>—Displays a report on top 10 sites that have the maximum number of active DVPN tunnels.</li> <li>• <b>Top Sites by Highest Packet Loss</b>—Displays a report on top 10 sites based on the highest cumulative average packet loss across all the links.</li> <li>• <b>Top Sites by Highest Latency</b>—Displays report on top 10 sites based on the highest cumulative average latency across all the links.</li> <li>• <b>Total Sites by Highest Jitter</b>—Displays report on top 10 sites based on the highest cumulative average jitter across all the links.</li> </ul> <p>For more information about SLA parameters and DVPN tunnels, see <i>SLA Profiles and SD-WAN Policies Overview</i> and <i>Dynamic VPN Tunnels Overview</i> in <i>Contrail Service Orchestration User Guide</i>.</p>
<b>Schedule Report</b>	
Add Schedule	<p>Click <b>Add Schedule</b> to schedule the report generation.</p> <p>The Add Report Schedule page is displayed.</p> <p>Specify whether you want to generate the report immediately or schedule it for a later date and time.</p> <ul style="list-style-type: none"> <li>• <b>Run now</b>—Select this option to generate the report immediately.</li> <li>• <b>Schedule at a later time</b>— Select this option to generate the report at a later date and time (in MM/DD/YYYY and HH:MM:SS format).</li> </ul>
<b>Email Recipients</b>	

Table 275: Fields on the Create Tenant Performance Report Definition (*continued*)

Field	Description
Add Email Recipients	<p>Click <b>Add Email Recipients</b> to add e-mail addresses of recipients to whom you want to send the SD-WAN reports.</p> <p>The Add Recipients page is displayed.</p> <ul style="list-style-type: none"> <li>• <b>Recipients</b>—Select e-mail addresses of users to whom you want to send the report. You can select more than one e-mail address.</li> <li>• <b>Subject</b>—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> <li>• <b>Comment</b>—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> </ul>

## RELATED DOCUMENTATION

[Creating SD-WAN Site Performance Report Definitions | 727](#)

[About the SD-WAN Report Definitions Page | 719](#)

[Editing, Deleting, and Cloning SD-WAN Report Definitions | 721](#)

## Creating SD-WAN Site Performance Report Definitions

Use this page to create SD-WAN site performance report definitions for specific sites of a tenant and generate the report based on the definitions. You can also schedule report generation and add one or more recipients to whom you want to send the reports.

The SD-WAN site performance report includes the following information:

- Top 10 applications and link utilization for site
- Top profiles not meeting SLA
- Top profiles switching links
- Top applications by highest packet loss
- Top applications by highest latency
- Top applications by highest jitter
- SLA performance between two sites

**NOTE:** Only users with the Tenant Administrator role can create SD-WAN site performance report definitions.

To create an SD-WAN site performance report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Click **Create > Site Performance**.

The Create SD-WAN Site Performance Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 276 on page 728](#).

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

4. Click **OK** to save the report definition.

A report definition is created and listed on the SD-WAN report definitions page.

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

Table 276: Fields on the Site Performance Report Definition Page

Field	Description
<b>General</b>	
Report Name	Enter a unique string of alphanumeric characters and some special characters (: . -). No spaces are allowed and the maximum length is 63 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.
<b>Content</b>	
Duration	Specify the duration (custom, last 24 hours, last 7 days, or last 30 days) for which the report is generated. When you select the custom option, you must specify the start ( <b>From</b> ) and end ( <b>To</b> ) of the time span.
<b>NOTE:</b> The <b>From</b> and <b>To</b> fields are listed only when you select the <b>Custom</b> duration.	
From	Specify the start date and time from which the report should be generated.
To	Specify the end date and time up to which the report should be generated.
Number of Top Logs	Enter the number of SLA events (1 through 20) that you want to retrieve and display for each section in the report.
Sites	Select one or more sites for which you want to generate the report. You can select up to five sites.

Table 276: Fields on the Site Performance Report Definition Page (*continued*)

Field	Description
Report Content	<p>Select the content that you want to view in the report.</p> <ul style="list-style-type: none"> <li>• <b>Top 10 Applications and Link Utilization</b>—Displays a report on top 10 applications and link utilization for the selected sites.</li> <li>• <b>Top Profiles Not Meeting SLA</b>—Displays a report on top SLA profiles not meeting SLA for the selected sites.</li> <li>• <b>Top Profiles Switching Links</b>—Displays a report on top SLA profiles switching links for the selected sites.</li> <li>• <b>Top Applications by Packet Loss</b>—Displays report on top 10 applications based on the selected site that has the highest average packet loss across SLA profiles.</li> <li>• <b>Top Applications by Latency</b>—Displays report on top 10 applications based on the selected site that has the highest average latency across SLA profiles.</li> <li>• <b>Total Applications by Jitter</b>—Displays report on top 10 applications based on the selected site that has the highest average jitter across SLA profiles.</li> <li>• <b>SLA Performance Between Two Sites</b>—Displays report on top 20 applications based on the performance of SLA parameters (latency, jitter, and packet loss) between the source and destination site that you have selected.</li> </ul> <p>For more information about SLA parameters and DVPN tunnels, see <i>SLA Profiles and SD-WAN Policies Overview</i> and <i>Dynamic VPN Tunnels Overview</i> in <i>Contrail Service Orchestration User Guide</i>.</p>
Sites	Select one or more sites, from the list of available sites, for which you want to generate the report.
<b>Schedule</b>	
Add Schedule	<p>Click <b>Add Schedule</b> to schedule the report generation.</p> <p>The Add Report Schedule page is displayed.</p> <p>You must specify whether you want to generate the report immediately or schedule it for a later date and time.</p> <ul style="list-style-type: none"> <li>• <b>Run now</b>—Select this option to generate the report immediately.</li> <li>• <b>Schedule at a later time</b>— Select this option to generate the report at a later date and time (in MM/DD/YYYY and HH:MM:SS formats).</li> </ul>
<b>E-Mail</b>	

Table 276: Fields on the Site Performance Report Definition Page (*continued*)

Field	Description
Add E-Mail Recipients	<p>Click <b>Add Email Recipients</b> to add e-mail addresses of recipients to whom you want to send the SD-WAN reports.</p> <p>The Add Recipients page is displayed.</p> <ul style="list-style-type: none"> <li>• <b>Recipients</b>—Select e-mail addresses of users to whom you want to send the report.</li> <li>• <b>Subject</b>—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> <li>• <b>Comment</b>—Enter the text to be included in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.</li> </ul>

## RELATED DOCUMENTATION

[Creating SD-WAN Tenant Performance Report Definitions | 723](#)

[About the SD-WAN Report Definitions Page | 719](#)

[Editing, Deleting, and Cloning SD-WAN Report Definitions | 721](#)

## About the SD-WAN Generated Reports Page

To access this page, click **Customer Portal > Reports > Generated Reports > SD-WAN**.

Use this page to view the list of tenant and site performance reports that are generated from the SD-WAN Report Definitions page. You must click on the report to view the report in PDF format. You can view the generated report up to 30 days and the report will be deleted after 30 days.

### Tasks You Can Perform

You can perform the following tasks from this page:

- Open the generated report.
- Select and delete the generated report.

### Field Descriptions

[Table 277 on page 731](#) provides guidelines on using the fields on the SD-WAN Generated Reports page.



Table 277: Fields on the SD-WAN Generated Reports Page

Field	Description
Name	View the name of the SD-WAN report.
Description	View the description of the report.
Generated Time	View the date and time when the report was generated.
Definition Name	View the name of the report definition.
Generated By	View the name of the tenant administrator who generated the report.
Recipients	View the recipients of the generated reports.

## RELATED DOCUMENTATION

[Reports Overview | 695](#)[About the SD-WAN Report Definitions Page | 719](#)