



Customer Portal Online Help

Release

3.3



Modified: 2018-09-27

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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

Customer Portal Online Help

3.3

Copyright © 2018 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <https://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	xxiii
	Documentation and Release Notes	xxiii
	Documentation Conventions	xxiii
	Documentation Feedback	xxv
	Requesting Technical Support	xxvi
	Self-Help Online Tools and Resources	xxvi
	Opening a Case with JTAC	xxvii
Part 1	Overview	
Chapter 1	Introduction	3
	Unified Administration and Customer Portal Overview	3
	Customer Portal Overview	4
	Switching the Tenant Scope	5
	Accessing Customer Portal	5
	Setting Up Your Network with Customer Portal	6
	Changing the Password on First Login	7
	Changing the Customer Portal Password	8
	Resetting the Password	8
	Extending the User Login Session	10
Part 2	Dashboard	
Chapter 2	Using the Dashboard	13
	About the Customer Portal Dashboard	13
	Tasks You Can Perform	13
	Field Descriptions	13
Chapter 3	Managing Objects	17
	Sorting Objects	17
	Viewing Object Details	17
	Searching for Text in an Object Data Table	18
Part 3	Monitoring the Customer Portal	
Chapter 4	Monitoring Security Alerts and Alarms	21
	About the Monitor Overview Page	21
	Tasks You Can Perform	21
	Field Descriptions	22
	Security Alerts Overview	22

	About the Generated Alerts Page	23
	Tasks You Can Perform	23
	Field Descriptions	23
	About the Security Alerts Definitions Page	24
	Tasks You Can Perform	24
	Field Descriptions	24
	Creating Security Alert Definitions	25
	Editing and Deleting Security Alert Definitions	26
	Editing Security Alert Definitions	26
	Deleting Security Alert Definitions	27
	Cloning Security Alert Definitions	27
Chapter 5	Monitoring Security and Device Events	29
	About the All Security Events Page	29
	Tasks You Can Perform	29
	Summary View	30
	Detail View	30
	About the Firewall Events Page	33
	Tasks You Can Perform	34
	Summary View	34
	Detail View	34
	About the Web Filtering Events Page	36
	Tasks You Can Perform	36
	Summary View	37
	Detail View	37
	About the IPsec VPNs Events Page	38
	Tasks You Can Perform	39
	Summary View	39
	Detail View	39
	About the Content Filtering Events Page	40
	Tasks You Can Perform	41
	Summary View	41
	Detail View	41
	About the Antispam Events Page	42
	Tasks You Can Perform	43
	Summary View	43
	Detail View	43
	About the Antivirus Events Page	44
	Tasks You Can Perform	44
	Summary View	45
	Detail View	45
	About the IPS Events Page	46
	Tasks You Can Perform	47
	Summary View	47
	Detail View	47
	About the Device Events Page	49
	Tasks You Can Perform	49
	Advanced Search	50
	Field Descriptions	51

	About the Screen Events Page	53
	Tasks You Can Perform	53
	Summary View	53
	Detail View	54
Chapter 6	Monitoring SD-WAN Events	57
	SD-WAN Events Overview	57
	About the SD-WAN Events Page	58
	Tasks You Can Perform	58
	Field Descriptions	58
Chapter 7	Monitoring Applications	61
	About the SLA Performance of a Single Tenant Page	61
	Tasks You Can Perform	61
	Field Descriptions	62
	Viewing the SLA Performance of a Site	63
	SLA Not Met by SLA Profiles	64
	Applications SLA Performance by Throughput	65
	SLA Performance for ALL	67
	Viewing the SLA Performance of an Application or Application Group	68
	Application Visibility Overview	69
	About the Application Visibility Page	69
	Tasks You Can Perform	70
	Chart View	70
	Grid View	71
	Selecting Devices	72
Chapter 8	Monitoring Threats	75
	About the Threats Map (Live) Page	75
	Tasks You Can Perform	75
	Field Descriptions	77
	Threat Types	78
Chapter 9	Monitoring Jobs	81
	About the Jobs Page	81
	Tasks You Can Perform	81
	Field Descriptions	81
	Field Descriptions	82
	Editing and Deleting Scheduled Jobs	83
	Editing Scheduled Jobs	83
	Deleting Scheduled Jobs	83
	Viewing Job Details	84

Part 4	Managing Resources	
Chapter 10	Managing Devices	87
	Multidepartment CPE Device Support	87
	About the Devices Page	88
	Tasks You Can Perform	88
	Field Descriptions	88
	Performing Return Material Authorization (RMA) for a Single-CPE Device	90
	Performing Return Material Authorization (RMA) for Dual-CPE Devices	92
	Performing RMA for an NFX Cluster	92
	Performing RMA for an SRX Cluster	94
	Granting RMA for a Device	95
	Granting RMA for a Single-CPE Device	95
	Granting RMA for a Dual-CPE Device	96
	Granting RMA for an SRX Device within an SRX Cluster	98
	Managing a Single CPE Device	99
	Rebooting a CPE Device	100
Chapter 11	Managing Device Images	103
	Device Images Overview	103
	About the Device Images Page	103
	Tasks You Can Perform	103
	Field Descriptions	103
	Deleting Device Images	104
Part 5	Managing Configuration	
Chapter 12	Managing Network Services	107
	Network Service Overview	107
	About the Network Services Page	108
	Tasks You Can Perform	108
	Field Descriptions	108
	About the Service Overview Page	109
	Tasks You Can Perform	110
	Field Descriptions	110
	About the Service Instances Page	111
	Tasks You Can Perform	111
	Field Descriptions	111
	Configuring VNF Properties	113
	vSRX VNF Configuration Settings	113
	LxCIPtable VNF Configuration Settings	117
	Cisco CSR-1000v VNF Configuration Settings	120
	Riverbed Steelhead VNF Configuration Settings	121

Chapter 13	Managing Firewall Policies	123
	Firewall Policy Overview	123
	About the Firewall Policy Page	124
	Tasks You Can Perform	124
	Field Descriptions	124
	Creating Firewall Policy Intents	125
	Editing, Cloning, and Deleting Firewall Policy Intents	131
	Editing Firewall Policy Intents	131
	Cloning Firewall Policy Intents	132
	Deleting Firewall Policy Intents	132
	Selecting Firewall Source	133
	Adding an End Point as Firewall Source	133
	Selecting Firewall Source Using Abbreviations	134
	Selecting a Firewall Source from the End Points Panel	134
	Creating and Selecting a Firewall Source from the End Points Panel	135
	Creating Addresses from Source	135
	Creating Departments from Source	135
	Selecting Firewall Destination	136
	Adding an End Point as Firewall Destination	137
	Selecting Firewall Destination Using Abbreviations	137
	Selecting a Firewall Destination from the End Points Panel	137
	Creating and Selecting a Firewall Destination from the End Points Panel	138
	Creating Addresses from Destination	138
	Creating Departments from Destination	139
	Firewall Policy Examples	139
	Example 1: Firewall Policy that Permits Traffic from Departments in Site A to the Departments in Site B	141
	Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B	143
	Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B	145
	Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A	146
	Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments	148
	Example 6: Firewall Policy that Denies Access to Social Networking Sites	154
	Example 7: Firewall Policy that Controls Access to an Address over the Internet (HTTP)	156
	Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service	161
	Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B	162
	Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A	164
	Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled	167
	Firewall Policy Schedules Overview	170

	About the Firewall Policy Schedules Page	170
	Tasks You Can Perform	170
	Field Descriptions	171
	Creating Schedules	171
	Editing, Cloning, and Deleting Schedules	173
	Editing Schedules	173
	Cloning Schedules	173
	Deleting Schedules	174
Chapter 14	Unified Threat Management	175
	UTM Overview	176
	UTM Licensing	177
	UTM Components	177
	Configuring UTM Settings	178
	About the UTM Profiles Page	179
	Tasks You Can Perform	179
	Field Descriptions	179
	Creating UTM Profiles	181
	Editing, Cloning, and Deleting UTM Profiles	183
	Editing UTM Profiles	184
	Cloning UTM Profiles	184
	Deleting UTM Profiles	185
	About the Web Filtering Profiles Page	185
	Tasks You Can Perform	186
	Field Descriptions	186
	Creating Web Filtering Profiles	187
	Editing, Cloning, and Deleting Web Filtering Profiles	191
	Editing Web Filtering Profiles	191
	Cloning Web Filtering Profiles	192
	Deleting Web Filtering Profiles	192
	About the Antivirus Profiles Page	193
	Tasks You Can Perform	193
	Field Descriptions	193
	Creating Antivirus Profiles	194
	Editing, Cloning, and Deleting Antivirus Profiles	196
	Editing Antivirus Profiles	196
	Cloning Antivirus Profiles	197
	Deleting Antivirus Profiles	197
	About the Antispam Profiles Page	198
	Tasks You Can Perform	198
	Field Descriptions	198
	Creating Antispam Profiles	199
	Editing, Cloning, and Deleting Antispam Profiles	201
	Editing Antispam Profiles	201
	Cloning Antispam Profiles	201
	Deleting Antispam Profiles	202
	About the Content Filtering Profiles Page	202
	Tasks You Can Perform	202
	Field Descriptions	203

	Creating Content Filtering Profiles	204
	Editing, Cloning, and Deleting Content Filtering Profiles	207
	Editing Content Filtering Profiles	207
	Cloning Content Filtering Profiles	207
	Deleting Content Filtering Profiles	208
	About the URL Patterns Page	209
	Tasks You Can Perform	209
	Field Descriptions	209
	Creating URL Patterns	209
	Editing, Cloning, and Deleting URL Patterns	211
	Editing URL Patterns	211
	Cloning URL Patterns	211
	Deleting URL Patterns	212
	About the URL Categories Page	212
	Tasks You Can Perform	212
	Field Descriptions	213
	Creating URL Categories	213
	Editing, Cloning, and Deleting URL Categories	214
	Editing URL Categories	214
	Cloning URL Categories	215
	Deleting URL Categories	215
Chapter 15	Managing SD-WAN	217
	SLA Profiles and SD-WAN Policies Overview	217
	SLA Profiles	217
	SD-WAN Policies	218
	About the SD-WAN Policy Page	220
	Tasks You Can Perform	220
	Field Descriptions	220
	Creating SD-WAN Policy Intents	221
	Editing and Deleting SD-WAN Policy Intents	225
	Editing SD-WAN Policy Intents	225
	Deleting SD-WAN Policy Intents	225
	About the Application SLA Profiles Page	226
	Tasks You Can Perform	226
	Field Descriptions	226
	Creating SLA Profiles	227
	Editing and Deleting SLA Profiles	229
	Editing an SLA Profile	229
	Deleting SLA Profiles	230
Chapter 16	Managing NAT Policies	231
	NAT Policies Overview	232
	About the NAT Policies Page	234
	Tasks You Can Perform	235
	Field Descriptions	235
	Creating NAT Policies	235
	Editing and Deleting NAT Policies	237
	Editing NAT Policies	237
	Deleting NAT Policies	238

	About the Single NAT Policy Page	238
	Tasks You Can Perform	238
	Field Descriptions	239
	Creating NAT Policy Rules	240
	Editing, Cloning, and Deleting NAT Policy Rules	246
	Editing NAT Policy Rules	246
	Cloning NAT Policy Rules	246
	Deleting NAT Policy Rules	247
	Deploying NAT Policy Rules	247
	Selecting NAT Source	248
	Adding an Endpoint as NAT Source	248
	Selecting Interfaces when GWR Resides Inside an NFX Box	249
	Selecting NAT Source Using Abbreviations	249
	Selecting a NAT Source from the End Points Panel	250
	Creating and Selecting a NAT Source from the End Points Panel	250
	Creating Addresses from Source Field	251
	Selecting NAT Destination	252
	Adding an Endpoint as NAT Destination	252
	Selecting Interfaces when GWR Resides Inside an NFX Box	252
	Selecting NAT Destination Using Abbreviations	253
	Selecting a NAT Destination from the End Points Panel	253
	Creating and Selecting a NAT Destination from the End Points Panel	254
	Creating Addresses from Destination Field	254
	Creating Services from Destination Field	255
	NAT Pools Overview	255
	About the NAT Pools Page	256
	Tasks You Can Perform	256
	Creating NAT Pools	257
	Editing, Cloning, and Deleting NAT Pools	259
	Editing NAT Pools	259
	Cloning NAT Pools	260
	Deleting NAT Pools	260
Chapter 17	Managing SSL Proxies	261
	SSL Forward Proxy Overview	261
	Supported Ciphers in Proxy Mode	263
	Server Authentication	263
	Root CA	264
	Trusted CA List	264
	Session Resumption	265
	SSL Proxy Logs	265
	About the SSL Proxy Policy Page	266
	Tasks You Can Perform	266
	Field Descriptions	267
	Creating SSL Proxy Policy Intents	267
	Editing, Cloning, and Deleting SSL Proxy Policy Intents	270
	Editing SSL Proxy Policy Intents	271
	Cloning SSL Proxy Policy Intents	271
	Deleting SSL Proxy Policy Intents	272

	Understanding How SSL Proxy Policy Intents Are Applied	272
	Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match	273
	Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match	273
	Example 3: Applying SSL Proxy Policy Intents on Internal (Site-to-Site) Traffic	274
	About the SSL Proxy Profiles Page	274
	Tasks You Can Perform	274
	Widget Descriptions	275
	Creating SSL Forward Proxy Profiles	276
	Editing, Cloning, and Deleting SSL Forward Proxy Profiles	280
	Editing SSL Forward Proxy Profiles	280
	Cloning SSL Forward Proxy Profiles	280
	Deleting SSL Forward Proxy Profiles	281
	Configuring and Deploying an SSL Forward Proxy Policy	282
Chapter 18	Managing Shared Objects	285
	Addresses and Address Groups Overview	285
	About the Addresses Page	286
	Tasks You Can Perform	286
	Field Descriptions	286
	Creating Addresses or Address Groups	287
	Editing, Cloning, and Deleting Addresses and Address Groups	289
	Editing Addresses and Address Groups	289
	Cloning Addresses and Address Groups	290
	Deleting Addresses and Address Groups	290
	Services and Service Groups Overview	291
	About the Services Page	291
	Tasks You Can Perform	292
	Field Descriptions	292
	Creating Services and Service Groups	292
	Creating Protocols	294
	Editing and Deleting Protocols	297
	Editing Protocols	297
	Deleting Protocols	298
	Editing, Cloning, and Deleting Services and Service Groups	298
	Editing Services and Service Groups	298
	Cloning Services or Service Groups	299
	Deleting Services and Service Groups	299
	Application Signatures Overview	300
	About the Application Signatures Page	300
	Tasks You Can Perform	300
	Field Descriptions	301
	Creating Application Signature Groups	301
	Editing, Cloning, and Deleting Application Signature Groups	302
	Editing Application Signature Groups	303
	Cloning Application Signature Groups	303
	Deleting Application Signature Groups	303

	About the Departments Page	304
	Tasks You Can Perform	304
	Field Descriptions	304
	Creating a Department	305
	Modifying a Department	306
	Deleting a Department	306
Chapter 19	Managing Deployments	309
	Deploying Policies Overview	309
	About the Deployments Page	310
	Tasks You Can Perform	310
	Field Descriptions	310
	Using the Deployment Icon to Deploy Policies	311
	Deploying Policies	312
Part 6	Managing Sites and Site Groups	
Chapter 20	Managing Sites	317
	About the Sites Page	317
	Tasks You Can Perform	318
	Field Descriptions	318
	Local Breakout Overview	319
	Multihoming Overview	320
	Device Redundancy Support Overview	321
	Prerequisites for SRX Series Devices	321
	Supported Connection Plans	322
	Create and Configure an SD-WAN Site	322
	Dual CPE Devices Logical Topology for NFX Network Services Platform	322
	Dual CPE Devices Logical Topology for SRX Series Gateway Devices	323
	Creating Spoke Sites for Hybrid WAN Deployment	323
	Creating Local Service Edge Sites for Hybrid WAN Deployment	325
	Creating Regional Service Edge Sites for Hybrid WAN Deployment	327
	Creating On-Premise Hub Sites for SD-WAN Deployment	329
	Creating On-Premise Spoke Sites for SD-WAN Deployment	331
	Creating Cloud Hub Sites for SD-WAN Deployment	336
	Creating Cloud Spoke Sites for SD-WAN Deployment	338
	Provisioning a Cloud Spoke Site in AWS VPC	343
	Add a Cloud Spoke Site	343
	Configure the Cloud Spoke Site	344
	Download the Cloud Formation Template	345
	Provision the Device on AWS Server	345
	Activate the Device	346
	Importing Multiple Sites	347
	Managing a Single Site	348
	Configuring a Single Site	349
	Managing LAN Segments on a Tenant Site	352
	Creating LAN Segments	352
	Deploying a LAN Segment	354
	Reassigning a LAN Segment to a Department	354
	Deleting LAN Segments	355

	Activating a CPE Device	355
	Activating Dual CPE Devices (Device Redundancy)	358
	Viewing the History of Tenant Device Activation Logs	360
	Configuring VRFs and PNE Details for a Site in a Centralized Deployment	362
Chapter 21	Managing Site Groups	365
	About the Site Groups Page	365
	Tasks You Can Perform	365
	Field Descriptions	365
	Creating Site Groups	366
Part 7	Viewing Reports	
Chapter 22	Security Reports	369
	Reports Overview	369
	About the Security Report Definitions Page	370
	Tasks You Can Perform	370
	Field Descriptions	370
	Performing Different Actions on Reports	371
	About the Security Generated Reports Page	372
	Tasks You Can Perform	372
	Field Descriptions	372
	Creating Log Report Definition	373
	Creating Bandwidth Report Definition	375
	Editing and Deleting Log Report Definitions	376
	Editing the Log Report Definition	376
	Deleting Log Report Definitions	376
	Editing and Deleting Bandwidth Report Definitions	377
	Editing the Bandwidth Report Definition	377
	Deleting Bandwidth Report Definitions	378
Chapter 23	SD-WAN Reports	379
	About the SD-WAN Report Definitions Page	379
	Tasks You Can Perform	379
	Field Descriptions	380
	Editing and Deleting SD-WAN Report Definitions	380
	Editing the SD-WAN Report Definition	381
	Deleting SD-WAN Report Definitions	381
	Creating SD-WAN Tenant Performance Report Definition	382
	Creating SD-WAN Site Performance Report Definition	384
	About the SD-WAN Generated Reports Page	386
	Tasks You Can Perform	386
	Field Descriptions	386

Part 8	Administration	
Chapter 24	Managing Tenant Users	391
	Role-Based Access Control Overview	391
	About the Tenant Users Page	392
	Tasks You Can Perform	392
	Field Descriptions	392
	Adding Tenant Users	393
	Editing and Deleting Tenant Users	394
	Editing Tenant Users	394
	Deleting Tenant Users	395
Chapter 25	Licenses	397
	About the Licenses Page	397
	Tasks You Can Perform	397
	Field Descriptions	397
Chapter 26	Signature Database	399
	Signature Database Overview	399
	About the Active Database Page	400
	Tasks You Can Perform	400
	Field Descriptions	400
	Installing Signatures	401
Chapter 27	Managing Certificates	403
	Certificates Overview	403
	About the Certificates Page	403
	Tasks You Can Perform	404
	Field Descriptions	404
	Importing a Certificate	405
	Installing and Uninstalling Certificates	407
	Installing a Certificate	407
	Uninstalling a Certificate	407
Chapter 28	Managing Juniper Identity Management Service	409
	Juniper Identity Management Service Overview	409
	Access Token Query	410
	Batch or Periodic Query	410
	IP Address Query	410
	User Mapping Query	411
	About the Identity Management Page	411
	Tasks You Can Perform	412
	Configuring CSO and JIMS Connection	412
	Configuring JIMS for an SRX Device	414

List of Figures

Part 5	Managing Configuration	
Chapter 13	Managing Firewall Policies	123
	Figure 1: Topology Diagram	140
Chapter 14	Unified Threat Management	175
	Figure 2: UTM Components	177
Chapter 17	Managing SSL Proxies	261
	Figure 3: SSL Forward Proxy on an Encrypted Payload	262
Part 6	Managing Sites and Site Groups	
Chapter 20	Managing Sites	317
	Figure 4: Dual CPE Device Topology - NFX Network Services Platform	322
	Figure 5: Dual CPE Device Topology - SRX Series Devices	323
Part 8	Administration	
Chapter 28	Managing Juniper Identity Management Service	409
	Figure 6: CSO-JIMS-SRX Connectivity Configuration	412

List of Tables

	About the Documentation	xxiii
	Table 1: Notice Icons	xxiv
	Table 2: Text and Syntax Conventions	xxiv
Part 1	Overview	
Chapter 1	Introduction	3
	Table 3: Customer Portal Menu	6
	Table 4: Fields on the Change Password Page	7
	Table 5: Fields on the Reset Password Page	9
Part 2	Dashboard	
Chapter 2	Using the Dashboard	13
	Table 6: Widgets on the Customer Portal Dashboard	14
Part 3	Monitoring the Customer Portal	
Chapter 4	Monitoring Security Alerts and Alarms	21
	Table 7: Fields on the Monitor Overview Page	22
	Table 8: Fields on the Generated Alerts Page	23
	Table 9: Fields on the Security Alert Definitions Page	24
	Table 10: Fields on the Security Alert Definitions Page	25
Chapter 5	Monitoring Security and Device Events	29
	Table 11: Widgets on the All Events Summary View Page	30
	Table 12: Fields on the All Events Detail View Page	31
	Table 13: Widgets on the Summary View Page	34
	Table 14: Fields on the Detail View Page	34
	Table 15: Widgets on the Summary View Page	37
	Table 16: Fields on the Detail View Page	37
	Table 17: Widgets on the Summary View Page	39
	Table 18: Fields on the Detail View Page	39
	Table 19: Widgets on the Summary View Page	41
	Table 20: Fields on the Detail View Page	41
	Table 21: Fields on the Detail View Page	43
	Table 22: Widgets on the Summary Page	45
	Table 23: Fields on the Detail View Page	45
	Table 24: Widgets on the Summary Page	47
	Table 25: Fields on the Detail View Page	48
	Table 26: Fields on the Device Events Detailed View Page	51
	Table 27: Widgets on the Summary Page	53

	Table 28: Fields on the Detail View Page	54
Chapter 6	Monitoring SD-WAN Events	57
	Table 29: Fields on the SD-WAN Events Page	58
Chapter 7	Monitoring Applications	61
	Table 30: Fields on the SLA Performance of a Single Tenant Page	62
	Table 31: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views	62
	Table 32: Fields on the Applications SLA Performance by Throughput Grid View	66
	Table 33: Fields on the Application or Application Group Details Page	68
	Table 34: Fields on the Chart View	70
	Table 35: Widgets on the Grid View	71
	Table 36: Detailed View of Applications	72
Chapter 8	Monitoring Threats	75
	Table 37: Country-Specific Threat Information	76
	Table 38: Fields on the Threats Map (Live) Page	77
	Table 39: Types of Threats	78
Chapter 9	Monitoring Jobs	81
	Table 40: Fields on the Jobs Page	81
	Table 41: Fields on the Scheduled Jobs Page	82
Part 4	Managing Resources	
Chapter 10	Managing Devices	87
	Table 42: Widgets on the Devices Page	89
	Table 43: Fields on the Devices Page	89
	Table 44: Fields on the Grant RMA for Single-CPE Device Page	96
	Table 45: Fields on the Grant RMA for Dual-CPE Device Page	97
	Table 46: Fields on the Grant RMA for Device Page (for SRX Device in an SRX Cluster)	98
Chapter 11	Managing Device Images	103
	Table 47: Fields on the Device Images Page	104
Part 5	Managing Configuration	
Chapter 12	Managing Network Services	107
	Table 48: Widgets on the Network Services Page	108
	Table 49: Fields on the Network Services Page	108
	Table 50: Fields on the Network Service Detail Page	109
	Table 51: Fields on the Service Overview Page	110
	Table 52: Fields on the Service Instances Page	112
	Table 53: Fields on the Service Instance Details Page	112
	Table 54: Fields for the vSRX Base Settings	114
	Table 55: Fields for the vSRX Firewall Settings	115
	Table 56: Fields for the LxCIP Base Settings	118
	Table 57: Fields for the LxCIP Firewall Policy Settings	118

	Table 58: Fields for the LxCIP NAT Policy Settings	119
	Table 59: Fields for the CSR-1000v Base Settings	120
	Table 60: Fields for the CSR-1000v Firewall Settings	121
Chapter 13	Managing Firewall Policies	123
	Table 61: Fields on the Firewall Policy Page	125
	Table 62: Fields on the Create Firewall Policy Page	126
	Table 63: LAN Segments Definition	141
	Table 64: Firewall Policy Intent Definition for Example - 1	142
	Table 65: Firewall Policy Intent Resolution for Example - 1	142
	Table 66: Firewall Policy Intent Definition for Example - 2	143
	Table 67: Firewall Policy Intent Resolution for Example - 2	144
	Table 68: Firewall Policy Intent Definition for Example - 3	145
	Table 69: Firewall Policy Intent Resolution for Example - 3	145
	Table 70: Firewall Policy Intent Definition for Example - 4	146
	Table 71: Firewall Policy Intent Resolution for Example - 4	146
	Table 72: Firewall Policy Intent Definition for Example - 5	148
	Table 73: Firewall Policy Intent Resolution for Example - 5	148
	Table 74: Firewall Policy Intent Definition for Example - 6	154
	Table 75: Firewall Policy Intent Resolution for Example - 6	154
	Table 76: Firewall Policy Intent Definition for Example - 7	156
	Table 77: Firewall Policy Intent Resolution for Example - 7	156
	Table 78: Firewall Policy Intent Definition for Example - 8	161
	Table 79: Firewall Policy Intent Resolution for Example - 8	161
	Table 80: Firewall Policy Intent Definition for Example - 9	162
	Table 81: Firewall Policy Intent Resolution for Example - 9	162
	Table 82: Firewall Policy Intent Definition for Example - 10	164
	Table 83: Firewall Policy Intent Resolution for Example - 10	165
	Table 84: Firewall Policy Intent Definition for Example - 11	167
	Table 85: Firewall Policy Intent Resolution for Example - 11	167
	Table 86: Fields on the Firewall Policy Schedules Page	171
	Table 87: Fields on the Create Schedules Page	172
Chapter 14	Unified Threat Management	175
	Table 88: UTM Settings	178
	Table 89: UTM Profiles Page Fields	179
	Table 90: UTM Profile Details Page Fields	180
	Table 91: UTM Profile Settings	181
	Table 92: Web Filtering Solutions Supported	185
	Table 93: Web Filtering Profiles Page Fields	186
	Table 94: Web Filtering Profile Details Page Fields	186
	Table 95: Creating Web Filtering Profiles Settings	188
	Table 96: Select URL Categories Settings	190
	Table 97: Antivirus Profiles Page Fields	193
	Table 98: Antivirus Profiles Details Page Fields	194
	Table 99: Antivirus Profile Settings	195
	Table 100: Antispam Profiles Page Fields	198
	Table 101: Antispam Profile Details Page Fields	199
	Table 102: Antispam Profile Settings	200
	Table 103: Content Filtering Profiles Page Fields	203

	Table 104: Content Filtering Profiles Details Page Fields	203
	Table 105: Supported Content Filter Types	204
	Table 106: Content Filtering Profile Settings	205
	Table 107: URL Patterns Page Fields	209
	Table 108: Create URL Patterns Settings	210
	Table 109: URL Categories Page Fields	213
	Table 110: Create URL Categories Settings	214
Chapter 15	Managing SD-WAN	217
	Table 111: SLA Profile Categories	217
	Table 112: Fields on the SD-WAN Policy Page	220
	Table 113: Fields on the Create SD-WAN Policy Intent Page	222
	Table 114: Fields on the Application SLA Profiles Page	226
	Table 115: Fields on the Create SLA Profile page	227
Chapter 16	Managing NAT Policies	231
	Table 116: Persistent NAT Support	233
	Table 117: Translated Address Pool Selection for Source NAT	234
	Table 118: Translated Address Pool Selection for Destination NAT And Static NAT	234
	Table 119: Fields on the NAT Policies Page	235
	Table 120: Fields on the Create NAT Policy Page	236
	Table 121: Fields on the Single NAT Policy Page	239
	Table 122: Fields on the Single NAT Policy Page for Creating NAT Rules	241
	Table 123: Fields on the Advanced Settings Page for Source NAT Rule	244
	Table 124: Fields on the Advanced Settings Page for Static NAT Rule	245
	Table 125: NFX and GWR Interface Mapping	249
	Table 126: NFX and GWR Interface Mapping	252
	Table 127: Fields on the NAT Pools Page	256
	Table 128: Fields on the Create NAT Pool Page	257
Chapter 17	Managing SSL Proxies	261
	Table 129: Supported Ciphers in Proxy Mode	263
	Table 130: SSL Proxy Logs	265
	Table 131: SSL Proxy Log Prefixes	265
	Table 132: SSL Proxy Policy Page Fields	267
	Table 133: Create SSL Proxy Policy Intent Settings	268
	Table 134: Keywords for Filtering Endpoints	270
	Table 135: Creating Endpoints	270
	Table 136: (Example) Match Between Firewall Policy Intent and SSL Proxy Policy Intent	273
	Table 137: (Example) No Match Between Firewall Policy Intent and SSL Proxy Policy Intent	274
	Table 138: (Example) Firewall Policy and SSL Proxy Policy Intents for Site-to-Site Traffic	274
	Table 139: Fields on the SSL Proxy Profiles Page	275
	Table 140: View SSL Forward Proxy Profile Details Page Fields	275
	Table 141: Creating SSL Forward Proxy Profile Settings	277
Chapter 18	Managing Shared Objects	285

	Table 142: Fields on the Addresses Page	286
	Table 143: Fields on the Create Addresses Page	287
	Table 144: Address Group Settings	288
	Table 145: Fields on the Service Page	292
	Table 146: Service Settings	293
	Table 147: Service Group Settings	293
	Table 148: Fields on Create Protocol Page Settings	295
	Table 149: Create Protocol Type Settings	295
	Table 150: Fields on the Application Signatures Page	301
	Table 151: Fields on the Create Application Signature Group Page	302
	Table 152: Fields on the Departments Page	304
	Table 153: Fields on the Create Departments Page	305
	Table 154: Fields on the Edit Department Page	306
Chapter 19	Managing Deployments	309
	Table 155: Fields on the Deployments Page	310
	Table 156: Fields on the Deployment Panel	312
	Table 157: Fields on the Deploy Page	313
Part 6	Managing Sites and Site Groups	
Chapter 20	Managing Sites	317
	Table 158: Fields on the Sites Page	318
	Table 159: Fields on the Add Spoke Site Page	323
	Table 160: Fields on the Add Local Service Edge Site Page	326
	Table 161: Fields on the Add Regional Service Edge Site Page	328
	Table 162: Fields on the Add On-Premise Hub Site Page	329
	Table 163: Fields on the Add On-Premise Spoke Site Page	332
	Table 164: Fields on the Add Cloud Site Page	337
	Table 165: Fields on the Add Cloud Spoke Site Page	339
	Table 166: Fields on the Configure Site Page	349
	Table 167: Create LAN Segment Page	353
	Table 168: Fields on the Activate Device Page	357
	Table 169: Fields on the Activate Device Page	358
	Table 170: Fields on the ZTP History Page	361
	Table 171: Fields on the ZTP Logs Page	361
	Table 172: Fields on the Job Status Page	361
	Table 173: Fields on the Device Configuration Page	362
Chapter 21	Managing Site Groups	365
	Table 174: Fields on the Site Groups Page	365
Part 7	Viewing Reports	
Chapter 22	Security Reports	369
	Table 175: Fields on the Report Definitions Page	370
	Table 176: Fields on the Generated Reports Page	372
	Table 177: Fields on the Create Log Report Definition Page	373
	Table 178: Fields on the Create Bandwidth Report Definition Page	375
Chapter 23	SD-WAN Reports	379

	Table 179: Fields on the SD-WAN Report Definitions Page	380
	Table 180: Fields on the Create Tenant Performance Report Definition	382
	Table 181: Fields on the Site Performance Report Definition Page	384
	Table 182: Fields on the SD-WAN Generated Reports Page	386
Part 8	Administration	
Chapter 24	Managing Tenant Users	391
	Table 183: Roles and Access Privileges	391
	Table 184: Fields on the Users Page	392
	Table 185: Fields on the Add User Page	394
Chapter 25	Licenses	397
	Table 186: Fields on the License Files Page	397
Chapter 26	Signature Database	399
	Table 187: Fields on the Active Database Page	400
Chapter 27	Managing Certificates	403
	Table 188: Fields on the Certificates Page	404
	Table 189: Fields on the Detailed View Page	404
	Table 190: Import Certificate Settings	406
Chapter 28	Managing Juniper Identity Management Service	409
	Table 191: Fields on the SRX-to-JIMS Configuration Panel	415

About the Documentation

- Documentation and Release Notes on page xxiii
- Documentation Conventions on page xxiii
- Documentation Feedback on page xxv
- Requesting Technical Support on page xxvi

Documentation and Release Notes

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

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

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

Documentation Conventions

Table 1 on page xxiv 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 xxiv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS CLI User Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>

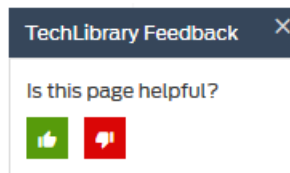
Table 2: Text and Syntax Conventions (continued)

Convention	Description	Examples
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	<pre>[edit] routing-options { static { route default { nexthop <i>address</i>; retain; } } }</pre>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

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



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

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>

- Join and participate in the Juniper Networks Community Forum:
<https://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

PART 1

Overview

- [Introduction on page 3](#)

CHAPTER 1

Introduction

- [Unified Administration and Customer Portal Overview on page 3](#)
- [Customer Portal Overview on page 4](#)
- [Switching the Tenant Scope on page 5](#)
- [Accessing Customer Portal on page 5](#)
- [Setting Up Your Network with Customer Portal on page 6](#)
- [Changing the Password on First Login on page 7](#)
- [Changing the Customer Portal Password on page 8](#)
- [Resetting the Password on page 8](#)
- [Extending the User Login Session on page 10](#)

Unified Administration and Customer Portal Overview

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

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

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

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

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

Related Documentation

- [Customer Portal Overview on page 4](#)
- [Switching the Tenant Scope on page 5](#)
- [Firewall Policy Overview on page 123](#)
- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [NAT Policies Overview on page 232](#)

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/

Related Documentation

- [Accessing Customer Portal on page 5](#)
- [Changing the Customer Portal Password on page 8](#)

Switching the Tenant Scope

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

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

To switch from one scope to another:

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

Related Documentation

- [Unified Administration and Customer Portal Overview on page 3](#)
- [Role-Based Access Control Overview on page 391](#)

Accessing Customer Portal

To start Customer Portal:

1. Obtain the following information from your service provider:
 - IP address for the Customer Portal host.
 - Login credentials:
 - Username
 - Password
2. Using a Web browser, access the URL for Customer Portal.

For example, if the IP address of the host on which Customer Portal resides is 192.0.2.1, the URL is <https://192.0.2.1>.



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

3. Log in with the credentials provided.

The Customer Portal Dashboard page appears and you can now start to activate sites.

From CSO Release 3.1 onward, the customer portal functionality has been enhanced to provide a richer user experience. 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 3 on page 6](#).

Table 3: Customer Portal Menu

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

- Related Documentation**
- [Changing the Customer Portal Password on page 8](#)
 - [Customer Portal Overview on page 4](#)

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 [“Creating On-Premise Spoke Sites for SD-WAN Deployment” on page 331](#).
2. Activate the on-premise site. See [“Configuring a Single Site” on page 349](#).
3. Deploy network services. See [“Managing a Single Site” on page 348](#).
4. View and manage policies.
 - View and manage a firewall policy. See [“Creating Firewall Policy Intents” on page 125](#) and [“Deploying Policies” on page 312](#).
 - View and manage an SD-WAN policy. See [“Creating SLA Profiles” on page 227](#), [“Creating SD-WAN Policy Intents” on page 221](#), and [“Deploying Policies” on page 312](#).

Related Documentation • [Accessing Customer Portal on page 5](#)

Changing the Password on First Login

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

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

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

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



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

2. Change your password following the guidelines provided in [Table 4 on page 7](#).

3. Click **Ok**.



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

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

Table 4: Fields on the Change Password Page

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

- Related Documentation**
- [Accessing Customer Portal on page 5](#)
 - [Changing the Customer Portal Password on page 8](#)
 - [Resetting the Password on page 8](#)

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.

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 on page 4](#)
 - [Accessing Customer Portal on page 5](#)

Resetting the Password

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



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

To reset the password:

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

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



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

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



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

3. Click **OK**.

The Reset Password page appears.

4. Change your password following the guidelines provided in [Table 5 on page 9](#).

5. Click **OK**.

Your password is reset.

Table 5: 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>NOTE: The password strength indicator displays the efficiency of the password that you enter. You cannot proceed to the next step if the password strength indicator shows that the password is weak.</p>
Confirm Password	<p>Reenter the password for confirmation.</p> <p>You can select Show Password to view the password.</p>

- Related Documentation
- [Accessing Customer Portal on page 5](#)
 - [Changing the Password on First Login on page 7](#)

- [Changing the Customer Portal Password on page 8](#)

Extending the User Login Session

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

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

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

To extend the login session:

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

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

Related Documentation

- [Changing the Customer Portal Password on page 8](#)

PART 2

Dashboard

- [Using the Dashboard on page 13](#)
- [Managing Objects on page 17](#)

CHAPTER 2

Using the Dashboard

- [About the Customer Portal Dashboard on page 13](#)

About the Customer Portal Dashboard

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

Each time you log in to Customer Portal, the first thing you see is a user-configurable dashboard that offers you a customized view of network services through its widgets.

You can drag these widgets from the 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 on a per user basis.
- Update the dashboard or an individual widget by clicking the refresh icon.
- Show or hide widget thumbnails by clicking **Select Widgets** at the top of the page.
- Add a widget to the dashboard by dragging the widget from the palette or thumbnail container into the workspace.
- Delete a widget from the dashboard page by clicking the delete icon (X) in the title bar.

Field Descriptions

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

[Table 6 on page 14](#) describes the dashboard widgets.

Table 6: Widgets on the Customer Portal Dashboard

Widget	Description
Alerts Donut Chart	<p>View 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>View the top five tenant sites receiving alerts.</p> <ul style="list-style-type: none"> • Name—Name of the tenant site. • Location—Location of the tenant site. • Status—Type of alerts received: critical, major, or minor.
Top Sites not meeting SLA	<p>View a bar chart of the top tenant sites that did not meet SLA requirements and the percentage of time that SLA requirements were not met.</p> <p>Sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles not meeting SLA	<p>View 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>Sort the information based on location and period ranging from the last hour to the last month.</p>
Top Sites Switching Links	<p>View 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>Sort the information based on profile and period ranging from the last hour to the last month.</p>
Top Profiles Switching Links	<p>View 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>Sort the information based on location and period ranging from the last hour to the last month.</p>
Top Applications by Throughput	<p>View 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>Sort the information based on profile, location, and time period.</p>
Firewall: Top Denials	<p>View a column chart of the top requests denied by the firewall based on their source IP addresses, sorted by count.</p> <p>Sort the information based on time period ranging from 5 minutes to 7 days.</p>
Firewall: Top Events	<p>View a bar chart of the top firewall events of the network traffic, sorted by count.</p> <p>Sort the information based on time period ranging from 5 minutes to 7 days.</p>
IPS: Top Events	<p>View the top IPS events of the network traffic, sorted by count.</p> <p>Sort the information based on time period ranging from 5 minutes to 7 days.</p>

Table 6: Widgets on the Customer Portal Dashboard (continued)

Widget	Description
Applications: Most Sessions	View a bar chart of the top applications with a maximum number of sessions, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
IP: Top Destinations	View the top IP destination addresses of the network traffic, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
IP: Top Sources	View the top IP source addresses of the network traffic, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
IP: Top Spams by Source IPs	View the number of spams detected by the source IPs. Sort the information based on time period ranging from 5 minutes to 7 days.
Virus: Top Blocked	View viruses with the maximum number of blocks, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
Web Filtering: Top Blocked Websites	View a bar chart of websites with the maximum number of blocks, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
IP: Top Source IPs by Volume	View the top source IP addresses based on volume of traffic, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
Application: Top Application by Volume	View the applications based on volume of traffic, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
IP: Top Users/IP by Sessions	View the top source IP addresses by sessions, sorted by count. Sort the information based on time period ranging from 5 minutes to 7 days.
Threat Map: Virus	View a world map showing total virus event count across countries. Sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.
Threat Map: IPS	World map showing total IPS event count across countries. Sort the information based on source, destination, and time period ranging from 5 minutes to 7 days.

Related Documentation • [Customer Portal Overview on page 4](#)

CHAPTER 3

Managing Objects

- [Sorting Objects on page 17](#)
- [Viewing Object Details on page 17](#)
- [Searching for Text in an Object Data Table on page 18](#)

Sorting Objects

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

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

To show or hide an object:

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

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

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

The objects are displayed or hidden as per the selection.

Related Documentation

- [Searching for Text in an Object Data Table on page 18](#)

Viewing Object Details

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

To view details for an object:

- Right-click the object that you want to see the detailed view for and click **Quick View**, or select the object and click **More > Details**.
- Alternatively, hover over the object name and click the **Detailed View** icon that appears before it.

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

**Related
Documentation**

- [Sorting Objects on page 17](#)

Searching for Text in an Object Data Table

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

To search for text:

1. Enter partial text or full text of the keyword in the search bar and click the search icon.
The search results are displayed.
2. Click **X** next to a search keyword or click **Clear All** to clear the search results.

**Related
Documentation**

- [Sorting Objects on page 17](#)
- [Viewing Object Details on page 17](#)

PART 3

Monitoring the Customer Portal

- [Monitoring Security Alerts and Alarms on page 21](#)
- [Monitoring Security and Device Events on page 29](#)
- [Monitoring SD-WAN Events on page 57](#)
- [Monitoring Applications on page 61](#)
- [Monitoring Threats on page 75](#)
- [Monitoring Jobs on page 81](#)

CHAPTER 4

Monitoring Security Alerts and Alarms

- [About the Monitor Overview Page on page 21](#)
- [Security Alerts Overview on page 22](#)
- [About the Generated Alerts Page on page 23](#)
- [About the Security Alerts Definitions Page on page 24](#)
- [Creating Security Alert Definitions on page 25](#)
- [Editing and Deleting Security Alert Definitions on page 26](#)
- [Cloning Security Alert Definitions on page 27](#)

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 cloud hub sites.
- View multiple sites.

Field Descriptions

Table 7 on page 22 shows the descriptions of the fields on the Monitor Overview page.

Table 7: Fields on the Monitor Overview Page

Field	Description
Sites	View the sites at which the service is deployed. Click the Sites drop-down list and select Show sites
Connections	View the connections in the network. Click the Connections drop-down list and select Show connections .
Only the node with alerts	View the nodes with issues with the service. Click the drop-down list located next to the Only the nodes with alerts check box and select the type of alerts. <ul style="list-style-type: none"> • Critical—Issues that prevent the node from working and require action from the operator. The nodes with critical alerts are displayed in red. • Major—Issues that prevent the node from working at this time, but they do not require action from the operator. The nodes with major alerts are displayed in orange. • Minor—Issues that allow a node to continue working, but not optimally. The network operator may need to take action to resolve the issue. The nodes with minor alerts are displayed in yellow. <p>NOTE: The nodes without any alerts are displayed in blue.</p>

- Related Documentation**
- [About the Security Alerts Definitions Page on page 24](#)
 - [Creating Security Alert Definitions on page 25](#)

Security 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. See "[Creating Security Alert Definitions](#)" on page 25 for using data criteria from filters.
- 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 Security Alerts Definitions Page on page 24](#)
- [Creating Security Alert Definitions on page 25](#)

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

Field Descriptions

[Table 8 on page 23](#) provides guidelines on using the fields on the Generated Alerts page.

Table 8: Fields on the Generated Alerts Page

Field	Description
Time	View the date and time when the alert was generated.
Alert Name	View the name of the alert.
Alert Description	View the description of the alert.

Table 8: Fields on the Generated Alerts Page (continued)

Field	Description
Alert Source	View the source address of the alert.
Alert Type	View the type of alert.
Severity	View the severity of the alert.
Site	View the tenant site.
Object Type	View the object type.
Alert ID	View the alert ID.

Related Documentation

- [About the Security Alerts Definitions Page on page 24](#)

About the Security Alerts Definitions Page

To access this page, click **Monitor > Alerts & Alarms > Security Alert Definitions**.

Use this page 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 page:

- Create security alert definition. See [“Creating Security Alert Definitions” on page 25](#).
- Edit and delete security alert definition. See [“Editing and Deleting Security Alert Definitions” on page 26](#).
- Clone security alert definition. See [“Cloning Security Alert Definitions” on page 27](#).

Field Descriptions

[Table 9 on page 24](#) provides guidelines on using the fields on the Security Alert Definitions page.

Table 9: Fields on the Security Alert Definitions Page

Field	Description
Alert Name	View the name of the alert.
Alert Description	View the description for the alert.
Filter	View filter values of the alert.

Table 9: Fields on the Security Alert Definitions Page (continued)

Field	Description
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**
- [Security Alerts Overview on page 22](#)
 - [Creating Security Alert Definitions on page 25](#)

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 > Security Alert Definitions**.
The Security Alert Definitions page appears.
2. Click the create icon (+) or add icon (+).
The Create an Alert Definition page appears.
3. Complete the configuration according to the guidelines provided in [Table 10 on page 25](#).
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 10: Fields on the Security Alert Definitions Page

Field	Description
General	
Alert Name	Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.

Table 10: Fields on the Security Alert Definitions Page (continued)

Field	Description
Alert Description	Enter a description for the alerts; maximum length is 1024 characters.
Alert Type	Displays the type of alert that is system-based.
Status	Select the Active check box to view only the active alerts.
Severity	Select the severity level of the alert: info, minor, major, critical.
Trigger	
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"> Click the Use data criteria from filters link. The Add Saved Filters page appears. Select the filters to be added. Click OK.
Add Data Criteria	Specifies the data criteria based on the Time Span period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.
Recipient(s)	
E-mail Address(es)	Specify the e-mail addresses for the recipients of the alert notification.
Custom Message	Enter a custom string for identifying the type of alert in the alert notification e-mail.

- Related Documentation**
- [About the Security Alerts Definitions Page on page 24](#)
 - [Editing and Deleting Security Alert Definitions on page 26](#)

Editing and Deleting Security Alert Definitions

You can edit and delete security alert definitions.

- [Editing Security Alert Definitions on page 26](#)
- [Deleting Security Alert Definitions on page 27](#)

Editing Security Alert Definitions

To edit the security alert definition:

1. Select **Monitor > Alerts & Alarms > Security Alert Definitions**.
The Security Alerts Definition page appears.
2. Select the check box of the security alert definition that you want to modify, and click the edit icon.

The Edit Alert Definition page appears. The options available on the Create Alert Definition page are available for editing.

3. Update the configuration as needed.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.

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 > Security Alerts**.

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

- [About the Security Alerts Definitions Page on page 24](#)
- [Creating Security Alert Definitions on page 25](#)

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 > Security Alert Definition**.

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.

3. Click **OK** to save the configuration.

A new alert definition is created.

- Related Documentation**
- [About the Security Alerts Definitions Page on page 24](#)
 - [Creating Security Alert Definitions on page 25](#)

CHAPTER 5

Monitoring Security and Device Events

- [About the All Security Events Page on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)
- [About the Device Events Page on page 49](#)
- [About the Screen Events Page on page 53](#)

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 30](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 30](#).

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 11 on page 30](#) describes the widgets on the All Events Summary View page.

Table 11: 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 12 on page 31 describes the fields on the All Events Detail View Page.

Table 12: 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.

Table 12: Fields on the All Events Detail View Page (continued)

Field	Description
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.
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.

Table 12: Fields on the All Events Detail View Page (continued)

Field	Description
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 on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 34](#)
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 34](#).

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 13 on page 34](#) describes the widgets on the Summary View page.

Table 13: 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 14 on page 34](#) provides guidelines on using the fields on the Detail View page.

Table 14: Fields on the Detail View Page

Field	Description
Time	View the time when the log was received.

Table 14: Fields on the Detail View Page (continued)

Field	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.
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.
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.

Table 14: Fields on the Detail View Page (continued)

Field	Description
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

- [About the All Security Events Page on page 29](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 37](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 37](#).

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 15 on page 37](#) describes the widgets on the Summary View page.

Table 15: 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 16 on page 37](#) provides guidelines on using the fields on the Detail View page.

Table 16: 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 16: 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 on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 39](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 39](#).

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 17 on page 39](#) describes the widgets on the Summary View page.

Table 17: 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 18 on page 39](#) provides guidelines on using the fields on the Detail View page.

Table 18: 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.

Table 18: Fields on the Detail View Page (continued)

Fields	Description
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 on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 41](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 41](#).

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 19 on page 41](#) describes the widgets on the Summary View page.

Table 19: 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.
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 20 on page 41](#) provides guidelines on using the fields on the Detail View page.

Table 20: 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.

Table 20: Fields on the Detail View Page (continued)

Fields	Description
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
Profile Name	View the name of the content filtering profile that triggered the event.

Related Documentation

- [About the All Security Events Page on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 (blacklists and whitelists) 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 43](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 43](#).

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 21 on page 43](#) provides guidelines on using the fields on the Detail View page.

Table 21: 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).

Table 21: Fields on the Detail View Page (continued)

Fields	Description
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 content filtering profile that triggered the event.

Related Documentation

- [About the All Security Events Page on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

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 45](#).

- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 45](#).

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 22 on page 45](#) provides guidelines on using the widgets on the Detail View page.

Table 22: 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 23 on page 45](#) provides guidelines on using the fields on the Detail View page.

Table 23: 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).

Table 23: Fields on the Detail View Page (continued)

Fields	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.
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 on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the IPS Events Page on page 46](#)

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 47](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 47](#).

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 24 on page 47](#) provides guidelines on using the widgets on the Detail View page.

Table 24: 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.
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 25 on page 48](#) provides guidelines on using the fields on the Detail View page.

Table 25: 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.
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.

Table 25: Fields on the Detail View Page (continued)

Column	Description
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

- [About the All Security Events Page on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)

About the Device Events Page

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

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

You can view comprehensive details of device events in a tabular format that includes sortable columns and a line graph (also known as swim lanes). The data presented in the line graph is refreshed automatically based on the selected time range. The line graph shows light blue areas that represent all device events and dark blue areas represent blocked device events

Tasks You Can Perform

You can perform the following tasks from this page:

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

Advanced Search

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

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

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

- Specific events originating from or landing within United States

Source Country = United States OR Destination Country = United States AND Event Name = IDP_ATTACK_LOG_EVENT, IDP_ATTACK_LOG_EVENT_LS, IDP_APPDDOS_APP_ATTACK_EVENT_LS, IDP_APPDDOS_APP_STATE_EVENT, IDP_APPDDOS_APP_STATE_EVENT_LS, AV_VIRUS_DETECTED_MT, AV_VIRUS_DETECTED, ANTISPAM_SPAM_DETECTED_MT, ANTISPAM_SPAM_DETECTED_MT_LS, FWAUTH_FTP_USER_AUTH_FAIL, FWAUTH_FTP_USER_AUTH_FAIL_LS, FWAUTH_HTTP_USER_AUTH_FAIL, FWAUTH_HTTP_USER_AUTH_FAIL_LS, FWAUTH_TELNET_USER_AUTH_FAIL, FWAUTH_TELNET_USER_AUTH_FAIL_LS, FWAUTH_WEBAUTH_FAIL,FWAUTH_WEBAUTH_FAIL_LS

- User wants to filter all RT flow sessions originating from IPs in specific countries and landing on IPs in specific countries

Event Name = RT_FLOW_SESSION_CREATE,RT_FLOW_SESSION_CLOSE AND Source IP = 177.1.1.1,220.194.0.150,14.1.1.2,196.194.56.4 AND Destination IP = 255.255.255.255,10.207.99.75,10.207.99.72,223.165.27.13 AND Source Country = Brazil,United States,China,Russia,Algeria AND Destination Country = Germany,India,United States

- Traffic between zone pairs for policy – IDP2

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

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

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

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

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

Field Descriptions

Table 26 on page 51 provides guidelines on using the fields on the Device Events page.

Table 26: 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.
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.

Table 26: Fields on the Device Events Detailed View Page (continued)

Field	Description
Service Name	View the name of the application service. For example, FTP, HTTP, SSH, and so on.
Nested Application	View the nested application in the log.
Source Zone	View the source zone of the log.
Destination Zone	View the destination zone of the log.
Protocol ID	View the protocol ID in the log.
Roles	View the role name associated with the log.
Reason	View the reason for the log generation. For example, a connection tear down may have an associated reason such as authentication failed.
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 on page 29](#)

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 53](#).
- View the comprehensive details of events in a tabular format that includes sortable columns. See [“Detail View” on page 54](#).

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 27 on page 53](#) describes the widgets on the Detail View page.

Table 27: 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.

Table 27: Widgets on the Summary Page (continued)

Field	Description
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 28 on page 54](#) describes the fields on the Detail View page.

Table 28: 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.
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.

Table 28: Fields on the Detail View Page (continued)

Fields	Description
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.
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.

Table 28: Fields on the Detail View Page (continued)

Fields	Description
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 on page 29](#)
- [About the Firewall Events Page on page 33](#)
- [About the Web Filtering Events Page on page 36](#)
- [About the IPsec VPNs Events Page on page 38](#)
- [About the Content Filtering Events Page on page 40](#)
- [About the Antispam Events Page on page 42](#)
- [About the Antivirus Events Page on page 44](#)
- [About the IPS Events Page on page 46](#)

CHAPTER 6

Monitoring SD-WAN Events

- [SD-WAN Events Overview on page 57](#)
- [About the SD-WAN Events Page on page 58](#)

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 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 on page 58](#)
- [SLA Profiles and SD-WAN Policies Overview on page 217](#)

About the SD-WAN Events Page

To access this page, click **Monitor > SD-WAN 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 details about all SD-WAN events.
- View details about SD-WAN events in a customized time range.
- Show or hide columns that contain information about SD-WAN events. See *Sorting Objects*.
- 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 29 on page 58 describes the fields on the SD-WAN Events page.

Table 29: 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>
Time	View the time at which the links were switched.
Site	View the site that switched links.
SLA Profile	View the SLA profile associated with the site.
Source	View the designated WAN link.
Destination	View the new WAN link to which the site switched.
Duration	View the time duration for which the SLA requirement for a site was not met before the site switched WAN links. A time 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.

Related Documentation

- [SD-WAN Events Overview on page 57](#)

CHAPTER 7

Monitoring Applications

- [About the SLA Performance of a Single Tenant Page on page 61](#)
- [Viewing the SLA Performance of a Site on page 63](#)
- [Viewing the SLA Performance of an Application or Application Group on page 68](#)
- [Application Visibility Overview on page 69](#)
- [About the Application Visibility Page on page 69](#)
- [Selecting Devices on page 72](#)

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 30 on page 62 describes the fields on the *Tenant-Name* SLA Performance page.

Table 30: 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, Previous 1 day 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 “Viewing the SLA Performance of a Site” on page 63.</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 “Viewing the SLA Performance of a Site” on page 63.</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 “Viewing the SLA Performance of a Site” on page 63.</p>

Table 31 on page 62 describes the fields in the card and grid views.

Table 31: 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.

Table 31: Fields on the SLA Performance of a Single Tenant Page in Card and Grid Views (continued)

Field	View	Description
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 Others . 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 on page 63](#)
 - [Viewing the SLA Performance of an Application or Application Group on page 68](#)
 - [SD-WAN Events Overview on page 57](#)
 - [Creating SLA Profiles on page 227](#)

Viewing the SLA Performance of a Site

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 on page 64](#)
- [Applications SLA Performance by Throughput on page 65](#)
- [SLA Performance for ALL on page 67](#)

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 68](#).

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 32 on page 66](#) describes the fields on the Applications SLA Performance by Throughput grid view.

Table 32: 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 68](#).

SLA Performance for ALL

View a graphical representation of the performance of the SLA parameters such as round-trip time (RTT), latency, packet loss, and jitter for the specified time range for MPLS and Internet WAN links for all SLA profiles. The y-axis represents the SLA parameters and the x-axis represents the specified time range. You can also view the respective target SLA parameters in the graphs.



NOTE: The graphical representation of the performance of all SLA parameters for the WAN links is available only in the graph view.

To view a graphical representation of the performance of all SLA parameters for the WAN links:

- Select **All** at the top right of the section. By default, All is selected.

A graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range for all WAN links is displayed.

- Select **wan_0**, **wan_1**, and so on at the top right of the section to view the performance of the SLA parameters for the MPLS and Internet WAN links. You can enable and configure **wan_0**, **wan_1**, and so on and map them to MPLS or Internet links when you create a site.

The graphical representation of the performance of the SLA parameters such as RTT, latency, packet loss, and jitter for the specified time range is refreshed and only the performance for the selected WAN link is displayed.

- (Optional) Click **Legend** at the bottom right of the section to view the plotting legend for the horizontal dotted lines parallel to the x-axis in the graphs. The horizontal dotted lines represent the respective target SLA parameters of the SLA profiles.



NOTE: RTT is represented as Delay on the “[Application SLA Profiles](#)” on [page 226](#) page.

Related Documentation

- [About the SLA Performance of a Single Tenant Page on page 61](#)
- [Viewing the SLA Performance of an Application or Application Group on page 68](#)

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 33 on page 68](#) describes the fields on the application or application group SLA Performance details page.

Table 33: Fields on the Application or Application Group Details Page

Field	Description
Category and Description	<p>View the category of the application or application group. The category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, Video, and so on.</p> <p>You can also view a description of the application or application group.</p>
SLA	View the name of the SLA profile associated with the application or application group.
Target	View the current target throughput defined in the SLA profile associated with the application or application group. If the target throughput was modified during runtime, the date and time when the throughput was modified and the previously defined throughput value are also displayed.
Avg. Performance	View the average throughout performance (in %) above or below the configured target throughput. The average throughput (in Mbps) is displayed within parentheses.
SLA Metrics by Throughput	View a graphical representation of the SLA metrics by throughput during the specified time range for that application or application group. The y-axis represents the throughput (in Mbps). The x-axis represents the specified time range. Hover over the graph to view the throughput value and time at any specified point. You can also view the sessions consumed by the WAN links for the application or application group time range.

Table 33: Fields on the Application or Application Group Details Page (continued)

Field	Description
Global SLA Profile Performance	<p>View the performance for all the SLA parameters of the SLA profile associated with the application or application group. The SLA performance is represented by a color-coded donut chart. The section in blue in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were met. The section in red in the donut chart indicates the percentage of time during which SLA requirements for the SLA profile were not met.</p> <p>Click the red colored section of the donut chart to view more information about when SLA requirements for the SLA profile were not met. The SLA Profile Performance page appears. The SLA Profile Performance page displays the following fields:</p> <ul style="list-style-type: none"> • SLA Profile—SLA profile associated with the application or application group • Target—Target throughput configured in the SLA profile • SLAs Not Met—Percentage of time SLA requirements were not met for the SLA profile • Sessions—Number of sessions consumed by the application or application group • Start Time—Time at which the WAN links associated with the application or application groups started to fail meeting the SLA requirements • End Time—Time at which SLA profile requirements started to be met again • Avg Val—Average throughput (in Mbps) when the SLA requirements started to fail • Duration—Total duration (in seconds) during which SLA requirements were not met • From—Source WAN link • To—Destination WAN link

- Related Documentation**
- [About the SLA Performance of a Single Tenant Page on page 61](#)
 - [Viewing the SLA Performance of a Site on page 63](#)

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 on page 69](#)
 - [Selecting Devices on page 72](#)

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 70](#).
- View application visibility data in **Grid View**. See [“Grid View” on page 71](#).
- Select a device to which the application visibility settings are applicable. See [“Selecting Devices” on page 72](#).

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 34 on page 70](#) provides guidelines on using the fields on the **Chart View** of the **Application Visibility** page.

Table 34: Fields on the Chart View

Field	Description
All Devices	Displays application visibility data for all the sites managed by CSO. Click Edit to select individual devices for which you want to view the data.
Show By	Select from the following options to view a user's data: <ul style="list-style-type: none"> • Bandwidth—Shows data based on the amount of bandwidth the application has consumed for a particular time range. • Number of Sessions—Shows data based on the number of sessions consumed by the application.
Time Span	Select the required time range to view a user's data. 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.
Select graph	Select from the following graphical representations to view an application's data: <ul style="list-style-type: none"> • Bubble Graph • Heat Map • Zoomable Bubble Graph By default, data is shown in the Bubble Graph format.

Table 34: Fields on the Chart View (continued)

Field	Description
Group By	Select from the following options to view the application's data: <ul style="list-style-type: none"> • Risk—Grouped by critical, high, unsafe, and so on. • Category—Grouped by categories such as web, infrastructure, and so on.
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.
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 35 on page 71](#) 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 35 on page 71](#) provides guidelines on using the fields on the **Grid View** of the **Application Visibility** page.

Table 35: 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 36 on page 72 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 36: 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 on page 69](#)
 - [Selecting Devices on page 72](#)
 - [About the SLA Performance of a Single Tenant Page on page 61](#)

Selecting Devices

You can select the devices to which the application visibility settings are applicable. By default, these settings are applicable to all devices.

To select devices:

1. Select **Monitor > Applications > Visibility**.
The **Application Visibility** page appears.
2. Click the **Edit** link that appears beside **All Devices**.
The **Select Devices** page appears.
3. Choose the **Selective** option. The available devices are displayed in the **Available** column.

4. Choose the devices from the **Available** column and click the greater-than icon (>) to move them to the **Selected** column.
5. Click **OK** to save your changes. If you want to discard your changes, click **Cancel** instead.

If you click **OK**, application visibility data will be displayed only for the selected devices.

**Related
Documentation**

- [Application Visibility Overview on page 69](#)
- [About the Application Visibility Page on page 69](#)

CHAPTER 8

Monitoring Threats

- [About the Threats Map \(Live\) Page on page 75](#)

About the Threats Map (Live) Page

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: Threats with unknown geographical IP addresses are displayed as undefined.

- [Tasks You Can Perform on page 75](#)
- [Field Descriptions on page 77](#)
- [Threat Types on page 78](#)

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 37 on page 76](#).

Table 37: Country-Specific Threat Information

Field	Description	Displayed In
Number-of-threat-events Threat Events since 12:00 am	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
Inbound (Number-of-threat-events)	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
Outbound (Number-of-threat-events)	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
Number-of-threat-events Events since 12:00 am	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
Number-of Inbound Events	Displays the total number of inbound threats for the country and the number of inbound threat events for each of the following categories: <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Device Authentication • Screen 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. Click the Top 5 IP Addresses (Inbound) to view the IP address and the number of events for that IP address for the top five inbound events.	<i>Country-Name</i> (Details) panel

Table 37: Country-Specific Threat Information (continued)

Field	Description	Displayed In
Number-of Outbound Events	<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"> • IPS Threats • Virus • Spam • Device Authentication • Screen <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 Top 5 IP Addresses (Outbound) 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 38 on page 77 displays the fields the Threats Map (Live) page.

Table 38: Fields on the Threats Map (Live) Page

Field	Description
Total Threats Blocked & Allowed	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.
Threats Blocked & Allowed	<p>Displays the total number of threats blocked and allowed by the following categories:</p> <ul style="list-style-type: none"> • IPS Threats • Virus • Spam • Device Authentication • Screen <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>
Top Target Devices	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.
Top Destination Countries	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.

Table 38: Fields on the Threats Map (Live) Page (continued)

Field	Description
Top Source Countries	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.

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 39 on page 78](#) describes different types of threats blocked and allowed.

Table 39: 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"> • Source of attack • Destination of attack • Type of attack • Session information • Severity • Policy information that permitted the traffic. • Action: traffic permitted or dropped.
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"> • Source of the infected file • Destination • Filename • URL used for accessing the file
Spam events	<p>E-mail spam that is detected based on the blacklist 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"> • Source • Action: E-mail is rejected or allowed. • Reason for identifying as e-mail spam.
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 39: 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">• Internet Control Message Protocol (ICMP) screening• IP screening• TCP screening• UDP screening

Related Documentation • [About the All Security Events Page on page 29](#)

CHAPTER 9

Monitoring Jobs

- [About the Jobs Page on page 81](#)
- [Editing and Deleting Scheduled Jobs on page 83](#)
- [Viewing Job Details on page 84](#)

About the Jobs Page

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

Use this page to view the list of all jobs and the jobs that are scheduled to be executed. You can view general information about the jobs and the overall progress and status of the jobs. You can also edit and delete scheduled jobs.

Tasks You Can Perform

You can perform the following tasks from this page:

- View details about a job. See [“Viewing Job Details” on page 84](#).
- Edit and delete scheduled jobs. See [“Editing and Deleting Scheduled Jobs” on page 83](#).

Field Descriptions

[Table 40 on page 81](#) provides guidelines on using the fields on the Jobs page.

Table 40: Fields on the Jobs Page

Field	Description
Job Name	View the name of the job. Example: MSEC_DOWNLOAD_IPS/APPLICATION_SIGNATURES_08_Jul_17_124229_024
Resource Name	View the resource name of the job. Example: Download IPS/Application Signatures
Status	View the status of the job to know whether the job succeeded or failed. Example: Success

Table 40: Fields on the Jobs Page (continued)

Field	Description
Owner	View the name of the owner who created the job. Example: cspadmin
Number of Tasks	View the number of tasks associated with the job. Example: 2 For example, the tasks site.ucpe-32 and customer.sdwan are associated with the job.
Job Type	View the job type. Example: tssm import pop
Start Date	View the start date and time of a task associated with the job.
End State	View the end date and time of a task associated with the job.

Field Descriptions

[Table 41 on page 82](#) provides guidelines on using the fields on the Scheduled Jobs page.

Table 41: Fields on the Scheduled Jobs Page

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

- Related Documentation**
- [Editing and Deleting Scheduled Jobs on page 83](#)

Editing and Deleting Scheduled Jobs

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

- [Editing Scheduled Jobs on page 83](#)
- [Deleting Scheduled Jobs on page 83](#)

Editing Scheduled Jobs

You can modify the date and time of deployment of scheduled jobs.

To modify a scheduled job:

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

The Scheduled Jobs page appears.

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

The Edit Schedule page appears.

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

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

The modified job and its details are displayed on a page

Deleting Scheduled Jobs

You can delete one or more scheduled jobs.

To delete a scheduled job:

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

The Scheduled Jobs page appears with a list of jobs.

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

The Confirm Delete page appears.

3. Click **Yes** to confirm.

The scheduled job is deleted.

- Related Documentation**
- [About the Jobs Page on page 81](#)
 - [Viewing Job Details on page 84](#)

Viewing Job Details

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

To view details of a job:

- Right-click the job name that you want to see the detailed view for and select **Detail View**, or select the job and click **More > Detail View**.
- Alternatively, hover over the job name and click the Detailed View icon that appears before it.

The Detailed View page appears, showing the details of the job and the number of tasks associated with the job. See the relevant topic [“About the Jobs Page” on page 81](#) for a description of the fields on these pages.

- Related Documentation**
- [About the Jobs Page on page 81](#)

PART 4

Managing Resources

- [Managing Devices on page 87](#)
- [Managing Device Images on page 103](#)

CHAPTER 10

Managing Devices

- [Multidepartment CPE Device Support on page 87](#)
- [About the Devices Page on page 88](#)
- [Performing Return Material Authorization \(RMA\) for a Single-CPE Device on page 90](#)
- [Performing Return Material Authorization \(RMA\) for Dual-CPE Devices on page 92](#)
- [Granting RMA for a Device on page 95](#)
- [Managing a Single CPE Device on page 99](#)
- [Rebooting a CPE Device on page 100](#)

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 on page 61](#)
- [Viewing the SLA Performance of a Site on page 63](#)

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 42 on page 89](#).
- Manage a single CPE. See [“Managing a Single CPE Device” on page 99](#).
- Reboot a CPE device. See [Rebooting a CPE Device](#).
- 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 single-CPE devices, see [“Performing Return Material Authorization \(RMA\) for a Single-CPE Device” on page 90](#)
 - For information on performing RMA on dual-CPE devices, see [“Performing Return Material Authorization \(RMA\) for Dual-CPE Devices” on page 92](#)
- View details about a CPE . Click the details icon that appears when you hover over the name of a device or click **More > Details**. See [“Viewing Object Details” on page 17](#).
- Show or hide columns about the CPE. See [“Sorting Objects” on page 17](#).
- Search an object about the CPE. See [“Searching for Text in an Object Data Table” on page 18](#).

Field Descriptions

- [Table 42 on page 89](#) describes widgets on the Devices page.
- [Table 43 on page 89](#) describes the fields on the Devices page.

Table 42: Widgets on the Devices Page

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

Table 43: Fields on the Devices Page

Field	Description
Device Name	<p>View the name of the device.</p> <p>Example: sunny-NFX-250</p>
Tenant	<p>View the name of the tenant.</p> <p>Example: tenant-blue</p>
Site Name	<p>View the name of the tenant site.</p> <p>Example: site-blue-white</p>
Management Status	<p>View the management status of the CPE devices deployed in the cloud.</p> <ul style="list-style-type: none"> • EXPECTED—Regional server has the activation details for the CPE device, but CPE device has not yet established a connection with the server. • RMA—CPE device has been tagged for RMA as a result of the user applying the Initiate RMA action on the device. • ACTIVE—CPE device has downloaded images, but not yet configured. • PROVISIONED—IPsec tunnel on NFX250 device is operational. • PROVISION_FAILED—CPE device failed when the vSRX was not instantiated properly.
Model	<p>View the name of the device model.</p> <p>Example: NFX</p>
Active Services	<p>View the number of services that are activated for the device.</p> <p>Example: 3</p>

Table 43: Fields on the Devices Page (continued)

Field	Description
Location	View the name of the location. Example: San Jose, CA
Status Message	View the latest status message. Example: IPsec provision success
WAN Links	View the number of WAN links. Example: 2
POP Name	View the name of the POP. Example: pop_blue
Image Name	View the name of the device image file. Example: install_nfx_fmfm_agent_1_0.sh
OS Version	View the Junos OS Release version. Example: 15.1X49-D40
Serial Number	View the serial number of the device. Example: DD0416AA0117

Related Documentation • [Managing a Single CPE Device on page 99](#)

Performing 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.

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 device.

Click **No** to cancel the process



NOTE:

- The **Initiate RMA** option is enabled for a device only if the management status is **PROVISIONED**.
- In the **Sites > Site Management** page, 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 getting a replacement for the device. This action is performed outside of CSO.

3. After you receive the replacement of the device, provide the details of the replacement device by clicking **More > Grant RMA**. See [“Granting RMA for a Device” on page 95](#).



NOTE: The **Grant RMA** option is enabled only if the management status is **RMA**.

4. To activate the device, select the device and click **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**.
5. To complete the RMA process, you must 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 will be restored automatically.

- **Licenses**—If the replaced device is a physical SRX device, you need to generate a new license and upload it.
- **Application Signatures**—Push the application signatures to the replaced device. See [“About the Application Signatures Page” on page 300](#).

- Certificates—Import and install the required certificates on the replaced device. See [“Importing a Certificate” on page 405](#) and [“Installing and Uninstalling Certificates” on page 407](#).
- Policies—Push the defined firewall and NAT policies to the replaced device. See [“About the Firewall Policy Page” on page 124](#) and [“About the NAT Policies Page” on page 234](#).

After you complete these steps, the **Management Status** of the replacement device remains in **PROVISIONED** state. The RMA process is complete and the device is now ready to be used.

**Related
Documentation**

- [About the Devices Page on page 88](#)
- [Granting RMA for a Device on page 95](#)

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

Sometimes, a single device or both the devices within an NFX or SRX cluster fail, and has to be replaced with a new or restored device(s). In such situations, you perform RMA to back-up the configuration of the faulty device(s), recall the faulty device and replace it with a new or restored device(s), push the required configuration to the replacement device(s), and activate the device(s) in order for CSO to recognize and manage the replacement device(s).

The following section discuss how you can perform RMA for an NFX or SRX cluster:

- [Performing RMA for an NFX Cluster on page 92](#)
- [Performing RMA for an SRX Cluster on page 94](#)

Performing RMA for an NFX Cluster

You can only perform RMA for an NFX cluster at the cluster level. That is, you have to perform RMA for both the devices in the NFX cluster even if only a single device in the cluster has failed.



NOTE: You cannot select an individual device in the NFX cluster and perform RMA for it.

To perform RMA for an NFX cluster:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

2. Select the NFX cluster for which you want to perform RMA and click **More > Initiate RMA**.

A confirmation page appears requesting for confirmation to go ahead with the initiate RMA process for the selected NFX cluster. Click **Yes** to confirm RMA for the NFX cluster.

Click **No** to cancel the process.



NOTE:

- The **Initiate RMA** option is enabled for an NFX cluster only if the management status is **PROVISIONED**.
- In the **Sites > Site Management** page, the **Site Status** for the NFX cluster 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 NFX cluster. The **Management Status** of the device changes to **RMA**.

After the NFX cluster is in the **RMA** state, you can raise a device replacement request for the faulty device(s) in the NFX cluster. This action is performed outside of CSO.

3. After you receive the replacement of the device(s), you have to provide the details of both the devices in the NFX cluster to CSO, by clicking **More > Grant RMA**. See [“Granting RMA for a Device” on page 95](#).



NOTE: The **Grant RMA** option is enabled only if the management status is **RMA**.

4. To activate the devices within the NFX cluster, select the cluster and click **Activate Device**. Enter the **Activation Code** for the primary and secondary devices to activate the devices of the NFX cluster for usage. When the device is activated, its **Management Status** changes to **PROVISIONED**.
5. To complete the RMA process, you must 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.
- **Application Signatures**—Push the application signatures to the replaced device. See [“About the Application Signatures Page” on page 300](#).
 - **Certificates**—Import and install the required certificates on the replaced devices. See [“Importing a Certificate” on page 405](#) and [“Installing and Uninstalling Certificates” on page 407](#).

- Policies—Push the defined firewall and NAT policies to the replaced devices. See [“About the Firewall Policy Page” on page 124](#) and [“About the NAT Policies Page” on page 234](#).

The RMA process is complete and the device(s) in the NFX cluster are now ready to be used.

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: For the CSO Release 3.3, you cannot perform the RMA process for an SRX cluster at the cluster level.

To return a faulty device within an SRX cluster 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 within the SRX cluster 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 device.

Click **No** to cancel the process.



NOTE:

- The **Initiate RMA** option is enabled for a device only if the management status is **PROVISIONED**.
- In the **Sites > Site Management** page, 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 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 device, provide the details of the replacement device by clicking **More > Grant RMA**. See [“Granting RMA for a Device” on page 95](#).



NOTE: The **Grant RMA** option is enabled only if the management status is **RMA**.

After you complete these steps, the **Management Status** of the replacement device(s) is changed to **PROVISIONED** state. The RMA process is complete and the device is now ready to be used.

- Related Documentation**
- [About the Devices Page on page 88](#)
 - [Performing Return Material Authorization \(RMA\) for a Single-CPE Device on page 90](#)
 - [Granting RMA for a Device on page 95](#)

Granting RMA for a Device

- [Granting RMA for a Single-CPE Device on page 95](#)
- [Granting RMA for a Dual-CPE Device on page 96](#)
- [Granting RMA for an SRX Device within an SRX Cluster on page 98](#)

Granting RMA for a Single-CPE Device

Before you perform **Grant RMA for a Device**, ensure that:

- You have received the replacement of the faulty device.
- You have the serial number and the activation code of the replacement device.

To perform **Grant RMA** for a device:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

2. Select the defective device that you have already performed RMA for 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 44 on page 96](#).

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 or restored device is added to the network.
- The management status of the device changes to **Expected** in the **Devices** page.

In the **Sites > Site Management** page, the **Site Status** for the device for which you performed **Grant RMA**, changes to **Expected**.



NOTE: You can see the progress of this job in 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 [“Performing Return Material Authorization \(RMA\) for a Single-CPE Device”](#) on page 90.

[Table 44 on page 96](#) provides guidelines on using the fields on the **Grant RMA for Device** panel.

Table 44: Fields on the Grant RMA for Single-CPE Device Page

Field	Description
Tenant 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 Grant RMA process.
Serial Number	Enter the serial number of the replacement device. The serial number is case sensitive. Example: DD2316AF0177
Activation Code	Enter the activation code for the replacement device. You will receive the activation code from the service provider, outside of CSO. Example: 545454

Granting RMA for a Dual-CPE Device

Before you perform **Grant RMA for a Device**, ensure that:

- You have received the replacement of the faulty device(s).
- You have the serial number(s) and the activation code(s) of the replacement device(s).

To perform **Grant RMA** for a cluster:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

2. Select the cluster that you have already performed RMA for 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 45 on page 97](#).

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

When you perform **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 device(s) are added to the network.
- The management status of the cluster changes to **Expected** in the **Devices** page.

In the **Sites > Site Management** page, the **Site Status** for the cluster for which you performed **Grant RMA**, changes to **Expected**.



NOTE: You can see the progress of this job in the **Monitor > Jobs** page. This job might take around 15 minutes to complete.

[Table 45 on page 97](#) provides guidelines on using the fields on the **Grant RMA for Device** panel.

Table 45: Fields on the Grant RMA for Dual-CPE Device Page

Field	Description
Tenant 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 cluster that will be replaced with new or restored devices through the Grant RMA process.
Primary Serial Number	Enter the serial number of the primary replacement device. The serial number is case sensitive. Example: DD2316AF0177
Primary Activation Code	Enter the activation code for the primary replacement 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 secondary replacement device. The serial number is case sensitive. Example: DD2316AF0145
Secondary Activation Code	Enter the activation code for the secondary replacement device. You will receive the activation code from the service provider, outside of CSO. Example: 545476

Granting RMA for an SRX Device within an SRX Cluster

Before you perform **Grant RMA for a Device**, ensure that:

- You have received the replacement of the faulty device.
- You have the serial number and the activation code of the replacement device.

To perform **Grant RMA** for a device:

1. Select **Resources > Devices**.

The **Devices** page appears displaying all the devices and clusters.

2. Select the defective device that you have already performed RMA for 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 46 on page 98](#).

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 object in CSO is updated with the serial number and activation code for the replacement device.
- The management status of the device is restored in the **Devices** page.

In the **Sites > Site Management** page, the **Site Status** for the device for which you performed **Grant RMA**, changes to **PROVISIONED**.



NOTE: You can see the progress of this job in the **Monitor > Jobs** page.

[Table 46 on page 98](#) provides guidelines on using the fields on the **Grant RMA for Device** panel.

Table 46: Fields on the Grant RMA for Device Page (for SRX Device in an SRX Cluster)

Field	Description
Tenant Name	Displays the name of the tenant who is performing RMA.

Table 46: Fields on the Grant RMA for Device Page (for SRX Device in an SRX Cluster) (continued)

Field	Description
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 Grant RMA process.
Serial Number	Enter the serial number of the replacement device. The serial number is case sensitive. Example: DD2316AF0177
Activation Code	Enter the activation code for the replacement device. You will receive the activation code from the service provider, outside of CSO. Example: 545454

**Related
Documentation**

- [About the Devices Page on page 88](#)
- [Performing Return Material Authorization \(RMA\) for a Single-CPE Device on page 90](#)
- [Performing Return Material Authorization \(RMA\) for Dual-CPE Devices on page 92](#)

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 > Devices > Device-Name**.

You can perform the following tasks from this page:

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

Related Documentation • [About the Devices Page on page 88](#)

Rebooting a CPE Device

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

To reboot a tenant device:

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

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



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

3. (Optional) Click the **Device Reboot** link to view the device reboot logs.
4. (Optional) You can view the job status on the **Monitor > Jobs** page.

To reboot a cloud hub device:

1. Select **Resources > Cloud Hub Devices**.
2. Select the cloud hub device that you want to reboot and select **More > Reboot**.

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



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

3. (Optional) Click the **Device Reboot** link to view the device reboot logs.
4. (Optional) You can view the job status on the **Monitor > Jobs** page.

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

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

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



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

**Related
Documentation**

- *About the Cloud Hub Devices Page*
- *About the Tenant Devices Page*

CHAPTER 11

Managing Device Images

- [Device Images Overview on page 103](#)
- [About the Device Images Page on page 103](#)
- [Deleting Device Images on page 104](#)

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 on page 103](#)

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

Field Descriptions

[Table 47 on page 104](#) shows the fields on the Images page.

Table 47: 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 on page 103](#)

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 on page 103](#)

PART 5

Managing Configuration

- [Managing Network Services on page 107](#)
- [Managing Firewall Policies on page 123](#)
- [Unified Threat Management on page 175](#)
- [Managing SD-WAN on page 217](#)
- [Managing NAT Policies on page 231](#)
- [Managing SSL Proxies on page 261](#)
- [Managing Shared Objects on page 285](#)
- [Managing Deployments on page 309](#)

CHAPTER 12

Managing Network Services

- [Network Service Overview on page 107](#)
- [About the Network Services Page on page 108](#)
- [About the Service Overview Page on page 109](#)
- [About the Service Instances Page on page 111](#)
- [Configuring VNF Properties on page 113](#)
- [vSRX VNF Configuration Settings on page 113](#)
- [LxCIPtable VNF Configuration Settings on page 117](#)
- [Cisco CSR-1000v VNF Configuration Settings on page 120](#)
- [Riverbed Steelhead VNF Configuration Settings on page 121](#)

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 on page 108](#)
- [About the Service Overview Page on page 109](#)
- [About the Service Instances Page on page 111](#)

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 107](#).

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 48 on page 108](#).
- 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 111](#).

Field Descriptions

[Table 48 on page 108](#) shows the descriptions of the widgets that appear at the top of the Network Services page.

Table 48: Widgets on the Network Services Page

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

[Table 49 on page 108](#) shows the descriptions of the fields on the Network Services page.

Table 49: Fields on the Network Services Page

Field	Description
Name	<p>View the name of the service.</p> <p>Click the name to view full information about a service.</p>
Tenants	View the names of the tenants that have access to the network service.

Table 49: Fields on the Network Services Page (continued)

Field	Description
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 50 on page 109 shows the descriptions of the fields on the Detail for *network service name* page.

Table 50: 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
Performance Goals	View performance parameters of the network service that include bandwidth, number of sessions, latency, and license cost.

- Related Documentation**
- [Network Service Overview on page 107](#)
 - [About the Service Overview Page on page 109](#)
 - [About the Service Instances Page on page 111](#)

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 51 on page 110](#).
- View resources required for the service and its performance specification. See *Service Requirements* and *Service Performance* in [Table 51 on page 110](#).
- View the service chain, with its constituent VNFs. See *Service Configuration* in [Table 51 on page 110](#).
- Configure VNFs. Click a VNF in the service chain graphic. See “[vSRX VNF Configuration Settings](#)” on page 113.

Field Descriptions

[Table 51 on page 110](#) provides guidelines on using the fields on the Service Overview page.

Table 51: 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"> • Discontinued—Service is no longer available for customers. • Published—Service designer has published service to network catalog, and it is available for customers.
Tenants	View the number of tenants using this service.
<i>Service Requirements</i>	
CPU	View the number of CPUs that the service needs (cores).
Memory	View the amount of RAM that the service needs in gigabytes (GB).
<i>Service Performance</i>	
Sessions	View the number of sessions concurrently supported by one instance of the service.
Bandwidth	View the data rate for the service in megabytes per second (Mbps) or gigabytes per second (Gbps).
Latency	View the time a packet takes to traverse the service in milliseconds (ms) or nanoseconds (ns).

Table 51: Fields on the Service Overview Page (continued)

Field	Description
License cost	Specify the license cost for the network service in USD.
<i>Service Configuration (graphic of the service chain)</i>	
I	View the ingress point—the point at which packets enter the service.
E	View the egress point—the point at which packets exit the service.
One or more VNFs	<p>Click to view settings for the VNF. See “vSRX VNF Configuration Settings” on page 113.</p> <p>The service designer can configure the VNF settings in Network Service Designer and the administrative user can configure the VNF settings in Customer Portal.</p> <p>BEST PRACTICE: The network service designer configures settings for the virtual machine (VM) in which the virtualized network function (VNF) resides and the administrative user configures settings for the service, such as policies. The service designer can also configure a few example settings for the service. These example settings should be generic and not network-specific.</p>

Related Documentation

- [Network Service Overview on page 107](#)
- [About the Network Services Page on page 108](#)
- [About the Service Instances Page on page 111](#)

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 53 on page 112](#).
- 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 113](#).

Field Descriptions

[Table 52 on page 112](#) shows the descriptions of the fields on the Service Instances page.

Table 52: Fields on the Service Instances Page

Field	Description
Name	View the name of the occurrence of a service at a specific tenant site.
Tenant	View the name of the tenant.
Status	View the state of the service at the customer site: <ul style="list-style-type: none"> Created—Administrative user for the tenant has enabled this service instance, which is active. Blank—Administrative user for the tenant has disabled this service instance.
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 53 on page 112](#) shows the descriptions of the fields on the Detail for *Service-Instance-Name* page.

Table 53: 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 on page 107](#)
 - [About the Network Services Page on page 108](#)
 - [About the Service Overview Page on page 109](#)

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 on page 111](#)

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 54 on page 114](#) 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 55 on page 115](#) shows the firewall settings you can configure.

Table 54: 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>
Enable Re-filter	<p>Select True to enable a stateless firewall filter that protects the Routing Engine from denial-of-service (DoS) attacks or False to allow DoS attacks.</p> <p>Example: True</p>
Enable Default Screens	<p>For a cloud site, select True to enable the default screens security profile for the destination zone or False 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>

Table 54: Fields for the vSRX Base Settings (continued)

Field	Description
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 True, 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 True, 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 True, specify the IP addresses of the VMs that contain the Junos Space Virtual Appliances.</p> <p>Example: 10.0.2.50</p>

Table 55: 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"> • left—Interface that transmits data to the host • right—Interface that receives data transmitted from the host <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>

Table 55: Fields for the vSRX Firewall Settings (continued)

Field	Description
Destination Zone	<p>Select the security zone to which packets are delivered.</p> <ul style="list-style-type: none"> • left—Interface that transmits data to the host • right—Interface that receives data transmitted from the host <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"> 1. Click the Source Address column. The source-address page appears. 2. Select any to match any source IP address of packets or ipp to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select ipp, specify a prefix. 4. Click OK. <p>Example: 10.0.2.30</p>
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"> 1. Click the Destination Address column. The destination-address page appears. 2. Select any to match any source IP address of packets or ipp to match a specific prefix in the source IP address for which the application enforces the policy. 3. If you select ipp, specify a prefix. 4. Click OK. <p>Example: 192.0.2.0/24</p>
Action	<p>Select permit to transmit packets that match the rule or deny to drop packets that match the rule.</p> <p>Example: permit</p>

Table 55: 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"> 1. Click the Application column. The application page appears. 2. In the allowed_apps field, select any to match any application or app to choose specific applications. If you select app, press and hold the Ctrl key and click the required applications from the drop-down list. <ul style="list-style-type: none"> • junos-tcp-any • junos-udp-any • junos-ftp • junos-http • junos-https • junos-icmp-all • junos-icmp-ping • junos-telnet • junos-tftp 3. Click OK. <p>Example:</p> <ul style="list-style-type: none"> • junos-tcp-any • junos-udp-any

- Related Documentation**
- [About the Network Services Page on page 108](#)
 - [About the Service Overview Page on page 109](#)
 - [About the Service Instances Page on page 111](#)
 - [Configuring VNF Properties on page 113](#)

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 56 on page 118](#) 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 57 on page 118](#) shows the firewall settings you can configure.
- [Table 58 on page 119](#) shows the Network Address Translation (NAT) settings you can configure.

Table 56: Fields for the LxCIP Base Settings

Field	Description
Loopback Address	Specify a loopback IP address. Example: 192.0.2.10
Operation	Select add to apply the policies to a specific route or del to prevent use of the policies on specific routes. Example: add
Route	Specify the IP prefix of the route to which the policies should apply. Example: 192.0.2.20/24
Next Hop	Specify the IP address of a Contrail gateway network to which the VM connects. Example: 192.0.2.20

Table 57: Fields for the LxCIP Firewall Policy Settings

Field	Description
<i>Firewall Policies</i>	
Prevent SSH Brute	Select True to prevent SSH brute attacks or False to allow SSH brute attacks. Example: False
Prevent Ping Flood	Select True to prevent ping flood attacks or False to allow ping flood attacks. Example: False
<i>Forwarding Rule Settings</i>	
Destination Address	Specify the destination IP address prefix that the network service uses as a match criterion for outgoing traffic. Example: 192.0.2.25/24

Table 57: Fields for the LxCIP Firewall Policy Settings (continued)

Field	Description
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"> • append—Append the rule to a rule chain. • insert-before—Insert the rule before a rule with the same name. • delete—Replace an existing rule with this name. <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"> • accept—Transmit packets that match the policy parameters. • drop—Drop packets that match the policy parameters. • reject—Reject packets that match the policy parameters. <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"> • http • smtp
Type	<p>Select the type of packet that the rule matches.</p> <ul style="list-style-type: none"> • input—Packets that the network service receives that are addressed to this VM • forward—Packets that the network service receives that are addressed to other VMs • output—Packets that the network service transmits <p>The application creates a chain of all rules with a particular type.</p> <p>Example: input</p>

Table 58: 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>

Table 58: Fields for the LxCIP NAT Policy Settings (continued)

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

Related Documentation

- [Managing a Single Site on page 348](#)

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 59 on page 120](#) 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 60 on page 121](#) shows the firewall settings you can configure.

Table 59: 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 60: 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
Left to Right Allowed Apps	Select the applications from the drop-down list for which the policy is enforced in outgoing packets. The following applications are available: <ul style="list-style-type: none"> • http • https • telnet • ftp • tcp • udp • icmp Example: http, https
Right to Left Allowed Apps	Select the application from the drop-down list for which the policy is enforced for incoming packets. The following applications are available: <ul style="list-style-type: none"> • http • https • telnet • ftp • tcp • udp • icmp Example: ftp, udp

Related Documentation • [Managing a Single Site on page 348](#)

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 on page 348](#)

CHAPTER 13

Managing Firewall Policies

- [Firewall Policy Overview on page 123](#)
- [About the Firewall Policy Page on page 124](#)
- [Creating Firewall Policy Intents on page 125](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)
- [Selecting Firewall Source on page 133](#)
- [Selecting Firewall Destination on page 136](#)
- [Firewall Policy Examples on page 139](#)
- [Firewall Policy Schedules Overview on page 170](#)
- [About the Firewall Policy Schedules Page on page 170](#)
- [Creating Schedules on page 171](#)
- [Editing, Cloning, and Deleting Schedules on page 173](#)

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.

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 perform threat management on permitted traffic using UTM profiles. For more information on UTM profiles, see [“UTM Overview” on page 176](#).

Related Documentation

- [About the Firewall Policy Page on page 124](#)
- [Firewall Policy Examples on page 139](#)
- [Creating Firewall Policy Intents on page 125](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)

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 [“Creating Firewall Policy Intents” on page 125](#).
- Modify, clone or delete firewall policy intents. See [“Editing, Cloning, and Deleting Firewall Policy Intents” on page 131](#).
- Deploy a firewall policy. See [“Deploying Policies” on page 312](#).



NOTE: An orange line is displayed against all undeployed firewall policy intents.

- Search for a firewall policy intent. See [“Searching for Text in an Object Data Table” on page 18](#).
- 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 61 on page 125](#) provides guidelines on using the fields on the **Firewall Policy** page.

Table 61: 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 on page 123](#)
- [Creating Firewall Policy Intents on page 125](#)
- [Firewall Policy Examples on page 139](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)
- [About the Deployments Page on page 310](#)
- [Deploying Policies on page 312](#)

Creating Firewall Policy Intents

Use this page to configure a firewall intent that controls transit traffic within a context (source zone to destination zone). 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 protection against multiple threat types including spam and malware, and control access to unapproved websites and content by enabling the UTM option and selecting an appropriate UTM profile.

To configure a firewall policy intent:

1. Select **Configuration > Firewall > Firewall Policy**.
2. Click the add icon (+).

The **Firewall Policy** page appears.

3. Complete the configuration according to the guidelines provided in [Table 62 on page 126](#).



NOTE: When you create a site specific firewall policy intent, the intent will be deployed on the respective site. However, when you create an address based firewall policy intent, the intent will be deployed to all the sites associated with a tenant.

4. 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 created.

[Table 62 on page 126](#) provides guidelines on using the fields on the **Create Firewall Policy** page.

Table 62: Fields on the Create Firewall Policy 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. Comments entered in this field are sent to the device.
Identify the traffic that the intent applies to	
Source	Click on the add icon (+) to select the source endpoints on which the firewall policy intent applies, from the displayed list of addresses, departments, sites, site groups, users, or the Internet. You can also select a source endpoint using the methods described in "Selecting Firewall Source" on page 133 .
Destination	Click on the add icon (+) to select the destination endpoints on which the firewall policy intent applies, from the displayed list of addresses, departments, sites, site groups, or the Internet. You can also select a destination endpoint using the methods described in "Selecting Firewall Destination" on page 136 .
Select Action	<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">• Allow—Device permits traffic using the type of firewall authentication you applied to the policy.• Deny—Device silently drops all packets for the session and does not send any active control messages such as TCP Resets or ICMP unreachable.• Reject—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.
Options	

Table 62: Fields on the Create Firewall Policy Page (continued)

Field	Description
Scheduling	<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>To add a schedule to a firewall policy:</p> <ol style="list-style-type: none"> 1. Click on Scheduling, to enable scheduling. 2. Click the add icon (+), to add an existing schedule. If you want to view more results in the End Points pane, click View more results. Alternately, you can add a schedule from the End Points panel, by selecting the schedule and clicking on the check mark icon (✓). 3. The selected schedule is added to the firewall policy. <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"> 1. Click on Scheduling, to enable scheduling. 2. Click the add icon (+), and then click Add new schedule. The Create Schedules page appears. 3. Alternately, click the lesser-than icon (<) to open the End Points panel. Click on the add icon (+) on the top right of the panel and select Schedule. The Create Schedules page appears. 4. Create a new schedule. See "Creating Schedules" on page 171. The new schedule appears in the list of schedules when you click on Scheduling and in the End Points tab, under Schedules. 5. Select the schedule and click on the add icon (+) to add it to the firewall policy.
Logging	<p>Enable logging by selecting the Logging option. You can see the logged firewall events in the Firewall Events page by using Monitor > Security Events > Firewall Events.</p> <p>For more information on the Firewall Events page, see "About the Firewall Events Page" on page 33.</p>

Table 62: Fields on the Create Firewall Policy Page (continued)

Field	Description
UTM	<p>Enable the UTM option for protection against multiple threat types including spam and malware, and control access to unapproved websites and content. Click Select UTM profile to select a UTM profile from the list of UTM profiles displayed.</p> <ul style="list-style-type: none">• Click on View more results to see more UTM profile in the Endpoints panel on the right.• Click Add new profile to create a new UTM profile. See “Creating UTM Profiles” on page 181 for more information on creating a new UTM profile.

Create source and destination endpoints

Table 62: Fields on the Create Firewall Policy Page (continued)

Field	Description
End Points	

Table 62: Fields on the Create Firewall Policy Page (continued)

Field	Description
	<p>To add an end point to the source or destination:</p> <ol style="list-style-type: none"> Click on Source or Destination and then click the lesser-than icon on the right side of the page to open the End Points panel. <p>The End Points panel displayed the end points relevant to the source or destination based on your selection.</p> <ul style="list-style-type: none"> End points from addresses, departments, users, and sites are displayed for source. <p>NOTE: If JIMS is not configured for CSO, users will not be listed in the Endpoints panel. Instead you will be provided with an option to import users through the Administration > Identity Management page. To import users, click Set Up and follow the steps provided in "About the Identity Management Page" on page 411.</p> End points from addresses, applications, departments, services, and sites are displayed for destination. <p>NOTE: You can also search for a specific end point using the search option.</p> (Optional) Click on the edit icon (pencil symbol) to modify an end point. (Optional) Click on the details icon on the right of the endpoint, to view more information about a source or destination endpoint. Select the end point you want to add and click on the check mark icon (✓) to add it the source or destination. <p>The selected end point is added to the source or destination.</p> <p>To create new source and destination endpoints:</p> <ol style="list-style-type: none"> Click the less-than icon (<) on the right side of the page, to open the End Points panel. Click on the add icon (+) on the top right of the End Points panel. <p>A list of end points that you can create is displayed.</p> Select the end point you want to create. <p>You can create the following end points:</p> <ul style="list-style-type: none"> Create an address. See "Creating Addresses or Address Groups" on page 287. Create a site group. See "Creating Site Groups" on page 366. Create a department. See "Creating a Department" on page 305. Create a service. See "Creating Services and Service Groups" on page 292. Create an application signature group. See "Creating Application Signature Groups" on page 301. Create a schedule. See "Creating Schedules" on page 171. Click Save to create the new end point. <p>The created end point is listed in the End Points panel.</p>

Table 62: Fields on the Create Firewall Policy Page (continued)

Field	Description
	<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 on page 123](#)
- [About the Firewall Policy Page on page 124](#)
- [Firewall Policy Examples on page 139](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)
- [Creating Addresses or Address Groups on page 287](#)
- [Creating Site Groups on page 366](#)
- [About the Sites Page on page 317](#)
- [Creating a Department on page 305](#)
- [Creating Application Signature Groups on page 301](#)
- [Creating Services and Service Groups on page 292](#)

Editing, Cloning, and Deleting Firewall Policy Intents

You can edit, clone, and delete firewall policy intents from the **Firewall Policy** page.

- [Editing Firewall Policy Intents on page 131](#)
- [Cloning Firewall Policy Intents on page 132](#)
- [Deleting Firewall Policy Intents on page 132](#)

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 intents associated with the policy.

2. Hover over the firewall policy intent 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 [“Creating Firewall Policy Intents” on page 125](#).
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.

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. Hover over the firewall policy intent that you want to clone, and then click on the clone icon 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. Update the cloned intent as required.
3. 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. Select the firewall policy intent you want to delete and then click the delete icon (X).
An alert message appears, verifying that you want to delete the selected intent.
3. Click **Yes** to delete the selected intent. If you do not want to delete, click **Cancel** instead.

If you click **OK**, the selected intent is deleted from the policy.

Related Documentation

- [Firewall Policy Overview on page 123](#)
- [About the Firewall Policy Page on page 124](#)
- [Firewall Policy Examples on page 139](#)

- [Creating Firewall Policy Intents on page 125](#)

Selecting Firewall Source

The following procedures provides various methods using which you can chose a Firewall source end point:

- [Adding an End Point as Firewall Source on page 133](#)
- [Selecting Firewall Source Using Abbreviations on page 134](#)
- [Selecting a Firewall Source from the End Points Panel on page 134](#)
- [Creating and Selecting a Firewall Source from the End Points Panel on page 135](#)
- [Creating Addresses from Source on page 135](#)
- [Creating Departments from Source on page 135](#)

Adding an End Point as Firewall Source

View and select the source end point from the complete list of addresses, sites, site groups, 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, and site groups 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**.

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 133](#).

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 135](#)

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, and site groups.

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 a 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 287](#).
- To create a new department, see [“Creating a Department” on page 305](#).
- To create a site or site group department, see [“Creating Site Groups” on page 366](#).

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 287](#).
 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.

Creating Departments from Source

Create a new department from the **Source** field and use the newly created department as a source end point:

To create a new department from **Source**:

1. In **Source**, type **dept**. The link **Add new department** appears at the bottom of the list of departments.

2. Click on **Add new department**, to create a new department.

The **Create Department** page appears.

3. Configure the new department. See [“Creating a Department” on page 305](#).

4. Click **Save** to save the new department.

The new department is created, and will be listed as an option for the source. Select the new department to add it to the source.

**Related
Documentation**

- [Selecting Firewall Destination on page 136](#)
- [Creating Firewall Policy Intents on page 125](#)
- [Firewall Policy Overview on page 123](#)
- [About the Firewall Policy Page on page 124](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)

Selecting Firewall Destination

The following procedures provides various methods using which you can chose a firewall destination end point:

- [Adding an End Point as Firewall Destination on page 137](#)
- [Selecting Firewall Destination Using Abbreviations on page 137](#)
- [Selecting a Firewall Destination from the End Points Panel on page 137](#)
- [Creating and Selecting a Firewall Destination from the End Points Panel on page 138](#)
- [Creating Addresses from Destination on page 138](#)
- [Creating Departments from Destination on page 139](#)

Adding an End Point as Firewall Destination

View and select the end point from the complete list of addresses, applications, departments, services, sites, or site groups.



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**.

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 137](#).

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 138](#).

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, and site groups.

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 287](#).
- To create a new department, see [“Creating a Department” on page 305](#).
- To create a site or site group department, see [“Creating Site Groups” on page 366](#).

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 287](#).
 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 Departments from Destination

Create a new department from the **Destination** field and use the newly created department as a destination end point:

To create a new department from **Destination**:

1. In **Destination**, type **dept**. The link **Add new department** appears at the bottom of the list of departments.
2. Click on **Add new department**, to create a new department.
The **Create Department** page appears.
3. Configure the new department. See [“Creating a Department” on page 305](#).
4. Click **Save** to save the new department.
The new department is created, and will be listed as an option for the destination. Select the new department to add it to the destination.

Related Documentation

- [Creating Firewall Policy Intents on page 125](#)
- [Firewall Policy Overview on page 123](#)
- [About the Firewall Policy Page on page 124](#)
- [Editing, Cloning, and Deleting Firewall Policy Intents on page 131](#)

Firewall Policy Examples

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.

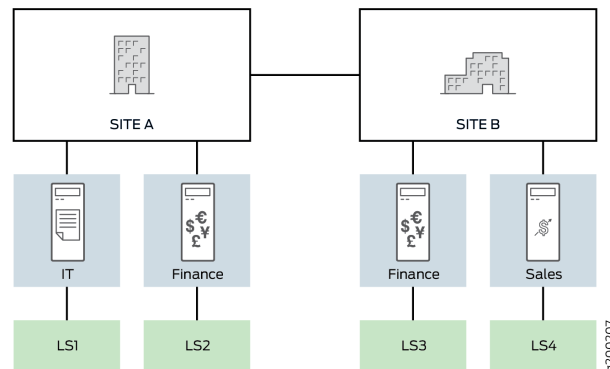


NOTE: For more information, see [“Firewall Policy Overview” on page 123](#) and [“Creating Firewall Policy Intents” on page 125](#).

For easier understanding, all the examples have been defined to use the topology in illustrated in [Figure 1 on page 140](#). 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 1: 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 63 on page 141](#) captures the addresses associated with the LAN segments used in the topology illustrated in [Figure 1 on page 140](#).

Table 63: 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 on page 141](#)
- [Example 2: Firewall Policy that Permits Internet Access for all Departments in Site A and Site B on page 143](#)
- [Example 3: Firewall Policy that Permits Any Public Internet Address to Access the Sales Department in Site B on page 145](#)
- [Example 4: Firewall Policy that Permits Social Media Access to all Departments in Site A on page 146](#)
- [Example 5: Firewall Policy that Controls Access to Specific Applications for Various Departments on page 148](#)
- [Example 6: Firewall Policy that Denies Access to Social Networking Sites on page 154](#)
- [Example 7: Firewall Policy that Controls Access to an Address over the Internet \(HTTP\) on page 156](#)
- [Example 8: Firewall Policy that Permits or Denies the Use of HTTP or FTP as a Service on page 161](#)
- [Example 9: Firewall Policy that Denies Access to BitTorrent to the Finance Departments across both Site A and Site B on page 162](#)
- [Example 10: Firewall Policy that Allows Access to Facebook for Users in User Group A on page 164](#)
- [Example 11: Firewall Policy that Permits User B in Site A Access to YouTube with UTM Enabled on page 167](#)

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 64 on page 142](#) shows the firewall policy intent that is defined:

Table 64: Firewall Policy Intent Definition for Example - 1

Source	Destination	Action
site A	site B	Permit

Table 65 on page 142 shows how this firewall policy intent is resolved:

Table 65: 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
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 1s-192.168.1.0/24-SP50-L2;
            destination-address [1s-198.51.100.0/24-SP50-L3,
1s-203.0.113.0/24-SP50-L4];
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone IT to-zone trust {
    policy Intent_1__1 {
        match {
            source-address 1s-192.0.2.0/24-S42-L1;
            destination-address [1s-198.51.100.0/24-SP50-L3,
1s-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 [1s-198.51.100.0/24-SP50-L3,
1s-203.0.113.0/24-SP50-L4];
      destination-address 1s-192.0.2.0/24-S42-L1;
      application any;
    }
    then {
      permit;
    }
  }
}
from-zone trust to-zone FINANCE {
  policy Intent_1__1 {
    match {
      source-address [1s-198.51.100.0/24-SP50-L3,
1s-203.0.113.0/24-SP50-L4];
      destination-address 1s-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 66 on page 143 shows the firewall policy intent that is defined:

Table 66: 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 67 on page 144 shows how this firewall policy intent is resolved:

Table 67: 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 68 on page 145 shows the firewall policy intent that is defined:

Table 68: Firewall Policy Intent Definition for Example - 3

Source	Destination	Action
Internet	Sales, site B	Permit

Table 69 on page 145 shows how this firewall policy intent is resolved:

Table 69: 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 1s-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 70 on page 146 shows the firewall policy intent that is defined:

Table 70: Firewall Policy Intent Definition for Example - 4

Source	Destination	Action
site A	Facebook	Permit

Table 71 on page 146 shows how this firewall policy intent is resolved:

Table 71: 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 1s-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 1s-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 72 on page 148 shows the firewall policy intents that are to fulfil this requirement:

Table 72: 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
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 73 on page 148 shows how this firewall policy intent is resolved:

Table 73: 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

Table 73: Firewall Policy Intent Resolution for Example - 5 (continued)

Source Department	Source Address	Zone	Destination Address	Service	Application Firewall Profile
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
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 1s-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 1s-192.0.2.0/24-S42-L1;
        destination-address any;
        application any;
    }
    then {
        permit {
            application-services {
                application-firewall {
                    rule-set AppFwProfile_3;
                }
            }
        }
    }
}
}
policy Intent_4__1 {
    match {
        source-address any;
        destination-address any;
        application [junos-telnet junos-ssh];
    }
}
```

```

    }
    then {
        deny;
    }
}
}

```

The hierarchy level for the following configuration sample is **[edit security application-firewall]**.

```

rule-sets AppFwProfile_1-1 {
    rule rule-1 {
        match {
            dynamic-application [junos:BBC junos:CNN];
            ssl-encryption any;
        }
        then {
            permit;
        }
    }
    default-rule {
        deny;
    }
}
rule-sets AppFwProfile_3 {
    rule rule-2 {
        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 74 on page 154 shows the firewall policy intent that is needed to fulfil this requirement:

Table 74: 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 75 on page 154 shows how this firewall policy intent is resolved:

Table 75: 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 1s-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 1s-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 76 on page 156 shows the firewall policy intents that are needed to fulfil this requirement:

Table 76: 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 77 on page 156 shows how this firewall policy intent is resolved:

Table 77: 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
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-f3d7-4cb3-89b6-78328e3bff38-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-f3d7-4cb3-89b6-78328e3bff38-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 78 on page 161 shows the firewall policy intents that are needed to fulfil this requirement:

Table 78: 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 79 on page 161 shows how this firewall policy intent is resolved:

Table 79: 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 80 on page 162 shows the firewall policy intents that are needed to fulfil this requirement:

Table 80: Firewall Policy Intent Definition for Example - 9

Source	Destination	Action
site A, Finance department	BitTorrent	Deny
site B, Finance department	BitTorrent	Deny

Table 81 on page 162 shows how this firewall policy intent is resolved:

Table 81: 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 1s-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 Finance1 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 1s-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 82 on page 164](#) shows the firewall policy intent that is needed to fulfil this requirement:

Table 82: Firewall Policy Intent Definition for Example - 10

Source	Destination	Action
user group A, site A	Facebook	Permit

[Table 83 on page 165](#) shows how this firewall policy intent is resolved:

Table 83: 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 84 on page 167 shows the firewall policy intent that is needed to fulfil this requirement:

Table 84: Firewall Policy Intent Definition for Example - 11

Source	Destination	Action
user B, site A	YouTube	Permit

Table 85 on page 167 shows how this firewall policy intent is resolved:

Table 85: 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 1s-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;
}
```

- Related Documentation**
- [Firewall Policy Overview on page 123](#)
 - [Creating Firewall Policy Intents on page 125](#)

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 on page 170](#)
- [Firewall Policy Examples on page 139](#)
- [Creating Schedules on page 171](#)
- [Editing, Cloning, and Deleting Schedules on page 173](#)

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 171](#).
- Modify, clone, or delete a firewall policy schedule. See [“Editing, Cloning, and Deleting Schedules” on page 173](#).

- 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**. See “[Viewing Object Details](#)” on page 17.
- Show or hide columns about the firewall policy schedule. See “[Sorting Objects](#)” on page 17.
- Search for a specific firewall policy schedule. See “[Searching for Text in an Object Data Table](#)” on page 18.

Field Descriptions

Table 86 on page 171 provides guidelines on using the fields on the **Firewall Policy Schedules** page.

Table 86: 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.
Second End Date	The second date and time from when the schedule ends.

Related Documentation

- [Firewall Policy Schedules Overview on page 170](#)
- [Firewall Policy Examples on page 139](#)
- [Creating Schedules on page 171](#)
- [Editing, Cloning, and Deleting Schedules on page 173](#)

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 87 on page 172](#).
- 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 87 on page 172](#) provides guidelines on using the fields to create a schedule.

Table 87: Fields on the Create Schedules Page

Field	Description
General Information	
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.
Dates	
Date Range	Select Ongoing if you want your schedules to always be active. Select Custom to configure two sets of start and end dates for a single schedule. For the first set, enter dates in the Start Date and End Date fields. You must enter the days in MM/DD/YYYY format. For the second set of the schedule, enter the start date in the Second Start Date field and enter the end date in the Second End Date field.
Times	
Time Ranges	Create a schedule to be active daily or for any specific times of the day.
Daily Options	Select Daily to make the schedule applicable daily. Select Custom 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. 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. Select Specify the same time for all days to enter a date and time that is applicable for all days.

- Related Documentation
- [Firewall Policy Schedules Overview on page 170](#)
 - [About the Firewall Policy Schedules Page on page 170](#)

- [Firewall Policy Examples on page 139](#)
- [Editing, Cloning, and Deleting Schedules on page 173](#)

Editing, Cloning, and Deleting Schedules

You can edit, clone, and delete schedules from the **Firewall Policy Schedules** page.

- [Editing Schedules on page 173](#)
- [Cloning Schedules on page 173](#)
- [Deleting Schedules on page 174](#)

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 171](#).
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 171](#).

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 on page 170](#)
- [About the Firewall Policy Schedules Page on page 170](#)
- [Creating Schedules on page 171](#)
- [Firewall Policy Examples on page 139](#)

CHAPTER 14

Unified Threat Management

- [UTM Overview on page 176](#)
- [Configuring UTM Settings on page 178](#)
- [About the UTM Profiles Page on page 179](#)
- [Creating UTM Profiles on page 181](#)
- [Editing, Cloning, and Deleting UTM Profiles on page 183](#)
- [About the Web Filtering Profiles Page on page 185](#)
- [Creating Web Filtering Profiles on page 187](#)
- [Editing, Cloning, and Deleting Web Filtering Profiles on page 191](#)
- [About the Antivirus Profiles Page on page 193](#)
- [Creating Antivirus Profiles on page 194](#)
- [Editing, Cloning, and Deleting Antivirus Profiles on page 196](#)
- [About the Antispam Profiles Page on page 198](#)
- [Creating Antispam Profiles on page 199](#)
- [Editing, Cloning, and Deleting Antispam Profiles on page 201](#)
- [About the Content Filtering Profiles Page on page 202](#)
- [Creating Content Filtering Profiles on page 204](#)
- [Editing, Cloning, and Deleting Content Filtering Profiles on page 207](#)
- [About the URL Patterns Page on page 209](#)
- [Creating URL Patterns on page 209](#)
- [Editing, Cloning, and Deleting URL Patterns on page 211](#)
- [About the URL Categories Page on page 212](#)
- [Creating URL Categories on page 213](#)
- [Editing, Cloning, and Deleting URL Categories on page 214](#)

UTM Overview

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 on page 177](#)
- [UTM Components on page 177](#)

UTM Licensing

All UTM components require licenses with the exception of content filtering with custom URLs only. 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 2 on page 177](#).

Figure 2: 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

- [Configuring UTM Settings on page 178](#)
- [About the UTM Profiles Page on page 179](#)
- [Creating UTM Profiles on page 181](#)

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 88 on page 178](#).

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 88: UTM Settings

Setting	Guideline
Antispam Settings	
Address Whitelist	<p>Select the URL pattern to be used as the antispam whitelist.</p> <p>Alternatively, click Create a New Pattern to create a new URL pattern to use as a whitelist.</p> <p>The Create URL Patterns page appears. For more information, see “Creating URL Patterns” on page 209 for an explanation of the fields on this page.</p>
Address Blacklist	<p>Select the URL pattern to be used as the antispam blacklist.</p> <p>Alternatively, click Create a New Pattern to create a new URL pattern to use as a blacklist.</p>
Antivirus Settings	
MIME Whitelist	Enter one or more MIME types (separated by commas) to exclude from antivirus scanning.
Exception MIME Whitelist	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 whitelist. This list is a subset of the MIME types that you specified in the MIME whitelist. For example, if you specify video/ in the whitelist and video/x-shockwave-flash in the exception whitelist, all objects of MIME type video/ except MIME type video/x-shockwave-flash are excluded from antivirus scanning.
URL Whitelist	Select the URL whitelist for the antivirus settings.

Table 88: UTM Settings (continued)

Setting	Guideline
Web Filtering Settings	
URL Whitelist	Select the URL whitelist for the Web filtering settings; these URLs are excluded from Web filtering.
URL Blacklist	Select the URL blacklist for the Web filtering settings; these URLs are blocked from Web access.

Related Documentation

- [About the UTM Profiles Page on page 179](#)

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 181](#).
- Edit, clone, or delete a UTM profile—See [“Editing, Cloning, and Deleting UTM Profiles” on page 183](#).
- 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 90 on page 180](#) 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 89 on page 179](#) describes the fields on the UTM Profiles page.

Table 89: UTM Profiles Page Fields

Field	Description
Name	Name of the UTM profile.

Table 89: UTM Profiles Page Fields (continued)

Field	Description
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 90: UTM Profile Details Page Fields

Field	Description
General Information	
Name	Name of the UTM profile.
Description	Description of the UTM profile.
Traffic Options-	
Action When Connection Limit Is Reached	Action to be taken when the configured connection limit per client is reached.
Web Filtering Profile	
HTTP	Web filtering profile to be used for HTTP traffic.
Antivirus Profile	
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.
Antispam Profile	
SMTP	Antispam profile to be used for SMTP traffic.

Related Documentation • [Creating UTM Profiles on page 181](#)

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 91 on page 181](#).



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 91: UTM Profile Settings

Setting	Guideline
General	
Name	Enter a unique name for the UTM profile. The maximum length is 29 characters.
Description	Enter a description for the UTM profile. The maximum length is 255 characters.
Traffic Options	
NOTE: 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.	

Table 91: UTM Profile Settings (continued)

Setting	Guideline
Connection Limit per Client	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.
Action when connection limit is reached	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 Next to continue.
Web Filtering	
HTTP	Select the Web filtering profile to be applied for HTTP traffic. Alternatively, click Create Another Profile to create a Web filtering profile. The Create Web Filtering Profiles wizard appears. See "Creating Web Filtering Profiles" on page 187 for an explanation of the fields on this wizard. Click Back to go the preceding step or click Next to go to the next step.
Antivirus	
Apply to all protocols	Select this check box to apply a single antivirus profile to all traffic protocols. and then specify the profile in the Default Profile field. Clear the check box if you want to apply traffic-specific profiles.
Default Profile	Select the antivirus profile to be applied to all traffic protocols. Click Back to go the preceding step or click Next to go to the next step.
NOTE: Click Create Another Profile to create an antivirus profile that you can then assign. The Create Antivirus Profiles wizard appears. See "Creating Antivirus Profiles" on page 194 for an explanation of the fields on this wizard.	
HTTP	Select the antivirus profile to be applied to HTTP traffic.
FTP Upload	Select the antivirus profile to be applied to FTP upload traffic.
FTP Download	Select the antivirus profile to be applied to FTP download traffic.
IMAP	Select the antivirus profile to be applied to IMAP traffic.
SMTP	Select the antivirus profile to be applied to SMTP traffic.
POP3	Select the antivirus profile to be applied to POP3 traffic. Click Back to go the preceding step or click Next to go to the next step.
Antispam	

Table 91: UTM Profile Settings (continued)

Setting	Guideline
SMTP	<p>Select the antispam profile to be applied for SMTP traffic.</p> <p>Alternatively, click Create Another Profile to create an antispam profile. The Create Antispam Profiles wizard appears. See “Creating Antispam Profiles” on page 199 for an explanation of the fields on this wizard.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Content Filtering	
Apply to all protocols	<p>Select this check box to apply a single content filtering profile to all traffic protocols, and then specify the profile in the Default Profile field.</p> <p>Clear the check box if you want to apply traffic-specific profiles.</p>
Default Profile	<p>Select the content filtering profile to be applied to all traffic protocols.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
<p>NOTE: Click Create Another Profile to create a content filtering profile that you can then assign. The Create Content Filtering Profiles wizard appears. See “Creating Content Filtering Profiles” on page 204 for an explanation of the fields on this wizard.</p>	
HTTP	Select the content filtering profile to be applied to HTTP traffic.
FTP Upload	Select the content filtering profile to be applied to FTP upload traffic.
FTP Download	Select the content filtering profile to be applied to FTP download traffic.
IMAP	Select the content filtering profile to be applied to IMAP traffic.
SMTP	Select the content filtering profile to be applied to SMTP traffic.
POP3	<p>Select the content filtering profile to be applied to POP3 traffic.</p> <p>Click Back to go the preceding step.</p>

- Related Documentation**
- [About the UTM Profiles Page on page 179](#)
 - [Configuring UTM Settings on page 178](#)

Editing, Cloning, and Deleting UTM Profiles

You can edit, clone, and delete UTM profiles from the UTM Profiles page. This topic has the following sections:

- [Editing UTM Profiles on page 184](#)
- [Cloning UTM Profiles on page 184](#)
- [Deleting UTM Profiles on page 185](#)

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.
3. Click **Yes** to delete the selected UTM profiles.
A confirmation message appears, indicating the status of the delete operation.

- Related Documentation**
- [Creating UTM Profiles on page 181](#)
 - [About the UTM Profiles Page on page 179](#)

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 92 on page 185](#) lists the Web filtering solutions that are supported and the license requirements.

Table 92: 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.

Table 92: Web Filtering Solutions Supported (continued)

Type	Description	License Requirement
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 whitelist or blacklist 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 187](#).
- Edit, clone, or delete a Web filtering profile—See [“Editing, Cloning, and Deleting Web Filtering Profiles” on page 191](#).
- 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 94 on page 186](#) 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 93 on page 186](#) describes the fields on the Web Filtering Profiles page.

Table 93: 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 94: Web Filtering Profile Details Page Fields

Field	Description
General Information	

Table 94: Web Filtering Profile Details Page Fields (continued)

Field	Description
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.
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"> • Very Safe • Moderately Safe • Fairly Safe • Suspicious • Harmful
URL Categories	URL categories associated with the Web filtering profile.

- Related Documentation**
- [Creating Web Filtering Profiles on page 187](#)
 - [Editing, Cloning, and Deleting Web Filtering Profiles on page 191](#)

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 95 on page 188](#).



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 95: Creating Web Filtering Profiles Settings

Setting	Guideline
General Information	
Name	Enter a unique name for the Web filtering profile. The maximum length is 29 characters.
Description	Enter a description for the Web filtering profile. The maximum length is 255 characters.
Timeout	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.
Engine Type	Select an engine type for Web filtering: <ul style="list-style-type: none"> • (Default) Juniper Enhanced—UTM-enhanced Web filtering. • Websense Redirect—Redirect Web filtering profile.
Safe Search	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. Clear the check box to disable safe search redirects. NOTE: 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.
Custom Block Message/URL	Specify the redirect URL or a custom message to be sent when HTTP requests are blocked. The maximum length is 512 characters. NOTE: 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. Click Back to go the preceding step or click Next to go to the next step.

Table 95: Creating Web Filtering Profiles Settings (continued)

Setting	Guideline
Custom Quarantine Message	<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"> • URL name • Quarantine name • Category (if available) • Site reputation (if available) <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: ***The requested webpage is blocked by your organization's access policy***.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Account	Specify the user account associated with the Websense Web filtering profile.
Server	Specify the hostname or IP address for the Websense server.
Port	Enter the number of sockets used for communication between the client and the server. The default value is 8.
Sockets	<p>Specify the port number to use to communicate with the Websense server. The default port value is 15968.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
URL Categories	
Deny Action List	<p>Click the Add URL Categories 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 Table 96 on page 190,</p> <p>The list of URL categories selected is displayed in a text box.</p>
Log & Permit Action List	<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 Table 96 on page 190.</p> <p>The list of URL categories selected is displayed in a text box.</p>
Permit Action List	<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 Table 96 on page 190</p> <p>The list of URL categories selected is displayed in a text box.</p>

Table 95: Creating Web Filtering Profiles Settings (continued)

Setting	Guideline
Quarantine Action List	<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 Table 96 on page 190.</p> <p>The list of URL categories selected is displayed in a text box.</p> <p>Click Back to go the preceding step or click Next to go to the next step.</p>
Fallback Options	
Global Reputation Actions	<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"> • Very Safe—Permit, log and permit, block, or quarantine a request if a site reputation of 90 through 100 is returned. By default, Permit is selected. • Moderately Safe—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. • Fairly Safe—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. • Suspicious—Permit, log and permit, block, or quarantine a request if a site reputation of 60 through 69 is returned. By default, Quarantine is selected. • Harmful—Permit, log and permit, block, or quarantine a request if a site reputation of zero through 59 is returned. By default, Block is selected.
Default Action	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.
Fallback Action	<p>Select the fallback action, which is used when:</p> <ul style="list-style-type: none"> • The ThreatSeeker Websense Cloud servers are unreachable. • A timeout occurs for requests to ThreatSeeker Cloud. • There are too many requests to be handled by the device.

Table 96: Select URL Categories Settings

Setting	Guideline
Show	<p>Choose which URL categories should be displayed for selection: All categories, Custom URL categories, or Websense URL categories.</p> <p>The Available column of the URL Categories field displays URL categories based on your selection.</p>

Table 96: Select URL Categories Settings (continued)

Setting	Guideline
URL Categories	<p>Select one or more URL categories in the Available column and click the forward arrow to confirm your selection. The selected URL categories are displayed in the Selected column.</p> <p>Alternatively, click Create New URL Category to create a URL category and assign it to the URL category. The Create URL Categories page appears; for more information, see “Creating URL Categories” on page 213.</p> <p>Click OK to confirm your selection. You are returned to the Create Web Filtering Profiles page.</p>

Related Documentation

- [Creating UTM Profiles on page 181](#)

Editing, Cloning, and Deleting Web Filtering Profiles

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 on page 191](#)
- [Cloning Web Filtering Profiles on page 192](#)
- [Deleting Web Filtering Profiles on page 192](#)

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 on page 187](#)
- [About the Web Filtering Profiles Page on page 185](#)

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 194](#).
- Edit, clone, or delete an antivirus profile—See [“Editing, Cloning, and Deleting Antivirus Profiles” on page 196](#).
- 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 98 on page 194](#) 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 97 on page 193](#) describes the fields on the Antivirus Profiles page.

Table 97: 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 98: Antivirus Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the antivirus profile.
Description	Description of the antivirus profile.
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 on page 181](#)

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 99 on page 195](#).



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 99: Antivirus Profile Settings

Setting	Guideline
General Information	
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	<p>Displays the engine type used for scanning. Currently, Sophos is the only antivirus engine supported.</p> <p>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.</p>
Fallback Options	
	<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"> • Content Size—Select an option to specify whether the content should be blocked (default) or logged and permitted if the content size the previously defined limit. • Content Size Limit—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. • Engine Error—Select the action to take (Block [default] or Log and Permit) 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. • Default Action—Select the default action (Block [default] or Log and Permit) to take when an error occurs.
Notification Options	

Table 99: Antivirus Profile Settings (continued)

Setting	Guideline
	<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"> • Fallback Deny—Select this option to notify mail senders that their messages were blocked. • Fallback Non-Deny—Select this option to warn mail recipients that they received unblocked messages despite problems. • Virus Detected—Select this option to notify mail recipients that their messages were blocked.

Related Documentation • [Creating UTM Profiles on page 181](#)

Editing, Cloning, and Deleting Antivirus Profiles

You can edit, clone, and delete antivirus profiles from the Antivirus Profiles page. This topic has the following sections:

- [Editing Antivirus Profiles on page 196](#)
- [Cloning Antivirus Profiles on page 197](#)
- [Deleting Antivirus Profiles on page 197](#)

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 on page 194](#)
- [About the Antivirus Profiles Page on page 193](#)

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 199](#).
- Edit, clone, or delete an antispam profile—See [“Editing, Cloning, and Deleting Antispam Profiles” on page 201](#).
- 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 101 on page 199](#) 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 100 on page 198](#) describes the fields on the Antispam Profiles page.

Table 100: Antispam Profiles Page Fields

Field	Description
Name	Name of the antispam profile.
Blacklist	Indicates whether server-based spam filtering or local spam filtering is used.
Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.
Description	Description of the antispam profile.

Table 101: Antispam Profile Details Page Fields

Field	Description
Name	Name of the antispam profile.
Description	Description of the antispam profile.
Sophos Blacklist	Indicates whether Sophos Blacklist is enabled (server-based filtering) or disabled (local filtering).
Default Action	Action to be taken when spam is detected.
Custom Tag	Custom-defined tag that identifies an e-mail message as spam.

Related Documentation • [Creating UTM Profiles on page 181](#)

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 whitelists (benign) and blacklists (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 102 on page 200](#).



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 102: 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>NOTE: Server-based spam filtering supports only IP-based spam block list blacklist lookup. Sophos updates and maintains the IP-based spam block list. Server-based antispam filtering is a separately licensed subscription service.</p>
Action	
Default Action	<p>Select the action to be taken when spam is detected:</p> <ul style="list-style-type: none"> • Tag Email Subject Line • Tag SMTP Header • Block Email • None
Custom Tag	Enter a custom string for identifying a message as spam. The maximum length is 512 characters and the default is ***SPAM*** .

Related Documentation

- [Creating UTM Profiles on page 181](#)

Editing, Cloning, and Deleting Antispam Profiles

You can edit, clone, and delete antispam profiles from the Antispam Profiles page. This topic has the following sections:

- [Editing Antispam Profiles on page 201](#)
- [Cloning Antispam Profiles on page 201](#)
- [Deleting Antispam Profiles on page 202](#)

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 on page 198](#)

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 204](#).
- Edit, clone, or delete a content filtering profile—See [“Editing, Cloning, and Deleting Content Filtering Profiles” on page 207](#).
- 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 104 on page 203](#) 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 103 on page 203](#) describes the fields on the Content Filtering Profiles page.

Table 103: 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 104: Content Filtering Profiles Details Page Fields

Field	Description
General Information	
Name	Name of the content filtering profile.
Description	Description of the content filtering profile.
General Information	
Notify Mail Sender	Specifies whether the option to notify the e-mail sender is enabled or disabled.
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.

Table 104: Content Filtering Profiles Details Page Fields (continued)

Field	Description
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 on page 181](#)

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 105 on page 204](#) 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 105: Supported Content Filter Types

Type	Description
MIME pattern filter	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. NOTE: The exception list has a higher priority than the block list.
Block Extension List	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.

Table 105: Supported Content Filter Types (continued)

Type	Description
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>NOTE: 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 106 on page 205](#).



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 106: Content Filtering Profile Settings

Setting	Guideline
General Information	

Table 106: Content Filtering Profile Settings (continued)

Setting	Guideline
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.
Notification Options	
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 (Protocol or Message) from the drop-down list.
Custom Notification Message	Enter a custom notification message. The maximum length is 512 characters.
Protocol Commands	
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>
Command Permit List	Enter specific commands to be permitted for the HTTP, FTP, SMTP, IMAP, and POP3 protocols. Use commas to separate each command.
Content Types	
Block Content Type	<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"> • Active X • Windows executables (.exe) • HTTP cookie • Java applet • ZIP files
File Extensions	
Extension Block List	<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>
MIME Types	
MIME Block List	Enter the MIME types you want to block over HTTP, FTP, SMTP, IMAP, and POP3 connections. Use commas to separate each MIME type.
MIME Permit List	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 on page 181](#)

Editing, Cloning, and Deleting Content Filtering Profiles

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 on page 207](#)
- [Cloning Content Filtering Profiles on page 207](#)
- [Deleting Content Filtering Profiles on page 208](#)

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 on page 204](#)

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 209](#).
- Edit, clone, or delete a URL pattern—See [“Editing, Cloning, and Deleting URL Patterns” on page 211](#).
- 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 107 on page 209](#).
- 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 107 on page 209](#) describes the fields on the URL Patterns page.

Table 107: 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 on page 212](#)

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 108 on page 210](#).



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 108: Create URL Patterns Settings

Settings	Guidelines
Name	<p>Enter a unique name for the URL pattern.</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 29 characters.</p>
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 Create New URL Category to create a URL category, enter the URL category name in the text box, and click Save to assign the URL pattern to the new category.
Add URLs	<p>Enter one or more URLs (separated by commas) in the text box, and click Add. The URLs are displayed in the URL List table.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • The following wildcard characters are supported: <ul style="list-style-type: none"> • asterisk (*) • period (.) • square brackets ([]) • question mark (?) • Precede all wildcard characters with http://. • The asterisk (*) can only be used at the beginning of a URL and must be followed by a period (.). • The question mark (?) can only be used at the end of a URL. • The following are examples of wildcard syntaxes that are supported: http://*example.net, http://www.example.ne?, and http://www.example.n??. • The following are examples of wildcard syntaxes that are not supported: *example.???, http://*example.net, http://?, and www.example.ne?.

Related Documentation

- [Creating URL Categories on page 213](#)

Editing, Cloning, and Deleting URL Patterns

You can edit, clone, and delete URL patterns from the URL Patterns page. This topic has the following sections:

- [Editing URL Patterns on page 211](#)
- [Cloning URL Patterns on page 211](#)
- [Deleting URL Patterns on page 212](#)

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 on page 209](#)

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 213](#).
- Edit, clone, or delete a URL category—See [“Editing, Cloning, and Deleting URL Categories” on page 214](#).
- 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 109 on page 213](#) 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 109 on page 213](#) describes the fields on the URL Categories page.

Table 109: 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"> • Predefined—URL categories that are loaded by default. • Custom—URL categories that are created by the user.
Description	Description of the URL category.

Related Documentation • [About the URL Patterns Page on page 209](#)

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 110 on page 214](#).



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 110: Create URL Categories Settings

Settings	Guidelines
Name	Enter a unique name for the URL category. 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.
Description	Enter a description for the URL pattern. The maximum length is 255 characters.
URL Patterns	Select one or more URL patterns in the Available column and click the forward arrow to confirm your selection. The selected URL patterns are displayed in the Selected column. Alternatively, click Create a New Pattern to create a URL pattern and assign it to the URL category. The Create URL Patterns page appears. For more information, see "Creating URL Patterns" on page 209 NOTE: You must select at least one URL pattern.

Related Documentation

- [Editing, Cloning, and Deleting URL Categories on page 214](#)

Editing, Cloning, and Deleting URL Categories

You can edit, clone, and delete URL categories from the URL Categories page. This topic has the following sections:

- [Editing URL Categories on page 214](#)
- [Cloning URL Categories on page 215](#)
- [Deleting URL Categories on page 215](#)

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 on page 213](#)

Managing SD-WAN

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [About the SD-WAN Policy Page on page 220](#)
- [Creating SD-WAN Policy Intents on page 221](#)
- [Editing and Deleting SD-WAN Policy Intents on page 225](#)
- [About the Application SLA Profiles Page on page 226](#)
- [Creating SLA Profiles on page 227](#)
- [Editing and Deleting SLA Profiles on page 229](#)

SLA Profiles and SD-WAN Policies Overview

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

SLA Profiles

SLA profiles are created for applications or groups of applications for all tenants. An SLA profile consists of a set of configurable constraints that can be defined in the unified portal for both the Administration and Customer Portals. [Table 111 on page 217](#) lists the categories of configurable constraints that are defined in an SLA profile.

Table 111: SLA Profile Categories

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

Table 111: SLA Profile Categories (continued)

SLA parameters	<p>For SLA profiles that are not used for local breakout, you can also define one or more than one of the following SLA parameters:</p> <ul style="list-style-type: none"> Throughput—Amount of data (in Mbps) that is sent upstream and received downstream by the site during the selected time period Latency—Amount of time (in ms) that a packet of data takes to travel from one designated point to another Packet loss—Percentage of data packets dropped by the network to manage congestion Jitter—Difference between the maximum and minimum round-trip times (in ms) of a packet of data <p>SLA parameters have precedence over path preference. Even if one SLA parameter is defined, then it is given a higher priority and will override the path preference. SD-WAN policies mapped to an SLA profile with defined SLA parameters are called dynamic policies. Dynamic policies applied to sites enable the site to override the path preference and switch WAN links when the preferred WAN link is not meeting SLA requirements as defined in the SLA parameters.</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"> Maximum upstream and downstream rates—The maximum upstream and downstream rate for all applications associated with the SLA profile. Maximum upstream and downstream burst sizes—The maximum size of a steady stream of traffic sent at average rates that exceed the upstream and downstream rate limits for short periods.



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

SD-WAN Policies

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

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

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

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

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

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

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

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

Related Documentation

- [About the Application SLA Profiles Page on page 226](#)
- [About the SD-WAN Policy Page on page 220](#)
- [SD-WAN Events Overview on page 57](#)
- [Local Breakout Overview on page 319](#)

About the SD-WAN Policy Page

To access this page, select **Configuration > SD-WAN > SD-WAN Policy** page in the Customer Portal.

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.
- Create SD-WAN policy intents. See [“Creating SD-WAN Policy Intents” on page 221](#).
- Edit or delete SD-WAN policy intents. See [“Editing and Deleting SD-WAN Policy Intents” on page 225](#).
- Deploy SD-WAN policy intents. See [“Deploying Policies” on page 312](#).
- 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 112 on page 220](#) describes the fields on the SD-WAN Policy page.

Table 112: Fields on the SD-WAN Policy Page

Field	Description
Source	View 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	View 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.
SLA Profile	View the SLA profile associated with the policy intents. The SLA profiles are used by SD-WAN policy intents for managing traffic flow.
Options	<ul style="list-style-type: none">• Name—View the name of the policy intents.• Description—View the descriptions of the policy intents.

- Related Documentation**
- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
 - [Creating SD-WAN Policy Intents on page 221](#)

- [Editing and Deleting SD-WAN Policy Intents on page 225](#)

Creating SD-WAN Policy Intents

You can create policy intents for SD-WAN policies from the **SD-WAN Policy** page.

To create a policy intent:

1. Click the add icon (+) on the **Configuration > SD-WAN > SD-WAN Policy** in the Customer Portal.

The options to create policy intents appear within the SD-WAN Policy page.

2. Enter the policy intent information according to the guidelines provided in [Table 113 on page 222](#).

3. Click **Save** to create the policy intent.

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

Table 113: Fields on the Create SD-WAN Policy Intent Page

Field	Guidelines
Source	<p>You can select the source endpoints in one of the following ways:</p> <ul style="list-style-type: none"> • 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. • Select the source endpoints from the complete list of departments, sites, and site groups. To view the complete list of departments, sites, and site groups. <ol style="list-style-type: none"> 1. Click View more results. The complete list of departments, sites, and site groups is displayed in the End Points pane on the right. 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. 3. Click the add icon (+) to select the endpoint. • Enter an abbreviation in the Source 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"> • Click the endpoints in the filtered list to select them. • Click View more results to select the endpoint from the complete list of departments, sites, and site groups. • Click Add new department or Add new sitegroup to create new departments or site groups and select them. The Create Site Group page or Create Department page appears based on your selection. See “Creating a Department” on page 305 and “Creating Site Groups” on page 366 for information about creating site groups and departments. • Create site groups or departments to select the source endpoint from the newly created site group or department. To create site groups or departments: <ol style="list-style-type: none"> 1. Click anywhere within the Source field. 2. Click the lesser-than icon (<) on the right. The list of available departments, sites, and site groups is displayed in the End Points pane on the right. 3. (Optional) To view more information about a source endpoint, hover over the endpoint click the details icon. 4. Click the add icon (+) on the top right of the pane. 5. Click Department or Site Group as needed. The Create Department page or Create Site Group page appears based on your selection. See “Creating a Department” on page 305 and “Creating Site Groups” on page 366 for information about creating departments and site groups. 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 Cancel instead.

Table 113: Fields on the Create SD-WAN Policy Intent Page (continued)

Field	Guidelines
Application	<p>You can select the application endpoints in one of the following ways:</p> <ul style="list-style-type: none"> • Select application endpoints from the displayed list of applications and application groups. Click the endpoints to select them. • 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"> 1. Click View more results. The complete list of applications and applications groups is displayed in the End Points pane on the right. 2. (Optional) Hover over an application group and click the edit icon to edit the application group. 3. (Optional) Hover over an application and click the details icon to view details about the application. 4. Click the add icon (+) to select the endpoint. • Enter an abbreviation in the Application 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"> • Click the endpoints in the filtered list to select them. • Click View more results to select the endpoint from the complete list of applications and applications groups. • Click Add new application to create a new application group and select the application group. The Create Application Signature Group page appears. See "Creating Application Signature Groups" on page 301 for information about creating application groups. • 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"> 1. Click anywhere within the Application field. 2. Click the lesser-than icon (<) on the right. <p>The list of available applications, departments, sites, and site groups is displayed in the End Points pane on the right.</p> 3. Click the add icon (+) on the top right of the pane. 4. Click Application. The Create Application Signature Group page appears. See "Creating Application Signature Groups" on page 301 for information about creating application groups. 5. Click the check mark icon (✓) if you want to save the application signature group to the policy intent. Alternatively, if you want to discard your updates, click Cancel instead.

Table 113: Fields on the Create SD-WAN Policy Intent Page (continued)

Field	Guidelines
SLA Profile	<p>Select an SLA profile to apply to the source and application endpoints. You can select the SLA profile in one of the following ways:</p> <ul style="list-style-type: none"> Select SLA profile from the displayed list of SLA profiles. Click the SLA profile to select it. Select the SLA profile from the complete list of SLA profiles. To view the complete list of SLA profiles. <ol style="list-style-type: none"> Click View more results. The complete list of SLA profiles is displayed in the End Points pane on the right. Click the add icon (+) to select the SLA profile. Select SLA profile by creating a custom SLA profile. To create an SLA profile: <ol style="list-style-type: none"> Click anywhere within the SLA Profile field. Click the lesser-than icon (<) on the right. The list of SLA profiles is displayed in the End Points pane on the right. Click the add icon (+) on the top right of the pane. Click SLA Profile. The Create SLA Profile Page appears. See "Creating SLA Profiles" on page 227 for information about creating SLA profiles. Click the check mark icon (✓) if you want to save the SLA profile to the policy intent. Alternatively, if you want to discard your updates, click Cancel instead.
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 on page 217](#)
 - [About the SD-WAN Policy Page on page 220](#)
 - [Editing and Deleting SD-WAN Policy Intents on page 225](#)
 - [Deploying Policies on page 312](#)

Editing and Deleting SD-WAN Policy Intents

You can edit or delete SD-WAN policy intents from the SD-WAN Policy page.

- [Editing SD-WAN Policy Intents on page 225](#)
- [Deleting SD-WAN Policy Intents on page 225](#)

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 221](#).

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

Alternatively, click **Cancel** to discard your changes.

Deleting SD-WAN Policy Intents

If an SD-WAN intent is no longer needed, you can delete SD-WAN policy intents from the SD-WAN Policy page.

To delete SD-WAN policy intents:

1. Select one or more policy intents that you want to delete and click the delete icon (X).

A page requesting confirmation of deletion appears.

2. Click **Yes** to confirm that you want to delete the selected policy intents.

The policy intents are deleted.

Related Documentation

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [About the SD-WAN Policy Page on page 220](#)
- [Creating SD-WAN Policy Intents on page 221](#)

About the Application SLA Profiles Page

To access this page, select **Configuration > SD-WAN > Application SLA Profiles** in the Customer Portal.

You can use the Application SLA Profiles page to view information about service-level agreement (SLA) 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 SLA profiles for all tenants.
- Create an SLA profile for the tenant. See [“Creating SLA Profiles” on page 227](#).
- Edit the configuration of an existing SLA profile. See [“Editing and Deleting SLA Profiles” on page 229](#).
- Show or hide columns that contain information about SLA profiles. See [“Sorting Objects” on page 17](#).
- Search for SLA profiles using keywords. Click the search icon. Enter partial text or full text of the keyword in the search bar and press Enter. The search results are displayed.

Field Descriptions

[Table 114 on page 226](#) shows the descriptions of the fields on the Application SLA Profiles page.

Table 114: Fields on the Application SLA Profiles Page

Field	Description
Priority	View the SLA profile priority.
Name	View the SLA profile name.
Link Paths	View WAN link paths associated with the SLA profile.
Tenant	View the tenant associated with the SLA profile.
Class of Service	View the class of service associated with the SLA profile.
Local Breakout	View whether local breakout is enabled on the SLA profile.
Throughput Target	View the target throughput for the SLA profile.
Latency Target	View the target latency for the SLA profile.
Packet Loss Target	View the target packet-loss for the SLA profile.
Jitter Target	View the target jitter for the SLA profile.

Table 114: Fields on the Application SLA Profiles Page (continued)

Field	Description
Delay Target	View the target delay for the SLA profile. Target delay is calculated as two times the target latency.

Related Documentation

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [Local Breakout Overview on page 319](#)
- [Creating SLA Profiles on page 227](#)
- [Editing and Deleting SLA Profiles on page 229](#)

Creating SLA Profiles

You can use the Create SLA Profile page to create a new service-level agreement (SLA) profile for the current tenant and configure target metrics for the SLA profile.

To add an SLA Profile to the tenant:

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

The Create SLA Profile page appears.

2. Enter the general SLA profile information according to the guidelines provided in [Table 115 on page 227](#).

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

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

Table 115: Fields on the Create SLA Profile page

Field	Guidelines
<i>General</i>	
Name	Enter a name for the SLA profile. Can be a unique string of not more than 15 characters that contains alphanumeric characters and hyphen (-).
<i>SLA Configuration</i>	
Traffic Type Profile	Choose a traffic type profile to apply the class-of-service configuration and priority to the SLA profile. You can select a traffic type profile only when it is in the Enabled state.

Table 115: Fields on the Create SLA Profile page (continued)

Field	Guidelines
Local Breakout	Enable local breakout for the SLA profile. Local breakout is the ability of the site to route Internet traffic directly from the site.
Path Preference	Select the preferred WAN link type to associate with the SLA profile. The options are Any, MPLS, and Internet. Any is the default value. For SLA profiles that are used for local breakout, you must select a path preference. For SLA profiles that are not used for local breakout, you must select a path preference or configure at least one SLA parameter.
Failover	<p>Enable failover to switch links when the active links fail to meet the SLA criteria. In such cases, the traffic is routed to links that meet SLA criteria. Failover is supported only for MPLS or Internet links.</p> <p>NOTE: The Failover option is supported only for bandwidth-optimized SD-WAN networks.</p>
Path Failover Criteria	<p>Choose one of the following options:</p> <ul style="list-style-type: none"> • Does not meet one or more SLA parameters—This triggers the path failover if any of the SLA parameters is violated. • Does not meet all SLA parameters—This triggers the path failover only when all the SLA parameters are violated.
<i>SLA Parameters</i>	
Throughput	Enter the target throughput (in Mbps) for the SLA profile. Throughput is the amount of data that is sent upstream and received downstream by the site during the selected time period.
Latency	Enter the target latency (in ms) for the SLA profile. Latency is the amount of time that a packet of data takes to travel from one designated point to another. Target delay is calculated as two times the target latency.
Packet Loss	Enter the target packet loss (in %) for the SLA profile. Packet loss is the percentage of data packets dropped by the network to manage congestion.
Jitter	Enter the target jitter (in ms) for the SLA profile. Jitter is the difference between the maximum and minimum round-trip times of a packet of data.
<i>Advanced Configuration—SLA Sampling</i>	
Session-sampling %	Specify the matching percentage of sessions for which you want to run the passive probes.
SLA-violation-count	Specify the number of SLA violations after which you want CSO to switch paths. The range is 1 through 32.
Sampling-period	Specify the sampling period, in milliseconds, for which the SLA violations are counted. The range is 2000 through 60000.
Switch-cool-off-period	Specify the waiting period, in milliseconds, only after which you want the link switch to happen if an active link comes back online. This parameter helps prevent frequent switching of traffic between active and backup links. The range is 5 through 300.
<i>Advanced Configuration—Rate Limiting</i>	

Table 115: Fields on the Create SLA Profile page (continued)

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



NOTE: You can also create SLA profiles from the **Configuration > SD-WAN > SD-WAN Policies** page in the Customer Portal.

Related Documentation

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [About the Application SLA Profiles Page on page 226](#)
- [Editing and Deleting SLA Profiles on page 229](#)

Editing and Deleting SLA Profiles

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

- [Editing an SLA Profile on page 229](#)
- [Deleting SLA Profiles on page 230](#)

Editing an SLA Profile

To edit an SLA Profile:

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

The Edit Application SLA Profile page appears.

2. Update the general SLA profile information as needed according to the guidelines provided in [“Creating SLA Profiles” on page 227](#). You cannot edit the SLA profile name.
3. Click **Next**.

The Configuration tab appears.

4. Update the configuration parameters as needed according to the guidelines provided in [“Creating SLA Profiles” on page 227](#).
5. Click **OK** to save the updated SLA profile configuration.

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

Deleting SLA Profiles

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

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

A page requesting confirmation for the deletion appears.

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

The SLA profile is deleted.

Related Documentation

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [About the Application SLA Profiles Page on page 226](#)
- [Creating SLA Profiles on page 227](#)

CHAPTER 16

Managing NAT Policies

- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)
- [About the Single NAT Policy Page on page 238](#)
- [Creating NAT Policy Rules on page 240](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [Deploying NAT Policy Rules on page 247](#)
- [Selecting NAT Source on page 248](#)
- [Selecting NAT Destination on page 252](#)
- [NAT Pools Overview on page 255](#)
- [About the NAT Pools Page on page 256](#)
- [Creating NAT Pools on page 257](#)
- [Editing, Cloning, and Deleting NAT Pools on page 259](#)

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 116 on page 233](#) shows the persistent NAT support for different source NAT and destination NAT addresses.

Table 116: 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 117 on page 234](#) and [Table 118 on page 234](#) show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 117: 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 118: 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 on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)

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 235](#).
- Modify or delete a NAT policy. See [“Editing and Deleting NAT Policies” on page 237](#).
- Create, modify, clone, and delete NAT policy rules. See [“About the Single NAT Policy Page” on page 238](#).
- Search for a specific NAT policy. See [“Searching for Text in an Object Data Table” on page 18](#).
- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

[Table 119 on page 235](#) provides guidelines on using the fields on the **NAT Policies** page.

Table 119: 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 on page 232](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)
- [About the Single NAT Policy Page on page 238](#)

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 policies.

3. Complete the configuration according to the guidelines provided in [Table 120 on page 236](#).



NOTE: You can associate only a single device or a device cluster with a site.



WARNING: NAT policy restriction for sites—While you can assign one NAT policy to multiple sites, you cannot assign multiple NAT policies to a single site.

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

A NAT policy with the configuration you provided is created.

[Table 120 on page 236](#) provides guidelines on using the fields on the **Create NAT Policy** page.

Table 120: 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 intent; maximum length is 1024 characters.
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>NOTE: 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>NOTE: 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>

Table 120: Fields on the Create NAT Policy Page (continued)

Field	Description
Sites Applied On	<p>Select the sites on which you want to apply the policy in the Available column and move them to the Selected column by clicking the greater-than icon (>).</p> <p>NOTE: The Available column lists only those sites that do not have a NAT policy associated with them.</p>
Sequence No.	<p>Click Select Policy Sequence. The Select Policy Sequence page appears, displaying all NAT policies. Select the policy you want to reorder and select Move Policy Up or Move Policy Down to reorder your NAT policy among the existing policies.</p>

Related Documentation

- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Editing and Deleting NAT Policies on page 237](#)
- [About the Single NAT Policy Page on page 238](#)
- [Creating NAT Policy Rules on page 240](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)

Editing and Deleting NAT Policies

You can edit or delete a NAT policy from the **NAT Policies** page.

- [Editing NAT Policies on page 237](#)
- [Deleting NAT Policies on page 238](#)

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 235.
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 on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)

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 240](#).
- 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 246](#).

- Deploy a NAT rule. See [“Deploying NAT Policy Rules” on page 247](#).
- Search for a specific NAT rule. See [“Searching for Text in an Object Data Table” on page 18](#).
- Show or hide columns. Click the **Show Hide Columns** icon in the top right corner of the page.

Field Descriptions

[Table 121 on page 239](#) provides information on the fields in the NAT rules contained within this NAT policy.

Table 121: 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 247](#).

Related Documentation

- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)
- [Creating NAT Policy Rules on page 240](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [Deploying NAT Policy Rules on page 247](#)

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 122 on page 241](#).
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 122 on page 241](#) provides guidelines on using the fields on the **Single NAT Policy** page.

Table 122: 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"> • The possible endpoints for source for a source NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Protocols • Ports • The possible endpoints for source for a destination NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Protocols • The possible endpoints for source for a static NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Ports <p>You can also select a source endpoint by using the methods described in “Selecting NAT Source” on page 248.</p>

Table 122: 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"> • The possible endpoints for destination for a source NAT rule are: <ul style="list-style-type: none"> • Addresses • Routing instances, interfaces, or zones • Services • Ports • The possible endpoints for destination for a destination NAT rule are: <ul style="list-style-type: none"> • Addresses • Services • Ports • The possible endpoints for destination for a static NAT rule are: <ul style="list-style-type: none"> • Addresses • Ports <p>You can select a destination endpoint by using the methods described in “Selecting NAT Destination” on page 252.</p> <p>NOTE: 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>[Any.Address] --> [Wan.IP] :: [Dest-Pool-1]</p> <p>Therefore, the recommendation in such cases is to use a destination NAT rule with destination field as [Address + Port]. For example:</p> <p>[Any.Address] --> [Wan.IP + Port] :: [Dest-Pool-1]</p>

Translation

Table 122: 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"> • None—No translation is required for the incoming traffic. • Interface—Performs interface-based translations on the source or destination packet. • Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the Select Pool field to choose the translation pool. <p>You can also create a new pool by clicking Add new pool. See “Creating NAT Pools” on page 257.</p> <p>Chose one among the following translation types for a static NAT rule:</p> <ul style="list-style-type: none"> • Address—Performs address-based translations on the source or destination packet. Click on the add icon (+) in the Select Address field to choose the translation address. <p>You can also create a new address by clicking Add new address. See “Creating Addresses or Address Groups” on page 287.</p> <p>NOTE: 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 Advanced Settings page. For more information on Advanced Settings, see Table 124 on page 245.</p> <ul style="list-style-type: none"> • Corresponding IPv4—Uses the corresponding IPv4 address to perform translations on the source or destination packet. <p>Chose one among the following translation types for a destination NAT rule:</p> <ul style="list-style-type: none"> • None—No translation is required for the incoming traffic. • Pool—Performs pool-based translations on the source or destination packet. Click on the add icon (+) in the Select Pool field to choose the translation pool. <p>You can also create a new pool by clicking Add new pool. See “Creating NAT Pools” on page 257.</p> <p>NOTE: 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>Address - IP1</p> <p>Site - the site hosting the webserver</p> <p>Routing instance - natVR_HR</p>
Advanced Settings (Optional)	<p>Click Configure to configure advance settings for a source or static NAT rule. For more information about advanced settings for the translation types Interface and Pool for a source NAT rule, see Table 123 on page 244. For more information about advanced settings for the translation types Interface and Pool for a static NAT rule, see Table 124 on page 245</p>
Details	
Name	<p>Enter a unique string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 255 characters.</p>

Table 122: Fields on the Single NAT Policy Page for Creating NAT Rules (continued)

Field	Description
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"> To create an address, click the add icon (+) and select Address. See “Creating Addresses or Address Groups” on page 287 to configure the parameters of the address. To create a service, click the add icon (+) and select Service. See “Creating Services and Service Groups” on page 292 to configure the parameters of the service. <p>To edit the configured parameters of an address or service, hover over it and click on the edit icon (pencil symbol).</p>

[Table 123 on page 244](#) provides guidelines on using the fields on the **Advanced Settings** page for a source NAT rule.

Table 123: 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>NOTE: 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>
Persistent NAT Type	<p>Configure persistent NAT mappings.</p> <ul style="list-style-type: none"> 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. 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. 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.
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>

Table 123: Fields on the Advanced Settings Page for Source NAT Rule (continued)

Field	Description
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	Select an address from the available list.
Pool Address	Displays the NAT pool address.
Host Address Base	Displays the base address of the original source IP address range. The host address base is used for IP address shifting.
Port Translation	Displays whether port translation is enabled or disabled for this NAT rule.
Overflow Pool Type	Displays the source pool to be used when the current address pool is exhausted.
Overflow Pool Name	Displays the name of the overflow pool.
Mapped Port Type	<p>Specify the type of port mapping:</p> <ul style="list-style-type: none"> Port—Enter a value for Port, ranging from 0 through 65,535. Range—Enter the port range values in the Start and End fields, ranging from 0 through 65,535.

[Table 124 on page 245](#) provides guidelines on using the fields on the **Advanced Settings** page for a static NAT rule.

Table 124: 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"> Port—Enter a value for Port, ranging from 0 through 65,535. Range—Enter the port range values in the Start and End fields, ranging from 0 through 65,535.
Routing Instance	Select the routing instance for the static NAT rule.

Related Documentation

- [About the Single NAT Policy Page on page 238](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [Deploying NAT Policy Rules on page 247](#)
- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)

- [Editing and Deleting NAT Policies on page 237](#)

Editing, Cloning, and Deleting NAT Policy Rules

You can edit, clone, or delete a NAT policy rule from the **NAT Policy** page.

- [Editing NAT Policy Rules on page 246](#)
- [Cloning NAT Policy Rules on page 246](#)
- [Deleting NAT Policy Rules on page 247](#)

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 240.

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 on page 238](#)
- [Creating NAT Policy Rules on page 240](#)
- [Deploying NAT Policy Rules on page 247](#)
- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)

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 312](#).

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 on page 238](#)
- [Creating NAT Policy Rules on page 240](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)

Selecting NAT Source

The following procedures provides various methods using which you can choose an endpoint as a NAT source:

- [Adding an Endpoint as NAT Source on page 248](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box on page 249](#)
- [Selecting NAT Source Using Abbreviations on page 249](#)
- [Selecting a NAT Source from the End Points Panel on page 250](#)
- [Creating and Selecting a NAT Source from the End Points Panel on page 250](#)
- [Creating Addresses from Source Field on page 251](#)

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 125 on page 249](#). These are the default mappings provided by Cloud CPE Solution. You may change these interface mappings based on your requirements, see “[Configuring a Single Site](#)” on page 349.

Table 125: 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 248](#).

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 250](#).

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 287](#).
- To create a new service, see [“Creating Services and Service Groups” on page 292](#).
- To create a new NAT pool, see [“Creating NAT Pools” on page 257](#).

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 287](#).
 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 on page 252](#)
- [Creating NAT Policy Rules on page 240](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [Deploying NAT Policy Rules on page 247](#)
- [About the Single NAT Policy Page on page 238](#)
- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)

Selecting NAT Destination

The following procedures provides various methods that you can use to choose an endpoint as a NAT destination:

- [Adding an Endpoint as NAT Destination on page 252](#)
- [Selecting Interfaces when GWR Resides Inside an NFX Box on page 252](#)
- [Selecting NAT Destination Using Abbreviations on page 253](#)
- [Selecting a NAT Destination from the End Points Panel on page 253](#)
- [Creating and Selecting a NAT Destination from the End Points Panel on page 254](#)
- [Creating Addresses from Destination Field on page 254](#)
- [Creating Services from Destination Field on page 255](#)

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 126 on page 252](#). These are the default mappings provided by Cloud CPE Solution. You may change these interface mappings based on your requirements, see “[Configuring a Single Site](#)” on page 349.

Table 126: 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

Table 126: NFX and GWR Interface Mapping (continued)

NFX Physical Interface	GWR Virtual Interface
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 **route**.

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 252](#).

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 254](#).

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 287](#).
- To create a new service, see [“Creating Services and Service Groups” on page 292](#).

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 287](#).

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 292](#).

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

- [About the Single NAT Policy Page on page 238](#)
- [Editing, Cloning, and Deleting NAT Policy Rules on page 246](#)
- [Creating NAT Policy Rules on page 240](#)
- [Deploying NAT Policy Rules on page 247](#)
- [NAT Policies Overview on page 232](#)
- [About the NAT Policies Page on page 234](#)
- [Creating NAT Policies on page 235](#)
- [Editing and Deleting NAT Policies on page 237](#)

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**
- [NAT Policies Overview on page 232](#)
 - [About the NAT Pools Page on page 256](#)
 - [Creating NAT Pools on page 257](#)
 - [Editing, Cloning, and Deleting NAT Pools on page 259](#)

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 257](#).
- Modify, clone, or delete a NAT pool. See [“Editing, Cloning, and Deleting NAT Pools” on page 259](#).
- 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**. See [“Viewing Object Details” on page 17](#).
- Search for a specific NAT pool. See [“Searching for Text in an Object Data Table” on page 18](#).
- Show or hide columns. Click the **Show Hide Columns** icon at the top right corner of the page.

[Table 127 on page 256](#) provides description of the fields on the **NAT Pools** page.

Table 127: 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 Source or Destination .

- Related Documentation**
- [NAT Pools Overview on page 255](#)
 - [Creating NAT Pools on page 257](#)
 - [Editing, Cloning, and Deleting NAT Pools on page 259](#)

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 128 on page 257](#).

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 128 on page 257](#) provides guidelines on using the fields on the **Create NAT Pool** page.

Table 128: Fields on the Create NAT Pool Page

Field	Description
General Information	
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"> • Source • Destination
Pool Address	Select a NAT pool address or click Add new address to create a new NAT pool address.
Routing Instance	

Table 128: Fields on the Create NAT Pool Page (continued)

Field	Description
Site	<p>Select the site to which the NAT pool is applicable.</p> <p>NOTE: In a hub and spoke topology, both hub and spoke sites are listed in the Site drop-down. Ensure that you select only a spoke site, when you are creating a destination NAT pool.</p>
Routing Instance	Select the required routing instance from the list of available routing instances for the selected site.
Advanced	
Host Address Base	Enter the base address of the original source IP address range. The Host Address Base is used for IP address shifting.
Translation	<p>Select the translation type for the incoming traffic:</p> <ul style="list-style-type: none"> • No Translation—There is no translation required for the incoming traffic. • Port/Range—Set the global default single port range for source NAT pools with port translation. • Overload—Multiple source addresses are translated to pool addresses. If you set Overload as the translation type, the value of the Pool Address field cannot be an IP range or subnet, but it will be a single address.
Address Pooling	<p>Select a NAT address pooling behavior:</p> <ul style="list-style-type: none"> • 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. • Non-Paired—Use this option for applications that can be assigned IP addresses in a round-robin fashion.
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 128: Fields on the Create NAT Pool Page (continued)

Field	Description
Overflow Pool Type	<p>Select a source pool to use when the current address pool is exhausted.</p> <ul style="list-style-type: none"> Interface—Allow the egress interface IP address to support overflow. Pool—Name of the source address pool. <ul style="list-style-type: none"> 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.)

- Related Documentation**
- [NAT Pools Overview on page 255](#)
 - [About the NAT Pools Page on page 256](#)
 - [Editing, Cloning, and Deleting NAT Pools on page 259](#)

Editing, Cloning, and Deleting NAT Pools

- [Editing NAT Pools on page 259](#)
- [Cloning NAT Pools on page 260](#)
- [Deleting NAT Pools on page 260](#)

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 257](#).

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 on page 255](#)
- [About the NAT Pools Page on page 256](#)
- [Creating NAT Pools on page 257](#)

CHAPTER 17

Managing SSL Proxies

- [SSL Forward Proxy Overview on page 261](#)
- [About the SSL Proxy Policy Page on page 266](#)
- [Creating SSL Proxy Policy Intents on page 267](#)
- [Editing, Cloning, and Deleting SSL Proxy Policy Intents on page 270](#)
- [Understanding How SSL Proxy Policy Intents Are Applied on page 272](#)
- [About the SSL Proxy Profiles Page on page 274](#)
- [Creating SSL Forward Proxy Profiles on page 276](#)
- [Editing, Cloning, and Deleting SSL Forward Proxy Profiles on page 280](#)
- [Configuring and Deploying an SSL Forward Proxy Policy on page 282](#)

SSL Forward Proxy Overview

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:

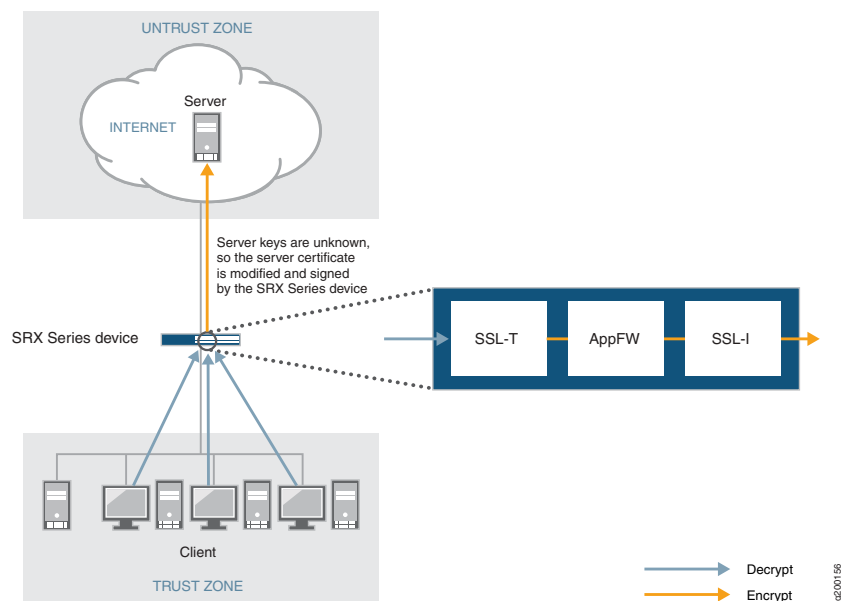
- For the server, SSL forward proxy acts as a client—Because SSL forward proxy generates the shared pre-master key, it determines the keys to encrypt and decrypt.
- For the client, SSL forward proxy acts as a server—SSL forward proxy first authenticates the original server and replaces the public key 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 3 on page 262 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 3: SSL Forward Proxy on an Encrypted Payload



This topic has the following sections:

- [Supported Ciphers in Proxy Mode on page 263](#)
- [Server Authentication on page 263](#)
- [Root CA on page 264](#)
- [Trusted CA List on page 264](#)
- [Session Resumption on page 265](#)
- [SSL Proxy Logs on page 265](#)

Supported Ciphers in Proxy Mode

An SSL cipher comprises encryption ciphers, authentication method, and compression. [Table 129 on page 263](#) displays a list of supported ciphers. NULL ciphers are excluded.

The following SSL protocols are supported:

- SSLv3
- TLS1

Table 129: 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
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 130 on page 265](#).

Table 130: 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 whitelisted.
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 131 on page 265](#) identifies the source of the message. Other fields are descriptively labeled.

Table 131: 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.

Table 131: SSL Proxy Log Prefixes (continued)

Prefix	Description
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 on page 266](#)
 - [About the SSL Proxy Profiles Page on page 274](#)
 - [Certificates Overview on page 403](#)

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 267](#).
- Edit, clone, or delete SSL proxy policy intents—See [“Editing, Cloning, and Deleting SSL Proxy Policy Intents” on page 270](#).
- 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 312](#).

Field Descriptions

[Table 132 on page 267](#) describes the fields on SSL Proxy Policy page.

Table 132: 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

- [SSL Forward Proxy Overview on page 261](#)

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 133 on page 268](#)
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 redeploy 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 133: 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 a combination of these.</p> <p>NOTE: A source IP address value of Any 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"> Click the add icon (+) and select the endpoints from the list of previously configured endpoints. Filter the endpoints by entering a search term or one or more predefined keywords in the Source field and select one or more endpoints. Table 134 on page 270 displays the list of predefined keywords. Click the View more results link to view additional configured endpoints. The list of endpoints is displayed in the End Points panel on the right. Do one of the following: <ul style="list-style-type: none"> To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint. To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the End Points panel, and select Source. Filter the endpoints by entering a search term or one or more predefined keywords in the End Points field and select one or more endpoints. Table 134 on page 270 displays the list of predefined keywords. <p>NOTE: You can also create endpoints by clicking the add icon (+) in the End Points panel. Table 135 on page 270 displays the endpoints that can be created.</p>

Table 133: Create SSL Proxy Policy Intent Settings (continued)

Setting	Guideline
Destination	<p>A destination endpoint can be an IP address, an IP address group, a site, a site group, or a department, or a combination of these.</p> <p>NOTE: A destination IP address value of Any signifies traffic going to the Internet (any address). Traffic within sites (internal traffic) is not covered by the destination IP address value of Any.</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"> Click the add icon (+) and select the endpoints from the list of previously configured endpoints. Filter the endpoints by entering a search term or one or more predefined keywords in the Destination field and select one or more endpoints. Table 134 on page 270 displays the list of predefined keywords. Click the View more results link to view additional configured endpoints. The list of endpoints is displayed in the End Points panel on the right. Do one of the following: <ul style="list-style-type: none"> To add one endpoint at a time, select an endpoint and click the check mark icon (✓) that appears when you hover over the endpoint. To add multiple endpoints, select one or more endpoints that you want to add, click the check mark icon (✓) at the top of the End Points panel, and select Destination. Filter the endpoints by entering a search term or one or more predefined keywords in the End Points field and select one or more endpoints. Table 134 on page 270 displays the list of predefined keywords. <p>NOTE: You can also create endpoints by clicking the add icon (+) in the End Points panel. Table 135 on page 270 displays the endpoints that can be created.</p>
SSL Proxy Profile	<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"> Click the add icon (+) and select the SSL proxy profile from the list of previously configured profiles. Filter the profiles by entering a search term in the SSL Proxy Profile field and select a profile. Create a SSL proxy profile—Click the Add New Profile link. The Create SSL Proxy Profiles page appears. See “Creating SSL Forward Proxy Profiles” on page 276. <p>NOTE: You can also create profiles by clicking the add icon (+) in the End Points panel and selecting SSL Proxy Profiles.</p> <ul style="list-style-type: none"> Click the View more results link to view additional configured profiles. The list of SSL proxy profiles is displayed in the End Points panel on the right. To add a profile, select it and click the check mark icon (✓) that appears when you hover over the profile.
Details	<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 134: Keywords for Filtering Endpoints

Endpoint	Keyword	Applicable to
Address or Address Group	addr or ADDR	Source Destination
Site	site or SITE	Source Destination
Site Group	stgp or STGP	Source Destination
Department	dept or DEPT	Source Destination

Table 135: Creating Endpoints

Endpoint	Procedure
Address or Address Group	Click the add icon (+) and select Address . The Create Addresses page appears. See "Creating Addresses or Address Groups" on page 287 .
Site Group	Click the add icon (+) and select Site Group . The Create Site Group page appears. See "Creating Site Groups" on page 366 .
Department	Click the add icon (+) and select Department . The Create Department page appears. See "Creating a Department" on page 305 .

Related Documentation

- [SSL Forward Proxy Overview on page 261](#)

Editing, Cloning, and Deleting SSL Proxy Policy Intents

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 on page 271](#)
- [Cloning SSL Proxy Policy Intents on page 271](#)
- [Deleting SSL Proxy Policy Intents on page 272](#)

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 267](#).

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 267](#).

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 on page 266](#)

Understanding How SSL Proxy Policy Intents Are Applied

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 on page 273](#)
- [Example 2: Firewall Policy Intent and SSL Proxy Policy Intent Do Not Match on page 273](#)
- [Example 3: Applying SSL Proxy Policy Intents on Internal \(Site-to-Site\) Traffic on page 274](#)

Example 1: Firewall Policy Intent and SSL Proxy Policy Intent Match

[Table 136 on page 273](#) 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 136: (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 137 on page 274](#) 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 137: (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 138 on page 274 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 138: (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 on page 261](#)
- [Configuring and Deploying an SSL Forward Proxy Policy on page 282](#)

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 276.
- Edit, clone, or delete an SSL proxy profile—See [“Editing, Cloning, and Deleting SSL Forward Proxy Profiles”](#) on page 280.
- 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 140 on page 275](#) 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 139 on page 275](#) describes the fields on the SSL Proxy Profiles page.

Table 139: Fields on the SSL Proxy Profiles Page

Field	Description
Name	Name of the SSL proxy profile.
Preferred Cipher	Preferred cipher associated with the profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform encryption and decryption functions.
Exempted Address	Addresses that can are exempted from SSL forward proxy processing.
Description	Description of the SSL proxy profile.
Root Certificate	Root certificate associated with the SSL proxy profile.

Table 140: View SSL Forward Proxy Profile Details Page Fields

Field	Description
General Information	
Name	Name of the SSL proxy profile.
Description	Description of the SSL proxy profile.
Preferred Cipher	Preferred cipher associated with the proxy profile.
Custom Ciphers	The set of ciphers, if the preferred cipher is Custom , which the SSH server uses to perform encryption and decryption functions.
Flow Trace Enabled	Indicates whether flow tracing is enabled or disabled.

Table 140: View SSL Forward Proxy Profile Details Page Fields (continued)

Field	Description
Certificates	Displays the root certificate and the trusted certificate authorities associated with the root certificate.
Exempted Address	Addresses that can are exempted from SSL forward proxy processing.
Exempted URL Categories	URL categories that are exempted from SSL forward proxy processing.
Actions	
Ignore	Indicates whether server authentication failure is ignored (Enabled) or not (Disabled).
Session Resumption	Indicates whether session information is cached to enable session resumption (Enabled) or not (Disabled).
Logging	If logging is enabled, indicates the type of events that are logged.
Renegotiation	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 on page 266](#)

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 141 on page 277](#).



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 141: Creating SSL Forward Proxy Profile Settings

Setting	Guideline
General Information	
Name	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.
Description	Enter a description for the profile. The maximum length is 255 characters.
Preferred Cipher	<div>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:</div> <ul style="list-style-type: none">• None (Default)—Do not specify a preferred cipher.• Medium—Use ciphers with key strength of 128 bits or greater.• Strong—Use ciphers with key strength of 168 bits or greater.• Weak—Use ciphers with key strength of 40 bits or greater.• Custom—Configure a custom cipher suite.

Table 141: Creating SSL Forward Proxy Profile Settings (continued)

Setting	Guideline
Custom Ciphers	<p>If you specified Custom 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"> • rsa-with-RC4-128-md5—RSA, 128-bit RC4, MD5 hash • rsa-with-RC4-128-sha—RSA, 128-bit RC4, SHA hash • rsa-with-des-cbc-sha—RSA, DES/CBC, SHA hash • rsa-with-3DES-ede-cbc-sha—RSA, 3DES EDE/CBC, SHA hash • rsa-with-aes-128-cbc-sha—RSA, 128-bit AES/CBC, SHA hash • rsa-with-aes-256-cbc-sha—RSA, 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, 256 bit AES/GCM, SHA384 hash • rsa-with-aes-256-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • rsa-with-aes-128-gcm-sha256—RSA, 128 bit AES/GCM, SHA256 hash • rsa-with-aes-128-cbc-sha256—RSA, 256 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-256-gcm-sha384—ECDHE, RSA, 256 bit AES/GCM, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha384—ECDHE, RSA, 256 bit AES/CBC, SHA384 hash • ecdhe-rsa-with-aes-256-cbc-sha—ECDHE, RSA, 256 bit AES/CBC, SHA hash • ecdhe-rsa-with-aes-3des-ede-cbc-sha—ECDHE, RSA, 3DES, EDE/CBC, SHA hash • ecdhe-rsa-with-aes-128-gcm-sha256—ECDHE, RSA, 128 bit AES/GCM, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha256—ECDHE, RSA, 128 bit AES/CBC, SHA256 hash • ecdhe-rsa-with-aes-128-cbc-sha—ECDHE, RSA, 128 bit AES/CBC, SHA hash
Flow Trace	Select this option to enable flow tracing to enable the troubleshooting of policy-related issues.
Root Certificate	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.
Trusted Certificate Authorities	<p>Choose whether you want to add all trusted certificates present on the device (All) or select specific trusted certificates. Before establishing a secure connection, the SSL proxy checks CA certificates to verify signatures on server certificates.</p> <p>NOTE:</p> <ul style="list-style-type: none"> • 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. • 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.
Actions	

Table 141: 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 Available column and click the forward arrow to confirm your selection. The selected addresses are then displayed in the Selected column. These addresses are used to create whitelists 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 whitelists.</p> <p>NOTE: You can also add addresses by clicking Add New Address. The Create Addresses page appears. See “Creating Addresses or Address Groups” on page 287.</p>
Exempted URL Categories	<p>Select the previously defined URL categories to create whitelists 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>
Logging	<p>Select one or more events to be logged. You can choose to log all events, warnings, general information, errors, or different sessions (whitelisted, allowed, dropped, or ignored). Logging is disabled by default.</p>
Renegotiation	<p>Select one of the following options if a change in SSL parameters requires renegotiation:</p> <ul style="list-style-type: none"> • None (default)—Indicates that renegotiation is not required. • Allow—Allow secure and nonsecure renegotiation. • Allow-secure—Allow secure negotiation only. • Drop—Drop session on renegotiation request. <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"> • Cipher keys need to be refreshed after a prolonged SSL session. • Stronger ciphers need to be applied for a more secure connection.

- Related Documentation**
- [About the SSL Proxy Policy Page on page 266](#)

Editing, Cloning, and Deleting SSL Forward Proxy Profiles

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 on page 280](#)
- [Cloning SSL Forward Proxy Profiles on page 280](#)
- [Deleting SSL Forward Proxy Profiles on page 281](#)

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 on page 276](#)
- [About the SSL Proxy Profiles Page on page 274](#)

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 405](#).
4. (Optional) Install the imported certificate on one or more sites (on the Install Certificate page); see ["Installing and Uninstalling Certificates" on page 407](#).
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 276](#).



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 267](#).
8. Deploy the SSL proxy policy; see ["Deploying Policies" on page 312](#).



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 on page 261](#)
- [Understanding How SSL Proxy Policy Intents Are Applied on page 272](#)

CHAPTER 18

Managing Shared Objects

- [Addresses and Address Groups Overview on page 285](#)
- [About the Addresses Page on page 286](#)
- [Creating Addresses or Address Groups on page 287](#)
- [Editing, Cloning, and Deleting Addresses and Address Groups on page 289](#)
- [Services and Service Groups Overview on page 291](#)
- [About the Services Page on page 291](#)
- [Creating Services and Service Groups on page 292](#)
- [Creating Protocols on page 294](#)
- [Editing and Deleting Protocols on page 297](#)
- [Editing, Cloning, and Deleting Services and Service Groups on page 298](#)
- [Application Signatures Overview on page 300](#)
- [About the Application Signatures Page on page 300](#)
- [Creating Application Signature Groups on page 301](#)
- [Editing, Cloning, and Deleting Application Signature Groups on page 302](#)
- [About the Departments Page on page 304](#)
- [Creating a Department on page 305](#)
- [Modifying a Department on page 306](#)
- [Deleting a Department on page 306](#)

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 on page 286](#)
 - [Creating Addresses or Address Groups on page 287](#)
 - [Editing, Cloning, and Deleting Addresses and Address Groups on page 289](#)

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 287](#).
- Modify, clone, or delete an address or address group. See [“Editing, Cloning, and Deleting Addresses and Address Groups” on page 289](#).
- View the configured parameters of an address or address group. Click the details icon that appears when you hover over the name of an image or select **More > Detailed View**. See [“Viewing Object Details” on page 17](#).
- Show or hide columns about the address or address group. See [“Sorting Objects” on page 17](#).
- Search for an address or address group. See [“Searching for Text in an Object Data Table” on page 18](#).

Field Descriptions

[Table 142 on page 286](#) provides guidelines on using the fields on the Addresses page.

Table 142: 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.

Table 142: Fields on the Addresses Page (continued)

Field	Description
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 on page 285](#)
- [Creating Addresses or Address Groups on page 287](#)
- [Editing, Cloning, and Deleting Addresses and Address Groups on page 289](#)

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 143 on page 287](#) and [Table 144 on page 288](#).
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 143: 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. Table 144 on page 288 describes address group configuration parameters.

Table 143: Fields on the Create Addresses Page (continued)

Field	Description
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.
Type	<p>Select a type of address and fill in the corresponding fields. Available types are:</p> <ul style="list-style-type: none"> • Host <ul style="list-style-type: none"> • Host IP—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 Look up hostname. • Hostname—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 Look up IP address. For example, enter www.company.com and click Look up IP address. Hostname lookup is supported for IPv4 and IPv6 addresses. • Range <ul style="list-style-type: none"> • Start Address—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. • End Address—Enter an ending IPv4 or IPv6 address for the address range. The range is validated after you enter the address. <p>NOTE: 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> • Network <ul style="list-style-type: none"> • Network—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. • Subnet Mask—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. • Wildcard <ul style="list-style-type: none"> • Network—Enter the network IPv4 or IPv6 address. For example: 192.0.2.0 or 2001:db8:4136:e378:8000:63bf:3fff:fdd2. • Wildcard Mask—Enter the wildcard mask for the network range. For example: 0.0.0.255. • DNS Host <ul style="list-style-type: none"> • DNS Name—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.

Table 144: 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. Table 143 on page 287 describes address group configuration parameters.

Table 144: Address Group Settings (continued)

Field	Description
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 Available column to the Selected 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 on page 285](#)
 - [About the Addresses Page on page 286](#)
 - [Editing, Cloning, and Deleting Addresses and Address Groups on page 289](#)

Editing, Cloning, and Deleting Addresses and Address Groups

You can edit, clone, and delete addresses and address groups from the **Addresses** page.

- [Editing Addresses and Address Groups on page 289](#)
- [Cloning Addresses and Address Groups on page 290](#)
- [Deleting Addresses and Address Groups on page 290](#)

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 287](#).
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 a 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 312](#) 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 on page 285](#)
 - [About the Addresses Page on page 286](#)
 - [Creating Addresses or Address Groups on page 287](#)
 - [Viewing Object Details](#)
 - [Sorting Objects](#)
 - [Searching for Text in an Object Data Table](#)

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**
- [About the Services Page on page 291](#)
 - [Creating Services and Service Groups on page 292](#)
 - [Editing, Cloning, and Deleting Services and Service Groups on page 298](#)

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 292](#).
- Modify, clone or delete a service or service group. See [“Editing, Cloning, and Deleting Services and Service Groups” on page 298](#).
- 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” on page 17](#).
- Show or hide columns about the services or service groups. See [“Sorting Objects” on page 17](#).
- Search a specific service or service group. See [“Searching for Text in an Object Data Table” on page 18](#).

Field Descriptions

[Table 145 on page 292](#) provides guidelines on using the fields on the **Services** page.

Table 145: 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 on page 291](#)
- [Creating Services and Service Groups on page 292](#)
- [Editing, Cloning, and Deleting Services and Service Groups on page 298](#)

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 146 on page 293](#).

If you want to configure a service group, see [Table 147 on page 293](#).

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 146 on page 293](#) provides guidelines on using the fields to create a service.

Table 146: Service Settings

Field	Description
Object Type	Select Service or Service Group . If you select Service Group , 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 Protocols table. You can also create a new protocol, or edit existing protocols:</p> <ul style="list-style-type: none"> • To create a new protocol, click on the add icon (+). See "Creating Protocols" on page 294. • To edit an existing protocol, click on the edit icon (pencil symbol). See "Editing and Deleting Protocols" on page 297.

[Table 147 on page 293](#) provides guidelines on using the fields to create a service group.

Table 147: Service Group Settings

Field	Description
Object Type	Select Service or Service Group . If you select Service Group , then the screen changes so you can select the services you want to include in your service group.

Table 147: Service Group Settings (continued)

Field	Description
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.
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 Available column to the Selected 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 on page 291](#)
- [About the Services Page on page 291](#)
- [Editing, Cloning, and Deleting Services and Service Groups on page 298](#)
- [Creating Protocols on page 294](#)
- [Editing and Deleting Protocols on page 297](#)

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 148 on page 295](#) and [Table 149 on page 295](#).
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 148 on page 295 provides guidelines on using the fields to create a protocol.

Table 148: Fields on Create Protocol Page Settings

Field	Description
General Information	
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 Table 149 on page 295 for the other protocol types.
Destination Port	Enter a destination port number for TCP. The range is from 0 to 65,535.
Advanced Settings	
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 149 on page 295 includes the settings and guidelines for the various protocol types.

Table 149: Create Protocol Type Settings

Field	Description
UDP	
Destination Port	Enter a destination port number for UDP. This is a value or value range from 0 through 65,535.
Advanced Settings	
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.
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.
ICMP	
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.

Table 149: Create Protocol Type Settings (continued)

Field	Description
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.
SUN-RPC	
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.
MS-RPC	
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.
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.
ICMPv6	
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 on page 297](#)
 - [About the Services Page on page 291](#)
 - [Creating Services and Service Groups on page 292](#)

Editing and Deleting Protocols

You can edit and delete protocols through the **Services** page.

- [Editing Protocols on page 297](#)
- [Deleting Protocols on page 298](#)

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 294.

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 on page 291](#)
- [About the Services Page on page 291](#)
- [Creating Services and Service Groups on page 292](#)
- [Editing, Cloning, and Deleting Services and Service Groups on page 298](#)
- [Creating Protocols on page 294](#)

Editing, Cloning, and Deleting Services and Service Groups

You can edit, clone, and delete services and service groups from the **Services** page.

- [Editing Services and Service Groups on page 298](#)
- [Cloning Services or Service Groups on page 299](#)
- [Deleting Services and Service Groups on page 299](#)

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 292](#).
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 on page 291](#)
- [About the Services Page on page 291](#)

- [Creating Services and Service Groups on page 292](#)

Application Signatures Overview

Juniper Networks regularly updates the predefined application signature database, making it available to subscribers on the Juniper Networks website. This database includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, and quality-of-service prioritization.

Use the **Application Signatures** page to get an overall, high-level view of your application signature settings. You can filter and sort this information to get a better understanding of what you want to configure.

Related Documentation

- [About the Application Signatures Page on page 300](#)
- [Creating Application Signature Groups on page 301](#)
- [Editing, Cloning, and Deleting Application Signature Groups on page 302](#)
- [Signature Database Overview on page 399](#)

About the Application Signatures Page

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

Use the **Application Signatures** page to view application signatures that are already downloaded and to create, modify, clone, and delete custom application signature groups. The **Application Signatures** page displays the name, object type, category and subcategory, risk associated with, and characteristics of the signature. You can create custom application signature groups with a set of similar signatures for consistent reuse when defining policies.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create an application signature group. See [“Creating Application Signature Groups” on page 301](#).
- Modify, clone, or delete an application signature group. See [“Editing, Cloning, and Deleting Application Signature Groups” on page 302](#).
- View the configured parameters of an application signature or application signature group. Click the details icon that appears when you hover over the name of an image or click **More > Details**. See [“Viewing Object Details” on page 17](#).
- Show or hide columns in the **Application Signatures**. See [“Sorting Objects” on page 17](#).

- Search for a specific application signature or application signature group. See [“Searching for Text in an Object Data Table” on page 18](#).
- 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 150 on page 301](#) provides guidelines on using the fields on the **Application Signatures** page.

Table 150: Fields on the Application Signatures Page

Field	Description
Name	Name of the application signature or application signature group.
Object Type	Signature type—either application signature or application signature group.
Category	UTM category of the application signature. For example, the value of Category can be Messaging, Web, Infrastructure, Remote-Access, Multimedia, and so on.
Subcategory	UTM subcategory of the application signature. For example, the value of Subcategory can be Wiki, File-Sharing, Multimedia, Social-Networking, News, and so on.
Risk	Level of risk associated with the application signature. For example, the value of Risk can be Low, High, unsafe, and so on.
Characteristic	One or more characteristics of the application signature.
Predefined or Custom	A list of predefined application signatures and application signature groups, and a list of custom application signature groups that you created.

Related Documentation

- [Application Signatures Overview on page 300](#)
- [Creating Application Signature Groups on page 301](#)
- [Editing, Cloning, and Deleting Application Signature Groups on page 302](#)
- [Signature Database Overview on page 399](#)
- [About the Active Database Page on page 400](#)

Creating Application Signature Groups

Application identification supports custom application signatures to detect applications as they pass through the device. When you create custom signature groups, make sure that your signature groups are unique, by providing a unique and relevant name.

To create an application signature group:

1. Select **Configure > Shared Objects > Application Signatures**.
2. Click the add icon (+).
3. Complete the configuration according to the guidelines provided in [Table 151 on page 302](#).
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 151 on page 302](#) provides guidelines on using the fields on the **Create Application Signature Group** page.

Table 151: 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 Add Application Signatures page, select the check boxes next to the signatures you want to add to the group.

**Related
Documentation**

- [Application Signatures Overview on page 300](#)
- [About the Application Signatures Page on page 300](#)
- [Editing, Cloning, and Deleting Application Signature Groups on page 302](#)
- [Signature Database Overview on page 399](#)
- [About the Active Database Page on page 400](#)

Editing, Cloning, and Deleting Application Signature Groups

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

- [Editing Application Signature Groups on page 303](#)
- [Cloning Application Signature Groups on page 303](#)
- [Deleting Application Signature Groups on page 303](#)

Editing Application Signature Groups

To modify the parameters configured for an application signature group:

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

The **Application Signatures** page appears.

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

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

3. Modify the parameters according to the guidelines provided in [“Creating Application Signature Groups” on page 301](#).
4. Click **Save** to save the changes. If you want to discard your changes, click **Cancel** instead.

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

Cloning Application Signature Groups

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

To clone an application signature group:

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

The **Application Signatures** page appears.

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

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

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

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

Deleting Application Signature Groups

To delete an application signature group:

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

The **Application Signatures** page appears.

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

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

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

Related Documentation

- [Application Signatures Overview on page 300](#)
- [About the Application Signatures Page on page 300](#)
- [Creating Application Signature Groups on page 301](#)
- [Signature Database Overview on page 399](#)

About the Departments Page

To access this page, click **Configuration > Network Services > Shared Objects > Departments**.

You can use the Departments page to create, view, edit, 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:

- Create a Department. Click **Configuration > Shared Objects > Departments > Create**. See [“Creating a Department” on page 305](#).
- Edit a Department. Select a department and click **Edit**. See [“Modifying a Department” on page 306](#).
- Delete a department. Select a department and click **Delete**. Before you delete a department, you must reassign all the LAN segments that are assigned to the department. You cannot delete a department that has a LAN segment assigned to it. See [“Deleting a Department” on page 306](#).

Field Descriptions

[Table 152 on page 304](#) shows the descriptions of the fields on the **Departments** page.

Table 152: Fields on the Departments Page

Field	Description
Name	Displays the name of the department.
Site/LAN Segments	Displays the LAN segments that are assigned to the department.

Table 152: Fields on the Departments Page (continued)

Field	Description
VPN	Displays the VPN to which the department is assigned.
Description	Displays a description of the department.

- Related Documentation**
- [Creating a Department on page 305](#)
 - [Modifying a Department on page 306](#)
 - [Deleting a Department on page 306](#)

Creating a Department

You can create new departments from the **Configuration > Shared Objects > Departments** page.

To create a department:

1. Click the add icon (+) on the **Departments** page.

The **Create Department** page appears.

2. Complete the configuration settings according to the guidelines provided in [Table 153 on page 305](#).

Table 153: Fields on the Create Departments Page

Field	Description
Name	Enter a name for the department. Enter a unique string of 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	Select a VPN to which you want to assign the department.

3. Click **OK**.

The new department is displayed on the **Departments** page.

- Related Documentation**
- [About the Departments Page on page 304](#)
 - [Modifying a Department on page 306](#)
 - [Deleting a Department on page 306](#)

Modifying a Department

You can modify a department on the **Configuration > Shared Objects > Departments** page.

To modify a department:

1. Select a department and click the edit icon on the **Departments** page.
The **Edit Department** page appears.
2. Complete the configuration settings according to the guidelines provided in [Table 154 on page 306](#).

Table 154: Fields on the Edit Department Page

Field	Description
Name	Modify the name of the department, as needed.
Description	Modify the description of the department.
VPN	Select a VPN to which you want to assign the department.

3. Click **OK**.

The updated department is displayed on the **Departments** page.

Related Documentation

- [About the Departments Page on page 304](#)
- [Creating a Department on page 305](#)
- [Deleting a Department on page 306](#)

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 if it has policies associated with it or LAN segments assigned to it. Before you delete the department, you must reassign the LAN segments assigned to that department.

To delete a department:

1. Select the department that you want to delete.
2. Click the delete icon (X).
The Delete Department page appears.
3. Click **OK** to confirm deletion.

The department is deleted.

**Related
Documentation**

- [About the Departments Page on page 304](#)
- [Creating a Department on page 305](#)
- [Modifying a Department on page 306](#)

CHAPTER 19

Managing Deployments

- [Deploying Policies Overview on page 309](#)
- [About the Deployments Page on page 310](#)
- [Using the Deployment Icon to Deploy Policies on page 311](#)
- [Deploying Policies on page 312](#)

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 311](#).



NOTE: The deployment icon is highlighted in orange if there are undeployed configurations.

- Use the **Deployments** page. See [“About the Deployments Page” on page 310](#).
- Select a firewall, NAT or SD-WAN policy from its respective landing pages and click **Deploy**. For more information, see [“Deploying Policies” on page 312](#).

Related Documentation

- [Using the Deployment Icon to Deploy Policies on page 311](#)
- [About the Deployments Page on page 310](#)
- [Deploying Policies on page 312](#)

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 312](#).

Field Descriptions

[Table 155 on page 310](#) provides guidelines on using the fields on the **Deployments** page.

Table 155: Fields on the Deployments Page

Field	Description
Awaiting Deployment	<p>The Awaiting Deployment 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"> • Name—Name of the policy that needs to be deployed. • Deployment Type—Type of the policy that needs to be deployed. • Summary—Description of the policy. • Owner—The tenant who has created the policy. • Last updated—The last time the policy was updated. <p>If you want to deploy a policy, select the policy and click Deploy. The policy is deployed and will no longer appear in the Awaiting Deployment tab.</p> <p>If you want to refresh the Awaiting Deployment tab, click the refresh icon provided below the details table.</p>

Table 155: Fields on the Deployments Page (continued)

Field	Description
Scheduled	<p>The Scheduled 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"> • Name—Name of the policy. • Deployment Type—Type of the policy that needs to be deployed. • Summary—Description of the policy. • Schedule—The date and time at which the policy is scheduled to be deployed. • Status—Displays whether the scheduled policy has been deployed or not. • Next Run—Date and time when the scheduled deployments will be run. <p>If you want to deploy a scheduled policy immediately, select the policy and click Deploy Now. If you want to modify the deployment schedule of a policy, select the policy and click the edit icon (pencil icon). The Deploy page appears displaying the current scheduling information. See “Deploying Policies” on page 312, to update the schedule.</p>
History	<p>The History 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"> • Name—Name of the deployed policy. • Deployment Type—Type of the deployed policy. • Summary—Description of the policy. • Status—Displays the status of the deployed policy. • Job Details—Details of the job. • Deployed On—Date and time the policy was deployed. <p>If you want to redeploy a policy, select the policy and click Re-Deploy. The policy is redeployed and the History tab details changes to reflect this information.</p>

- Related Documentation**
- [Deploying Policies Overview on page 309](#)
 - [Using the Deployment Icon to Deploy Policies on page 311](#)
 - [Deploying Policies on page 312](#)

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 156 on page 312](#).

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 312](#).

[Table 156 on page 312](#) provides guidelines on using the fields on the deployment panel.

Table 156: Fields on the Deployment Panel

Field	Description
Awaiting Deployment	The Awaiting Deployment tab displays all the policies that are awaiting deployment.
In Progress	The In Progress tab displays all the policies that are currently being deployed.

- Related Documentation**
- [Deploying Policies Overview on page 309](#)
 - [About the Deployments Page on page 310](#)
 - [Deploying Policies on page 312](#)

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 311](#).



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 157 on page 313](#).
3. Click **Deploy**.

[Table 157 on page 313](#) provides guidelines on using the fields on the **Deploy** page.

Table 157: Fields on the Deploy Page

Field	Description
Summary	
Policies	The summary of the policy that is to be deployed.
Choose Deployment Time	
Type	<ul style="list-style-type: none">• Select Run now if you want to deploy the policy immediately.• Select Schedule at a later time if you want to schedule the deployment for a later date and time.

- Related Documentation**
- [Deploying Policies Overview on page 309](#)
 - [Using the Deployment Icon to Deploy Policies on page 311](#)
 - [About the Deployments Page on page 310](#)

PART 6

Managing Sites and Site Groups

- [Managing Sites on page 317](#)
- [Managing Site Groups on page 365](#)

CHAPTER 20

Managing Sites

- [About the Sites Page on page 317](#)
- [Local Breakout Overview on page 319](#)
- [Multihoming Overview on page 320](#)
- [Device Redundancy Support Overview on page 321](#)
- [Creating Spoke Sites for Hybrid WAN Deployment on page 323](#)
- [Creating Local Service Edge Sites for Hybrid WAN Deployment on page 325](#)
- [Creating Regional Service Edge Sites for Hybrid WAN Deployment on page 327](#)
- [Creating On-Premise Hub Sites for SD-WAN Deployment on page 329](#)
- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)
- [Creating Cloud Hub Sites for SD-WAN Deployment on page 336](#)
- [Creating Cloud Spoke Sites for SD-WAN Deployment on page 338](#)
- [Provisioning a Cloud Spoke Site in AWS VPC on page 343](#)
- [Importing Multiple Sites on page 347](#)
- [Managing a Single Site on page 348](#)
- [Configuring a Single Site on page 349](#)
- [Managing LAN Segments on a Tenant Site on page 352](#)
- [Activating a CPE Device on page 355](#)
- [Activating Dual CPE Devices \(Device Redundancy\) on page 358](#)
- [Viewing the History of Tenant Device Activation Logs on page 360](#)
- [Configuring VRFs and PNE Details for a Site in a Centralized Deployment on page 362](#)

About the Sites Page

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

You can use the **Sites** page to view existing sites and to create on-premise sites and cloud sites. 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:

- View information about a site. Click the details icon that appears when you hover over the name of a site or click **More > Detailed View**. See [“Viewing Object Details” on page 17](#).
- Click on the site name to view the site details and to manage the site configurations for a single site. See [“Managing a Single Site” on page 348](#).
- Configure a site by uploading a JSON file. . See [“Importing Multiple Sites” on page 347](#).
- View device activation logs. Click **Device Activation Logs**. See [“Viewing the History of Tenant Device Activation Logs” on page 360](#).
- Create the following sites for a Hybrid WAN topology:
 - Create a spoke site. See [“Creating Spoke Sites for Hybrid WAN Deployment” on page 323](#).
 - Create a local service edge site. See [“Creating Local Service Edge Sites for Hybrid WAN Deployment” on page 325](#).
 - Create a regional service edge site. See [“Creating Regional Service Edge Sites for Hybrid WAN Deployment” on page 327](#).
- Create the following sites for an SD-WAN topology:
 - Create on-premise hub site. See [“Creating On-Premise Hub Sites for SD-WAN Deployment” on page 329](#).
 - Create on-premise spoke site. See [“Creating On-Premise Spoke Sites for SD-WAN Deployment” on page 331](#).
 - Create a cloud hub site. See [“Creating Cloud Hub Sites for SD-WAN Deployment” on page 336](#).
 - Create a cloud spoke site. See [“Creating Cloud Spoke Sites for SD-WAN Deployment” on page 338](#).
- Delete a site. Select a site and click the delete icon (X).
- Configure a site. Select a site and click **Configure Site**. See [“Configuring a Single Site” on page 349](#).

Field Descriptions

[Table 158 on page 318](#) describes the fields on the **Sites** page.

Table 158: Fields on the Sites Page

Field	Description
Site Name	Displays the name of the tenant site.
Location	Displays the location of the tenant site.

Table 158: Fields on the Sites Page (continued)

Field	Description
Connected To	Displays the point of presence (POP) that the site is connected to.
State	View the current status of the tenant site. The possible statuses are Active , Provisioned , and Failed .
Device Status	Displays the device status. The status indicates whether or not a device is provisioned for the site.
Role	Indicates whether the site is a hub site or a spoke site.
Active Services	Displays the number of active services configured for the site.
Device Serial Number	Displays the serial number of the device that is provisioned for the site.
Local Breakout	Indicates whether local breakout is enabled or disabled on the site.
Auto-NAT	Indicates whether Autocreate Source NAT Rule is enabled or disabled on the site.

- Related Documentation**
- [Local Breakout Overview on page 319](#)
 - [Creating Cloud Hub Sites for SD-WAN Deployment on page 336](#)
 - [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)

Local Breakout Overview

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

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

You can create a source Network Address Translation (NAT) rule while enabling local breakout on a spoke site. The source NAT rule is interface-based and is implicitly defined and applied to the site. This automatically created source NAT rule is not visible on the **NAT Policies** page. The automatically created source NAT rule has the least priority

among rules and can be overridden by a user-created NAT policy. The automatically created source NAT rule can be enabled and disabled only from the **Configuring a Site** page. For an on-premise hub site, the option for automatic creation of source NAT rule is not available on the **Configuring a Site** page, and you need to create a source NAT rule.

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

Applications are classified into the following categories:

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

**Related
Documentation**

- [SLA Profiles and SD-WAN Policies Overview on page 217](#)
- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)
- [Configuring a Single Site on page 349](#)
- [Creating SLA Profiles on page 227](#)

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.

Related •
Documentation

Device Redundancy Support Overview

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



NOTE: You must use the same device model for both primary and secondary devices and the devices must have the same version of Junos OS installed.

The following SD-WAN features are not supported for device redundancy:

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



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

Prerequisites for SRX Series Devices

The prerequisites to configure an SD-WAN site with dual CPE SRX Series devices are as follows:

- For SRX Series, you need to form the cluster manually by connecting two SRX Series devices together using a pair of the same type of Ethernet connections. To create an SRX cluster, see [Chassis Cluster Feature Guide for SRX Series Devices](#).
- Log in to any one of the SRX Series devices, copy the **Stage-1** configuration from the **Sites** page and paste it into the console screen and commit the configuration.

Supported Connection Plans

The following connection plans are supported for device redundancy:

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

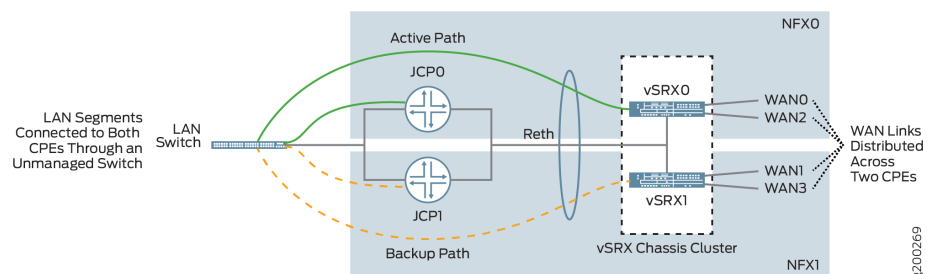
Create and Configure an SD-WAN Site

You can create and configure an SD-WAN site with dual CPE devices and the two devices back up each other, with one node acting as the primary device and the other as the secondary device. The workflow to add and configure a site with dual CPE devices is similar to the single CPE device. For more information about creating and configuring a site with dual CPE devices, see “[Creating On-Premise Spoke Sites for SD-WAN Deployment](#)” on page 331 and “[Configuring a Single Site](#)” on page 349.

Dual CPE Devices Logical Topology for NFX Network Services Platform

Figure 4 on page 322 shows the logical topology of the NFX Series dual CPE devices.

Figure 4: Dual CPE Device Topology - NFX Network Services Platform



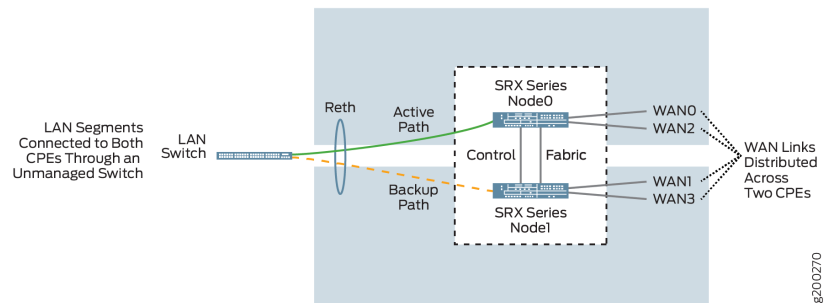
You can form a cluster using two NFX Series devices. The front panel ports of the NFX Series devices are used to interconnect two NFX Series devices and to carry the control and fabric interconnect traffic between the two NFX250 devices.

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 5 on page 323 shows the logical topology of the SRX Series dual CPE devices.

Figure 5: Dual CPE Device Topology - SRX Series Devices



You can form a cluster using two SRX devices. A chassis cluster is formed between these nodes and performs as a single logical router. On the LAN, the active/backup mechanism is used and if the primary device fails, the secondary device takes over traffic processing. On the WAN, the active/active mechanism is used and all four WAN links are active and distributed across two NFX Series device.

Related Documentation

- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)
- [Configuring a Single Site on page 349](#)
- [Activating Dual CPE Devices \(Device Redundancy\) on page 358](#)

Creating Spoke Sites for Hybrid WAN Deployment

You create a spoke site from the **Sites** page. This page describes how to create a spoke site for a tenant in hybrid WAN deployment.

To create a cloud site:

1. Select **Sites > Site Management**.
The Sites page appears.
2. Click **Add** and select **Spoke Site**.
The Add Site for *Tenant -Name* page appears.
3. Complete the configuration settings in the General and Connectivity Requirements section according to the guidelines provided in [Table 159 on page 323](#).

Table 159: Fields on the Add Spoke Site Page

Field	Description
General	

Table 159: Fields on the Add Spoke Site Page (continued)

Field	Description
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 15 characters.
Site Type	Displays the site type. This field cannot be modified. Example: Spoke
Tenant Topology	Displays the topology of the tenant that was selected during the creation of the tenant. This field cannot be modified. Example: standalone
Site Group	Select a site group to which you want to assign the site. Example: hybridwan-spoke
Address	
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.
Country	Select the country where the site is located. Click the Validate button to verify the address. The site address verification successful message is displayed if the address is correct. You can click the View location on a map link to see the address location. If you enter the wrong address and click the Validate button to verify the address, the Site address could not be validated message is displayed .
Contact Information	
Contact Name	Enter the name of a contact person for the site.
Email	Enter the e-mail ID of the contact person.
Phone	Enter the phone number of the contact person.
Connectivity Requirements	
Click a connection plan to select the plan for WAN connectivity.	
A connection plan contains information prepopulated from the device template, and includes the device information, a list of supported features and the number of WAN links supported.	
Based on the connection plan, the following fields are populated:	
WAN Underlay Links	

Table 159: Fields on the Add Spoke Site Page (continued)

Field	Description
WAN_0 WAN_1	Displays the WAN link. Depending on the connection plan selected, you can configure up to two WAN links per site that support the hybrid WAN. You can configure these links as MPLS or Internet links.
Name	Displays the name of the WAN link. This field cannot be modified.
Type	<p>Displays the link type for WAN underlays. The default link types supported by the device templates are listed below:</p> <ul style="list-style-type: none"> • NFX_deployment_option_1—Link type for WAN_0 is MPLS and WAN_1 is Internet. • SRX_deployment_option_1—Link type for WAN_0 is MPLS and WAN_1 is Internet. • SRX_Managed_Internet_CPE—Link type for WAN_0 is Internet. • NFX_Managed_Internet_CPE—Link type for WAN_0 is Internet. • NFX_deployment_option_4—Link type for WAN_0 is Internet.

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

5. Click **OK**.

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

- Related Documentation**
- [About the Sites Page on page 317](#)
 - [About the Site Groups Page on page 365](#)

Creating Local Service Edge Sites for Hybrid WAN Deployment

You create a local service edge site when the site is directly connected to the Internet or when you access the Internet through a corporate VPN. You use the **Sites** page to create the local service edge site.

To create a local service edge site:

1. Select **Sites > Site Management**.

The Sites page appears.

2. Click **Add** and select **Local Service Edge**.

The Add Local Service Edge site page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 160 on page 326](#).

Table 160: Fields on the Add Local Service Edge Site Page

Field	Description
Site Information	
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 15 characters.
Address	
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.
Country	Select the country name from the drop-down list.
Contact Information	
Contact Name	Enter the name of a contact person for the site.
Email	Enter the e-mail ID of the contact person at the site.
Phone	Enter the phone number of the contact person at the site.
Configuration	
Service POP	Select the name of the point of presence (POP) for the site. A network point of presence is a location at which a service provider instantiates a network function, such as a virtualized network function (VNF).
VIM	Select a virtualized infrastructure manager (VIM). The VIM controls and manages the compute, storage, and network resources in the NFV infrastructure. The VIM also collects and forwards performance measurements and events.
Resource Pool	Select a resource pool for the VIM. Resource pools identify the compute zones for the VIM for the POP.
Route Target	Enter a route target for the virtual network. Example: 64512:10000
SDN Gateway Router	Click the toggle button to enable SDN gateway router that is configured in the POP. The SDN gateway router provides a Layer 3 routing service to customer sites in a centralized deployment. <ul style="list-style-type: none"> Enabled : Managed—Select Managed option if you use Contrail Service Orchestration to manage the device. Disabled : Unmanaged—Select Unmanaged option if you use another application to manage the device.

Table 160: Fields on the Add Local Service Edge Site Page (continued)

Field	Description
PE Router	Specify the name of the device.
VRF Name	Specify the name of the virtual routing and forwarding (VRF) instance for the tenant.
Service Attachment Points	
Local Internet Breakout	Enable or disable Internet access to the site.
Left Subnet Prefix	Select one or more IPv4 prefixes for the management network.
Right Virtual Network Name	Select the network to which the site transmits Internet traffic.
Right Network - Internet Information	
Internet Network Name	Select the network to which the site transmits Internet traffic.
Site to VPN	Click the toggle button to enable VPN.
Left Subnet Prefix	Select one or more IPv4 prefixes for the management network.
Right Virtual Network Name	Select the network to which the site transmits Internet traffic.

4. Click **OK**.

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

- Related Documentation**
- [About the Sites Page on page 317](#)
 - [About the Site Groups Page on page 365](#)

Creating Regional Service Edge Sites for Hybrid WAN Deployment

You create a regional service edge site when you have to assign common services, such as NAT or UTM to multiple sites. The traffic from customer site is serviced and forwarded to common service and then to Internet. You create a cloud site from the **Sites** page. This page describes how to create a regional service edge site for a tenant.

To create a regional service edge site:

1. Select **Sites > Site Management**.

The Sites page appears.

2. Click **Add** and select **Regional Service Edge**.

The Add Regional Service Edge Site page appears.

3. Complete the configuration settings according to the guidelines provided in [Table 161 on page 328](#).

Table 161: Fields on the Add Regional Service Edge Site Page

Field	Description
Site Information	
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 15 characters.
Address	
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.
Country	Select the country name from the drop-down list.
Contact Information	
Contact Name	Enter the name of a contact person for the site.
Email	Enter the e-mail ID of the contact person.
Phone	Enter the phone number of the contact person.
Configuration	
Service POP	Select the name of the point of presence (POP) for the site. A network point of presence is a location at which a service provider instantiates a network function, such as a virtualized network function (VNF).
VIM	Select a virtualized infrastructure manager (VIM). The VIM controls and manages the compute, storage, and network resources in the NFV infrastructure. The VIM also collects and forwards performance measurements and events.
Resource Pool	Select a resource pool for the VIM. Resource pools identify the compute zones for the VIM for the POP.
Route Target	Enter a route target for the virtual network.
Virtual Network Name	Enter a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters. A virtual network is a representation of your own network in the cloud.
Left Subnet Prefix	Select one or more IPv4 prefixes for the management network.
Service Attachment Points	

Table 161: Fields on the Add Regional Service Edge Site Page (continued)

Field	Description
Local Internet Breakout	Click the toggle button to enable or disable the Internet access to the site.
Internet Network Name	Select the network to which the site transmits Internet traffic.

- Click **OK**.

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

- Related Documentation**
- [About the Sites Page on page 317](#)
 - [About the Site Groups Page on page 365](#)

Creating On-Premise Hub Sites for SD-WAN Deployment

An on-premise hub represents an automation end point that is part of customer premise equipment at headquarter or main branch office. The hub site is connected to multiple spoke sites using the overlay connections. You create an on-premise hub site from the **Sites** page.

To create an on-premise hub site:

- Click **Add** and select **On-Premise Hub**.

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

- Complete the configuration settings according to the guidelines provided in [Table 162 on page 329](#).

Table 162: Fields on the Add On-Premise Hub Site Page

Field	Description
General	
Site Name	Enter a site name for the tenant.
Site Type	Displays the site type. This field cannot be modified.
Tenant Topology	Displays the topology of the tenant that was selected while creating the tenant. This field cannot be modified.
Site Group	Select a site group to which you want to assign the site.
Street Address	Enter the street address of the site.
City	Enter the name of the city where the site is located.

Table 162: Fields on the Add On-Premise Hub Site Page (continued)

Field	Description
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. Click the Validate button to verify the address. The site address verification successful message is displayed if the address is correct. You can click the View location on a map link to see the address location.</p> <p>If you enter the wrong address and click the Validate button to verify the address, the Site address could not be validated message is displayed .</p>
Contact Name	Enter the name of the contact person at the site.
Email	Enter the e-mail address of the contact person at the site.
Phone	Enter the phone number for the site.
Connectivity Requirements	
Connectivity Requirements for the Selected Plan	<p>Click a connection plan to select the plan for WAN connectivity.</p> <p>A connection plan contains information prepopulated from the device template, and includes the device information, a list of SD-WAN features supported, and the number of links supported.</p>
WAN Underlay Links	
WAN_0	Displays the WAN link. Depending on the connection plan selected, you can configure up to four WAN links per site that support SD-WAN. You can configure these links as MPLS or Internet links.
WAN_1	
WAN_2	
WAN_3	
Enable WAN_0	Select this check box to enable the WAN link.
Enable WAN_1	
Enable WAN_2	
Enable WAN_3	
Name	Displays the name of the WAN link. This field cannot be modified.
Type	Select the link type of the WAN link—MPLS or Internet.

Table 162: Fields on the Add On-Premise Hub Site Page (continued)

Field	Description
Subscribed Bandwidth	Enter the maximum bandwidth to be allowed for a specific WAN link.
Provider	Enter the name of the Internet Service Provider (ISP).
Cost/Month	Enter the cost per month in the specified currency for the subscribed bandwidth.
Additional Requirements	
Site Type	Displays the site type. This field cannot be modified.
<i>Local Breakout</i>	
Enable Local Breakout	Select this option to enable local breakout on the site. Local breakout is the ability of the site to route Internet traffic directly from the site.
Links for Breakout	Select the WAN links on which you want to enable local breakout. You can also choose to use each WAN link exclusively for local breakout traffic or for both local breakout as well as WAN traffic. You cannot select previously selected default WAN links to be used exclusively for local breakout traffic. NOTE: You must select at least one WAN link to enable breakout.
LAN Segment	
NOTE: A hub site does not require a LAN Segment. Please click next and proceed.	

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

4. Click **OK**.

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

- Related Documentation**
- [About the Sites Page on page 317](#)
 - [Local Breakout Overview on page 319](#)

Creating On-Premise Spoke Sites for SD-WAN Deployment

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 create an on-premise spoke site from the **Sites** page.

You can also add an SD-WAN on-premise site using dual CPE devices. The workflow to add a site with dual CPE devices is similar to the single CPE device. When you create a

site, select the appropriate connection plan, which supports the dual CPE solution. The device templates that support the dual CPE device solution are as follows:

- NFX_SDWAN_Dual_CPE—Supports dual CPE devices on NFX250 Network Services Platform devices.
- SRX_SDWAN_Dual_CPE—Supports dual CPE devices on SRX300 line of devices or SRX550 Services Gateway devices.

After you select the connection plan, enable the required WAN links (MPLS or Internet). These WAN links are distributed across two NFX250, SRX300 line of devices, or SRX550 devices.



NOTE: You must enable at least one WAN link per CPE device.

To create an on-premise spoke site:

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

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

2. Complete the configuration settings according to the guidelines provided in [Table 163 on page 332](#).

Table 163: Fields on the Add On-Premise Spoke Site Page

Field	Description
General	
Site Name	Enter a site name for the tenant. You can use alphanumeric characters and hyphen (-). The maximum length is 15 characters.
Site Type	Displays the site type. This field cannot be modified.
Tenant Topology	Displays the topology of the tenant that was selected while creating the tenant. This field cannot be modified.
Site Group	Select a site group to which you want to assign the site.
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 163: Fields on the Add On-Premise Spoke Site Page (continued)

Field	Description
Country	<p>Select the country where the site is located. Click the Validate button to verify the address. The site address verification successful message is displayed if the address is correct. You can click the View location on a map link to see the address location.</p> <p>If you enter the wrong address and click the Validate button to verify the address, the Site address could not be validated message is displayed .</p>
Contact Name	Enter the name of the contact person at the site.
Email	Enter the e-mail address of the contact person at the site.
Phone	Enter the phone number for the site.
Connectivity Requirements	
Connectivity Requirements for the Selected Plan	<p>Click a connection plan to select the plan for WAN connectivity.</p> <p>A connection plan contains information prepopulated from the device template, and includes the device information, a list of SD-WAN features supported, and the number of links supported.</p>
WAN Underlay Links	
WAN_0	Displays the WAN link. Depending on the connection plan selected, you can configure up to four WAN links per site that support SD-WAN. You can configure these links as MPLS or Internet links.
WAN_1	
WAN_2	
WAN_3	
Enable WAN_0	Select this check box to enable the WAN link.
Enable WAN_1	
Enable WAN_2	
Enable WAN_3	
Name	Displays the name of the WAN link.
Type	Select the connection type of the WAN link—MPLS or Internet.

Table 163: Fields on the Add On-Premise Spoke Site Page (continued)

Field	Description
Access Type	<p>Select the access type for WAN connectivity.</p> <ul style="list-style-type: none"> Ethernet—Enables WAN connectivity through Ethernet port. LTE—Enables Long-Term Evolution (LTE) USB dongle support. <p>NOTE:</p> <ul style="list-style-type: none"> The LTE access type is supported only on NFX250 devices. You can select only one WAN link with LTE access type. LTE is not supported when you create an SD-WAN on-premise site with dual CPE devices. <p>NOTE:</p>
Subscribed Bandwidth	<p>Enter the maximum bandwidth to be allowed for a specific WAN link. The range is 1 through 999999999.</p> <p>NOTE: If the access type for the WAN link is LTE, then you cannot configure the bandwidth.</p> <p>NOTE: LTE is not supported when you create an SD-WAN on-premise site with dual CPE devices.</p>
Provider	Enter the name of the Internet Service Provider (ISP).
Cost/Month	Enter the cost per month of the subscribed bandwidth in the specified currency. The range is 1 through 999999999.
WAN Link (Primary or Secondary)	Displays whether it is a primary device WAN link or secondary device WAN link. This field cannot be modified and it is displayed only when you select a SRX or NFX dual CPE connection plan.
Additional Requirements Based on the connectivity requirement, the following fields are populated:	
Site Type	Displays the site type. This field cannot be modified.
Default Link	<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>

Table 163: Fields on the Add On-Premise Spoke Site Page (continued)

Backup Link	<p>Select a backup link through which traffic can be routed when the primary links are unavailable. In the hub-and-spoke topology, if an LTE link is available, the LTE link is by default selected as the backup link. You cannot change the default selection. If no LTE link is assigned, you can select any of the links other than the default links. Note that you cannot assign the backup link for exclusive breakout traffic (the Use only for breakout traffic 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> <p>NOTE: LTE is not supported when you create an SD-WAN on-premise site with dual CPE devices.</p>
Enable Local Breakout	<p>Click the toggle button to enable local breakout on the site. If you specify LTE as the access type for a WAN link, by default, the WAN link is selected as the local breakout link.</p> <p>NOTE: LTE is not supported when you create an SD-WAN on-premise site with dual CPE devices.</p>
Links for Breakout	<p>Select the WAN links on which you want to enable local breakout. You can also choose to use each WAN link exclusively for local breakout traffic or for both local breakout and WAN traffic. You cannot select previously selected default WAN links to be used exclusively for local breakout traffic.</p>
Preferred Breakout Link	<p>Select the preferred link for local breakout. If no link is selected, then the breakout link is chosen using ECMP from the available links.</p> <p>If you select LTE as the access type for a WAN link, by default, the WAN link is selected as the local breakout link.</p> <p>NOTE: LTE is not supported when you create an SD-WAN on-premise site with dual CPE devices.</p>
Enable Hub Multihoming	<p>Select this option to enable multihoming on the site. Multihoming is the ability of a spoke site to connect to multiple hub sites, thereby providing redundancy. To enable multihoming on a site, you must select the hub-and-spoke topology when you create the tenant.</p>
Device Redundancy	<p>Displays the device redundancy mode. This field cannot be modified.</p> <ul style="list-style-type: none"> • true—Supports dual CPE devices on an SD-WAN on-premise spoke site • false—Does not support dual CPE devices on an SD-WAN on-premise spoke site.
Add LAN Segment	
NOTE: You must add at least one LAN segment.	
Name	<p>Enter a unique string of alphanumeric characters and special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p>
Port	<p>Select a port number from the list. Depending on the device configured in the connection plan, you can specify up to two port numbers.</p>
VLAN ID	<p>Enter the VLAN ID that is associated with the MPLS data link in the range 1 through 4094.</p>
Department	<p>Select a department to which the LAN segment is to be assigned. Click Create Department to create a new department and assign the LAN segment to it. You group LAN segments as departments for ease of management and for applying policies at the department-level.</p>

Table 163: Fields on the Add On-Premise Spoke Site Page (continued)

DHCP	Enable or disable DHCP. Enable DHCP to assign IP addresses by using a DHCP sever. Disable DHCP to assign static IP addresses. By default, DHCP is disabled.
IP Address Prefix	Enter one or more IPv4 prefixes for the site management network.
Subnet	Enter the subnet mask of the DHCP IP address pool.
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	Specify the maximum duration of time (in seconds) for which a client can request for and hold a lease on a DHCP server. You can enter a value in the range 0 through 4,294,967,295 seconds.
Name Server	Enter the IPv4 address of the DNS server. DNS servers are used for resolving host names to IP addresses.

3. (Optional) You can review the configuration in the **Summary** tab and modify the settings, if required.

4. Click **OK**.

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

**Related
Documentation**

- [About the Sites Page on page 317](#)
- [Local Breakout Overview on page 319](#)

Creating Cloud Hub Sites for SD-WAN Deployment

In a cloud site, customers access network services from the service provider's cloud. You create a cloud site from the **Sites** page. This page describes how to create a cloud site for a tenant.

To create a cloud site:

1. Select **Sites > Site Management**.

The **Sites** page appears.

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

The **Add Cloud Site** page appears.

3. Complete the configuration settings in the Site Information, Configuration, and Service Attachment Points sections according to the guidelines provided in

[Table 164 on page 337.](#)

Table 164: Fields on the Add Cloud Site Page

Field	Description
Site Information	
Site Name	Enter a site name. You can use any number of alphanumeric characters, including special characters. The maximum length is 15 characters.
Cloud Hub Type	<p>Select the cloud hub type—Regional Service Edge, Local Service Edge, or Cloud Hub. All three hub types are hosted on a point of presence (POP). However, on a POP, you can configure only one hub type at a time. By default, the Cloud Hub type is displayed when configuring a cloud site.</p> <p>Select Local Service Edge if the site is directly connected to the Internet. Traffic from customer site is serviced and forwarded to Internet. This is similar to the local breakout feature.</p> <p>Select Regional Service Edge when you want to assign common services, such as NAT or UTM to multiple sites.</p>
Address	
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.
Contact Name	Enter the name of a contact person for the site.
E-mail	Enter the e-mail ID of the contact person.
Phone	Enter the phone number of the contact person.
Virtual Network Name	<p>Enter a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.</p> <p>A virtual network is a representation of your own network in the cloud.</p>
Configuration	
Based on the cloud hub device, the following fields are populated:	
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 cloud hub device name for the site.

Table 164: Fields on the Add Cloud Site Page (continued)

Field	Description
GRE Interfaces	(Optional) Select one or more generic routing encapsulation (GRE) tunnel interfaces. All the interfaces configured while adding a cloud hub device are listed. A subset of the interface(s) can also be selected. To delete the interface name, click x.
MS Interfaces	(Optional) Select one or more multiservices (MS) tunnel interfaces. All the interfaces configured while adding a cloud hub device are listed. A subset of the interfaces can also be selected. To delete the interface name, click x.
VT Interfaces	(Optional) Select one or more virtual tunnel (VT) interfaces. All the interfaces configured while adding a cloud hub device are listed. A subset of the interface(s) can also be selected. To delete the interface name, click x.
Logical Interface Unit Range	(Optional) Enter the logical interface range for the tunnel interface. The default range is set during CSO setup. If you do not specify any value, then the default range is considered.
VIM	Select a virtualized infrastructure manager (VIM). The VIM controls and manages the compute, storage, and network resources in the NFV infrastructure. The VIM also collects and forwards performance measurements and events.
Resource Pool	Select a resource pool for the VIM. Resource pools identify the compute zones for the VIM for the POP.
Route Target	Enter a route target for the virtual network.
Service Attachment Points	
Local Internet Breakout	Enable or disable Internet access to the site.
Left Subnet Prefix	Select one or more IPv4 prefixes for the management network.
Internet Network Name	Select the network to which the site transmits Internet traffic.

4. Click **OK**.

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

- Related Documentation**
- [About the Sites Page on page 317](#)
 - [About the Site Groups Page on page 365](#)

Creating Cloud Spoke Sites for SD-WAN Deployment

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

To create a cloud spoke site:

1. Select **Sites > Site Management**.

The Sites page appears.

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

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

3. Complete the configuration settings in the Site Information, Configuration, and Service Attachment Points sections according to the guidelines provided in [Table 165 on page 339](#).

Table 165: Fields on the Add Cloud Spoke Site Page

Field	Description
Site Information	
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 Type	Displays the site type as Spoke . This field cannot be modified.
Tenant Topology	Displays the topology of the tenant that was selected during the creation of the tenant. This field cannot be modified. NOTE: Only hub-and-spoke topology is supported.
Site Group	(Optional) Select a site group to which you want to assign the site. Example: cloud-spoke
Cloud Information	
Region	Select the region to which the site belongs. The regions in CSO are mapped to the regions in the AWS account. Example: Ohio

Table 165: Fields on the Add Cloud Spoke Site Page (continued)

Field	Description
VPC ID	<p>Enter the VPC ID from the AWS account. Ensure that the VPC is attached to the Internet gateway.</p> <p>To obtain VPC ID:</p> <ol style="list-style-type: none"> Log in to AWS account. Search for VPC service. Click the VPC dashboard. Select a VPC ID. <p>Ensure that the VPC is attached to the Internet gateway.</p> <p>To check whether VPC is attached:</p> <ol style="list-style-type: none"> Log in to AWS account. Search for VPC service. Click the Internet Gateway dashboard. Check whether the VPC state is attached. <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"> Use an existing subnet in AWS account Create new
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 prefix other than the reserved IP prefix.</p> <p>Example: 105.0.1.5/24</p>
Connectivity Requirements	<p>Click a connection plan to select the plan for WAN connectivity.</p> <p>A connection plan contains information prepopulated from the device template, and includes the device information, a list of SD-WAN features supported, and the number of links supported.</p> <p>NOTE: vSRX_AWS_SDWAN_Endpoint_option_1 template supports cloud spoke site for AWS VPC.</p>
WAN Underlay Links	

Table 165: Fields on the Add Cloud Spoke Site Page (continued)

Field	Description
WAN_0 WAN_1	Select the check boxes to configure the WAN links. Depending on the connection plan selected, you can configure up to two WAN links per site that support SD-WAN. You can configure these links as MPLS or Internet links.
Name	Displays the name of the WAN link. This field cannot be modified.
Type	Displays the connection type for WAN underlays. Only Internet link is supported.
Subscribed Bandwidth	Enter the maximum bandwidth (in Mbps) to be allowed for a specific WAN link.
Provider	Enter the name of the Internet Service Provider (ISP).
Cost/Month	Enter the cost per month of the subscribed bandwidth in the specified currency.
Static IP Prefix	<p>Enter the private IPv4 address 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 inside 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>Enter the IPv4 address for the gateway. Typically, the first IP address in the subnet is selected for gateway IP address.</p> <p>Example: 105.0.2.1</p>
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>
Traffic Type	<p>Select the traffic type. The options available are:</p> <ul style="list-style-type: none"> DATA_ONLY—Select this option if you want to use the WAN link to transmit only data traffic. OAM_AND_DATA—Select this option if you want to use the WAN link to transmit both data traffic and management traffic. <p>NOTE: You must select at least one WAN link with the OAM_AND_DATA traffic type.</p>
Additional Requirements	Based on the connectivity requirement, the following fields are populated:
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>

Table 165: Fields on the Add Cloud Spoke Site Page (continued)

Field	Description
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 Use only for breakout traffic 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>
Enable Local Breakout	Click the toggle button to enable local breakout on the site.
Links for Breakout	Select the WAN links on which you want to enable local breakout. You can also choose to use any one WAN link exclusively for local breakout traffic or for both local breakout and WAN traffic.
Preferred Breakout Link	Select the preferred link for local breakout. If no link is selected, then the breakout link is chosen using ECMP from the available links.
LAN Segments	Add at least one LAN segment.
Name	Enter a unique string of alphanumeric characters and special characters (-). No spaces are allowed and the maximum length is 15 characters.
Ports	<p>Select a LAN port from the drop-down list.</p> <p>NOTE: The ports in LAN segment must be contiguous. For example, If both WAN_0 and WAN_1 are enabled and are using interfaces ge-0/0/0 and ge-0/0/1 respectively, then LAN_0 must use ge-0/0/2. If only WAN_0 is enabled and is using interface ge-0/0/0, the LAN_0 must use ge-0/0/1.</p>
IP Address Prefix	<p>Enter one or more IPv4 prefixes for the LAN segment for the service. The IP prefix is for the network on the LAN side of the CPE device with vSRX instance. Go to AWS account, check the subnet and provide an IPv4 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: 105.0.4.5/24</p>
Department	Select a department to which you want to assign the LAN segment. Click Create Department to create a new department and assign the LAN segment to it. You group LAN segments as departments for ease of management and for applying policies at the department level.
Departments	Create departments to group LAN segments within a site. You use departments to apply specific policies to LAN segments that are members of a department.
Name	Enter a name for the department.
Description	Enter a description for the department.
VPN	Select a VPN to which you want to assign the department.

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

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

**Related
Documentation**

- [Provisioning a Cloud Spoke Site in AWS VPC on page 343](#)
- [About the Sites Page on page 317](#)
- [About the Site Groups Page on page 365](#)

Provisioning a Cloud Spoke Site in AWS VPC

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) to 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 to 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.

To set up and monitor your network:

- [Add a Cloud Spoke Site on page 343](#)
- [Configure the Cloud Spoke Site on page 344](#)
- [Download the Cloud Formation Template on page 345](#)
- [Provision the Device on AWS Server on page 345](#)
- [Activate the Device on page 346](#)

Add a Cloud Spoke Site

To add a cloud spoke site:

1. Select **Sites > Site Management > Add > Cloud Spoke**.
2. Specify the site information such as, site name, AWS region, VPC ID, management subnet, IP prefix and click **Next**.

3. Specify vSRX_AWS_SDWAN_Endpoint_option_1 as the connection plan.

**NOTE:**

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

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

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

5. Specify additional requirements and click **Next**.

6. Specify LAN segment information and click **Next**.

7. In the **Summary** tab, check the configuration and click **Edit** to modify the settings.

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

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

Configure the Cloud Spoke Site

To configure a cloud spoke site:

1. Select **Sites > Site Management**.

The sites page appears.

2. Select the cloud spoke site that you created and click **Configure Site**.

The configure site page appears.

3. In the **Connectivity** tab, specify the primary hub site detail, overlay tunnel information, and WAN interface details.

4. Click **Ok**.

5. Click **Devices** tab and enter the activation code provided by your service provider.

6. Click **Ok**

The site status is changed to **Configured**.

Download the Cloud Formation Template

To download the cloud formation template:

1. Click **Resources > Devices**.

2. Identify the device that you want to activate.

You can activate a device if it has the status as Expected.

3. Select the device and click **Activate Device**.

The Activate device page appears.

4. Enter the activation code supplied by the service provider.

You can download the cloud formation template after you enter the correct activation code.

5. 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. Specify the Custom Image Id for the vSRX.

You must ensure that you have the supported software image for the AWS spoke. If the image is unavailable on the AWS marketplace, you must do the following to get the AMI number for your desired region:

- a. Search the public AMI for `media-srxmr-vm disk-Version-Number`, where *Version-Number* is the vSRX software image supported on AWS, and note down the AMI ID (for your region) that corresponds to this image.

For example, if the supported software version is 15.1X49.D133, then search the public AMI for `media-srxmr-vm disk-15.1X49-D133` and note down the AMI ID.

- b. Paste the AMI ID in the **CustomImageId** field.



NOTE: You must specify the Custom Image ID field because not doing so results in failure during stack creation or provisioning.

7. In the Parameters section, specify the KeyName for your EC2 instance.

8. Click **Next**.

9. Select **I acknowledge that AWS CloudFormation might create IAM Resources**.

10. 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

- [Creating Cloud Spoke Sites for SD-WAN Deployment on page 338](#)

Importing Multiple Sites

You can use the **Import Sites** page to configure a site by uploading a JSON file. To configure a site by using the site upload feature, specify the site parameters in a JavaScript Object Notation (JSON) file. You can also use the site upload feature to edit the configuration information of a site. This method enables you to modify only the required parameters without going through the site creation workflow.



TIP: You can download a sample JSON file from the **Download Sample JSON** link and edit the parameters based on the requirements of the site that you want to configure.

To configure a site by uploading a JSON file:

1. Click **Sites > Add > Import Sites**.

The **Import Sites** page is displayed.

2. Click **Browse** and navigate to the directory that contains the JSON file.

Alternatively, download a sample JSON file by clicking the **Download Sample JSON** link and edit the parameters according to the requirements of the site.

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

4. Click **Import**.

A success message is displayed indicating that the file is uploaded successfully.

Related Documentation

- [About the Sites Page on page 317](#)

Managing a Single Site

You can use the **Site Management** page to view the site details and to manage the site configurations for a single site. To access the page, click **Sites > Site Management > Site-Name**.

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.

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. Because the full mesh topology supports only static SD-WAN policies, SLA parameters such as throughput, latency, packet loss, delay, and jitter are not computed.

- 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 352](#).
- On the **Devices** tab, view a list of devices in your network. See [“About the Devices Page” on page 88](#).

Related Documentation

- [About the Sites Page on page 317](#)

Configuring a Single Site

You can specify the underlay configuration of a hub device by using the **Configure Site** feature on the **Site Management** page.

You can also configure an SD-WAN on-premise spoke site using dual CPE devices. The workflow to configure a site with dual CPE devices is similar to single CPE device. You need at least one WAN link per CPE to act as a OAM_AND_DATA for redundancy, so that the individual nodes establish connectivity with CSO.

You must provide the serial number and the activation code for both the primary and the secondary devices.

To configure a site:

1. Click the **Configure Site** button on the **Sites > Site Management** page.
The **Configure Site Site Name** page is displayed.
2. Complete the configuration settings according to the guidelines provided in [Table 166 on page 349](#).

Table 166: Fields on the Configure Site Page

Field	Description
Site Type	Displays the site type.

Table 166: Fields on the Configure Site Page (continued)

Field	Description
Management Region	Displays the regional server with which the CPE device communicates based on the information in the device profile. This field cannot be modified.
Selected Plan	Displays the connection plan that you selected when you created the site. This field cannot be modified.
Hub Multihoming	Displays whether multihoming was enabled or disabled on the site during the creation of the site. This field cannot be modified.
<i>Configuration</i>	
Connectivity	
Management Connectivity	
OAM Traffic Information	Enable Operation, Administration, and Maintenance (OAM) traffic information to specify the OAM VLAN ID, IP prefix for the site management network, and gateway IP address of the default route.
VLAN ID	Specify the OAM VLAN ID for in-band management of the site.
IP Prefix	Specify one or more prefixes for the site management network. You can specify IPv4 or IPv6 addresses. Example: 10.0.2.16/24
Gateway IP	Specify the IP address of the default route for the management network. You can use an IPv4 or IPv6 address.
WAN_0, WAN_1, WAN_2, WAN_3	
WAN Interface	Displays the interface name configured in the device profile. This field cannot be modified.
Link Type	Displays the link type (MPLS or Internet) configured in the device profile. This field cannot be modified.
Address Assignment	Select the method of IP address assignment. Select DHCP to assign IP addresses by using a DHCP sever or Static to assign a static IP address.
Traffic Type	Select the traffic type. You specify whether you want to use the WAN link to transmit only data traffic or both management traffic and data traffic. You must select the traffic type as OAM_and_DATA when you configure a site with dual CPE devices. You need at least one WAN link per CPE to act as a OAM_AND_DATA for redundancy.
Data VLAN ID	VLAN ID associated with the WAN link.

Table 166: Fields on the Configure Site Page (continued)

Field	Description
Local Breakout	<p>Displays whether local breakout was enabled on the WAN link during creation of the site. This field cannot be modified.</p> <p>If the WAN link is selected to be used for only local breakout traffic, then the <i>Overlay Tunnel</i> section is not displayed.</p>
Autocreate Source NAT Rule	<p>Select this option to enable interface-based source NAT on the WAN link.</p> <p>NOTE: If this option is enabled for a WAN interface W1 during the site creation 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> <p>Zone1 --> W1: Translation=Interface</p> <p>Zone2 --> W1: Translation=Interface</p> <p>Zone3 --> W1: Translation=Interface</p> <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> <p>Zone1 --> W1 : Translation=Pool-2</p> <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> <p>Zone1, Port 56578 --> W1: Translation=Pool-2</p>
Overlay Tunnel	
Tunnel Type	Select the tunnel type—GRE or GRE over IPsec.
Peer Device	Displays the hub device to which the site is connected.
Interface Name	Select the name of the interface of the hub device to which the MPLS or Internet link is connected.
Devices	
<i>Assign CPE Devices</i>	
Device Redundancy	Displays whether device redundancy is enabled or disabled for an SD-WAN on-premise spoke site.
Primary Device Serial Number	Enter the serial number of the primary CPE device. You can use a unique string of alphanumeric characters. The maximum length is 64 characters. Serial numbers are case-sensitive.

Table 166: Fields on the Configure Site Page (continued)

Field	Description
Primary Device Activation Code	Enter the activation code of the primary device that your service provider supplied for the device. NOTE: If you do not want to specify an activation code, on the Resources > Device Templates > Template Settings page, disable the ACTIVATION_CODE_ENABLED field and save the changes.
Secondary Device Serial Number	Enter the serial number of the secondary CPE device. You can use a unique string of alphanumeric characters. The maximum length is 64 characters. Serial numbers are case-sensitive.
Activation Code	Enter the activation code of the secondary device that your service provider supplied for the device. NOTE: If you do not want to specify an activation code, on the Resources > Device Templates > Template Settings page, disable the ACTIVATION_CODE_ENABLED field and save the changes.
Boot Image	(Optional) Select the boot image from the drop-down list. The boot image is the device image that was previously uploaded to the image management system through the “Images” page. 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. See <i>Uploading a Device Image</i> .

3. Click **OK**.

Related Documentation

- [About the Sites Page on page 317](#)
- [Local Breakout Overview on page 319](#)

Managing LAN Segments on a Tenant Site

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 **Sites > Site Management > Site Name > LAN** tab.

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

- [Creating LAN Segments on page 352](#)
- [Deploying a LAN Segment on page 354](#)
- [Reassigning a LAN Segment to a Department on page 354](#)
- [Deleting LAN Segments on page 355](#)

Creating LAN Segments

You create LAN segments from the **Sites > Site Management > Site Name** page.

To create a LAN segment:

1. Click the add icon (+) on the **LAN** tab.
2. Complete the configuration settings according to the guidelines provided in [Table 167 on page 353](#).

Table 167: Create LAN Segment Page

Field	Description
Name	Enter a unique string of alphanumeric characters and some special characters (. -). No spaces are allowed and the maximum length is 15 characters.
Ports	Select a port number from the list. Depending on the device configured in the connection plan, you can select up to two port numbers.
VLAN ID	Specify the VLAN ID that is associated with the MPLS data link.
DHCP	Enable or disable DHCP. Enable DHCP to assign IP addresses by using a DHCP sever. Disable DHCP to assign static IP addresses. By default, DHCP is disabled.
Subnet	Enter the IP address and subnet mask for the DHCP address pool. For example, 192.0.2.0/24. The subnet mask is validated as you enter it.
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	Specify the maximum duration of time (in seconds) for which a client can request for and hold a lease on a DHCP server. You can enter a value in the range 0 through 4,294,967,295 seconds.
Name Server	Enter the IPv4 address of the DNS server. DNS servers are used for resolving hostnames to IP addresses.
Department	Select a department to which the LAN segment is to be assigned. You group LAN segments as departments for ease of management and for applying policies at the department-level. To create a new department and assign the LAN segment to it, click the Create Department link. See "Creating a Department" on page 305 .



NOTE: You must select at least one port, one IP address prefix, or one VLAN ID.

3. Click **OK**.
The new LAN segment is displayed on the tenant site page.

Deploying a LAN Segment

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

To deploy a LAN segment:

1. Click the **LAN** tab.
2. Select the LAN segment that you want to deploy and click **Deploy**.
A **Deploy LAN Segment** job is created.
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 LAN Segment to a Department

You can reassign the department assigned to a LAN segment from the **Sites > Site Management > 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 **Sites > Site Management > 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.

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, click **Sites > Stage-1 Config**.

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 168 on page 357](#).

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 168: 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 Hub	View the name of the hub to which the CPE device is connected.
Device Model	View the device model.
Serial Number	View the 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	View the recipient details.

Related Documentation

- http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/nfx-series/product/

- [About the Sites Page on page 317](#)
- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)
- [Configuring a Single Site on page 349](#)
- [About the Certificates Page on page 403](#)

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 169 on page 358](#).

Table 169: Fields on the Activate Device Page

Field	Description
Site Name & Type	View the name of the site on which the CPE device is activated.

Table 169: Fields on the Activate Device Page (continued)

Field	Description
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>NOTE: If you do not want to specify an activation code, on the Resources > Edit Template > Template Settings page, disable the ACTIVATION_CODE_ENABLED field and save the changes.</p>
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>NOTE: If you do not want to specify an activation code, on the Resources > Edit Template > Template Settings page, disable the ACTIVATION_CODE_ENABLED 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 on page 321](#)
- [Activating a CPE Device on page 355](#)
- [About the Sites Page on page 317](#)
- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)
- [Configuring a Single Site on page 349](#)
- [About the Certificates Page on page 403](#)

Viewing the History of Tenant Device Activation Logs

You can use the Activation Logs page to view the history of device activation logs. You can also view the details of the activation logs and their status.

To view the device activation logs:

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

The Tenant Devices page appears, which list all devices.

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

The Activation Logs page is displayed. [Table 170 on page 361](#) describes the fields on the Activation Logs page.

3. Click a task name.

The ZTP Logs page appears. [Table 171 on page 361](#) describes the fields on the ZTP Logs page.

4. Click the Task Name.

The Job Status page appears. [Table 172 on page 361](#) describes the fields on the Job Status page.

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

Table 170: 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 171: 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 172: 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.

Table 172: Fields on the Job Status Page (continued)

Field	Description
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](#)

Configuring VRFs and PNE Details for a Site in a Centralized Deployment

If you use a physical network element (PNE) for a centralized deployment, you can use the Device Configuration page to configure the virtual routing and forwarding instances for your customer sites if you have not done so in Contrail and in Junos OS on the MX Series router.

To configure a VRF and PNE details for a site:

1. Click **Sites**.

The Sites page appears.

2. Select the site name.

3. Click **More > Advanced Configuration**.

The Device Configuration page appears.

4. Complete the configuration according to the guidelines provided in [Table 173 on page 362](#).

5. Click **OK**.

Table 173: Fields on the Device Configuration Page

Field	Description
Site VRF Name	Specify the name of the virtual routing and forwarding (VRF) instance for the tenant. Example: tenantA-VRF
Interface Name	Specify the MX Series router interface that connects to the customer site. This value matches the interface that you configure for the MX Series router physical network element (PNE). Example: xe-2/2/2

Table 173: Fields on the Device Configuration Page (continued)

Field	Description
Interface VLAN	<p>(Optional) Specify a valid VLAN identifier, which is an integer in the range 1 to 4094. Specifying a VLAN identifier enables VLAN tagging. If you do not specify a value, the VLAN is untagged.</p> <p>Example: 52</p>
Interface Address	<p>(Optional) Specify an IPv4 address with a network mask for the VLAN interface.</p> <p>Example: 192.0.2.16/24</p>
Default Gateway	<p>(Optional) Specify the IPv4 address for the default route for Internet traffic.</p> <p>Example: 192.0.2.20</p>
Route Target	<p>Specify the route target for the site. This value matches the route target value that you configure for the MX Series router PNE.</p> <p>Example: 64512:1102</p>
Route Distinguisher	<p>Specify a unique route distinguisher for the site. You can specify any unique route distinguisher, such as the route target for the site.</p> <p>Example: 64512:1102</p>

**Related
Documentation**

- [Creating On-Premise Spoke Sites for SD-WAN Deployment on page 331](#)

CHAPTER 21

Managing Site Groups

- [About the Site Groups Page on page 365](#)
- [Creating Site Groups on page 366](#)

About the Site Groups Page

To access this page, click **Sites > 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 existing site groups. See *Viewing Object Details*.
- Create site groups. See [“Creating Site Groups” on page 366](#).
- 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 174 on page 365](#) shows the descriptions of the fields on the **Site Groups** page.

Table 174: 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 on page 366](#)

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 **Sites > 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 on page 365](#)

PART 7

Viewing Reports

- [Security Reports on page 369](#)
- [SD-WAN Reports on page 379](#)

CHAPTER 22

Security Reports

- [Reports Overview on page 369](#)
- [About the Security Report Definitions Page on page 370](#)
- [Performing Different Actions on Reports on page 371](#)
- [About the Security Generated Reports Page on page 372](#)
- [Creating Log Report Definition on page 373](#)
- [Creating Bandwidth Report Definition on page 375](#)
- [Editing and Deleting Log Report Definitions on page 376](#)
- [Editing and Deleting Bandwidth Report Definitions on page 377](#)

Reports Overview

Reports are generated based on the summary of network activity and overall network status. You can use the predefined reports as-is, or you can build custom reports that meet your needs for specific data.

Using reports, you can:

- Schedule reports based on the defined filters.
- Schedule reports based on the available default reports.
- Generate reports with multiple sections, where each section has its own criteria.

The generated report will have a table of contents (TOC) with links to each section of the report. When the system generates a report, you and other designated recipients will receive the report in PDF format through e-mail.

Reports enable you to perform trend analysis of your network's activities.

The following are the types of security reports:

- **Log Based Reports**—Allows you to schedule reports based on the default reports and the default defined filters. You can also generate reports with different data criteria, which includes filters, aggregation criteria, and time range.
- **Bandwidth Based Reports**—Allows you to analyze the bandwidth usage of an application or a user.

The following are the types of SD-WAN reports:

- **SD-WAN Tenant Performance Reports**—Enables you to view the parameters (top applications by bandwidth, top sites not meeting the SLA, top sites meeting the SLA with switching, and sites meeting the SLA without switching applications) that measure the SLA performance across all sites in a tenant.
- **SD-WAN Site Performance Reports**—Enables you to view 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 generate report up to five sites in a tenant.

- Related Documentation
- [About the Security Report Definitions Page on page 370](#)
 - [About the SD-WAN Report Definitions Page on page 379](#)

About the Security Report Definitions Page

To access this page, click **Customer Portal > Reports > Report Definitions > Security**.

The Security Report Definitions page shows a list of predefined and custom reports. You can use the predefined reports as-is, or you can build custom reports.

Tasks You Can Perform

You can perform the following tasks from this page:

- Create a log report definition. See [“Creating Log Report Definition” on page 373](#).
- Create a bandwidth report definition. See [“Creating Bandwidth Report Definition” on page 375](#).
- You can also edit, run, and clone reports. See [“Performing Different Actions on Reports” on page 371](#).

Field Descriptions

[Table 175 on page 370](#) provides guidelines on using the fields on the Report Definitions page.

Table 175: Fields on the Report Definitions Page

Field	Description
Name	View the name of the report (user created or predefined). Example: Top Destination Countries
Description	View the description of the report definition. Example: Report for Top Destinations by Countries

Table 175: Fields on the Report Definitions Page (continued)

Field	Description
Type	View the type of report definition used such as bandwidth report or log report. Example: BANDWIDTH
Definition Type	View the type of report definition. Example: PREDEFINED
Report Content	View the details of the sections in the report. For example, Top Applications, Top Applications Blocked, Top Roles, and so on.
Schedule	View the report generation schedule whether to run the report immediately or schedule it for a later date and time.
Recipients	View the recipients of the generated reports.
Last Generated	View the time when the last report was generated if the report is scheduled at a later time.
Job ID	View the Job ID of the report.

**Related
Documentation**

- [Reports Overview on page 369](#)
- [Creating Log Report Definition on page 373](#)
- [Creating Bandwidth Report Definition on page 375](#)

Performing Different Actions on Reports

You can perform various actions on reports such as running a report immediately, editing a schedule, editing e-mail recipients, previewing a report in PDF, sending reports, and cloning reports.

To perform these actions on the report:

1. Select **Reports > Report Definitions**.
2. Select the report definition or right-click the report definition or click the **More** drop-down list.
3. Select the appropriate action from the drop-down list:

- **Delete Report**—You can select one or more report definitions and click the delete icon (X) to delete the report definition (s).
- **Run Now**—Runs the report immediately and provides a link to view the report in PDF format. You can view the archived reports by clicking the **Generated Reports** link on the left navigation pane.

This option is also available as the **Run Now** button on the Report Definitions page.

- **Preview as PDF**—Provides the PDF preview of the report.
- **Send Report**—Sends the report through e-mail to the recipient immediately. The user receives a notification once the report is sent. The user can also use the job ID to see more details of the job.
- **Edit Schedule**—Allows user to edit the schedule such as adding a recurrence, start date, end date, and time.
- **Edit Recipients**—Allows user to edit or add the recipients, e-mail address, subject, and comments.
- **Clone**— Allows the user to clone an existing report definition.

Related Documentation

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 176 on page 372](#) provides guidelines on using the fields on the Generated Reports page.

Table 176: 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.

Table 176: Fields on the Generated Reports Page (continued)

Field	Description
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**
- [Reports Overview on page 369](#)
 - [About the Security Report Definitions Page on page 370](#)

Creating Log Report Definition

You can use this page to create log report definitions. Log-based reports help you to schedule reports based on default reports and default defined filters. You can also generate reports with additional data criteria, including filters, aggregation criteria, and time range.

1. Select **Reports > Report Definitions**.
The 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 177 on page 373](#).
4. Click **OK** to save the log report definition. If you want to discard your changes, click **Cancel** instead.

Table 177: Fields on the Create Log Report Definition Page

Field	Description
General	
Report Name	Enter a unique name for the report definition that is a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 29 characters.
Description	Enter a description for the report definition; maximum length is 1024 characters.
Content	

Table 177: Fields on the Create Log Report Definition Page (continued)

Field	Description
Use Data Criteria from Filters	<p>Click Use Data Criteria from Filters.</p> <p>Select the data criteria from the list of default and user--created filters that are saved from the Events and Logs page.</p> <p>The details of the filters displayed are:</p> <ul style="list-style-type: none"> • Filter Name—Name of the filter. • Filter Description—Description of the filter. • Group By—Selected Group By option. • Time Span—Duration for which the data is displayed. • Filter By—List of default and user-created filters. <p>NOTE: The default time stamp value is the last 3 hours.</p>
Schedule	
Add Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule that you want to use:</p> <ul style="list-style-type: none"> • Run now—Select this option to schedule and publish the configuration at the current time. • Schedule at a later time—Select this option if you want to schedule and publish the configuration at a later time.
E-Mail	
Add E-Mail Recipients	<p>Click Add E-mail Recipients.</p> <ul style="list-style-type: none"> • Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external e-mail addresses. • Subject—Enter the subject for the e-mail notification. • Comment—Enter the comments for the e-mail notification. <p>NOTE: The reports are not sent if a specified recipient does not have permission for a device or domain included in the report configuration when the report is generated.</p>

Related Documentation

- [About the Security Report Definitions Page on page 370](#)
- [Creating Bandwidth Report Definition on page 375](#)

Creating Bandwidth Report Definition

You can use this page to create bandwidth report definitions. Bandwidth reports helps in analyzing the bandwidth usage of an application or a user. It gives you important information on bandwidth usage and helps you identify top applications and top users consuming bandwidth.

1. Select **Reports > Report Definitions**.

2. Click **Create > Bandwidth Report Definitions**.

The Create Bandwidth Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 178 on page 375](#).

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

Table 178: Fields on the Create Bandwidth Report Definition Page

Field	Description
General	
Report Name	Enter a unique name for the report definition 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 report definition; maximum length is 1024 characters.
Content	
Show Top	Specify the number of top events to be displayed. The value ranges from 1-20. The default value is 10.
Last	Specify the time period to generate the report from the last 3, 6, 12, or 24 hours.
Schedule	
Add Schedule	<p>Click Add Schedule.</p> <p>Select the type of report schedule that you want to use:</p> <ul style="list-style-type: none"> Run now—Select this option to schedule and publish the configuration at the current time. Schedule at a later time—Select this option if you want to schedule and publish the configuration at a later time.
E-Mail	

Table 178: Fields on the Create Bandwidth Report Definition Page (continued)

Field	Description
Add E-Mail Recipients	<p>Click Add E-mail Recipients.</p> <ul style="list-style-type: none">Recipients—Enter or select the e-mail addresses of the recipients. By default, you can search by first name and select registered users. You can also type in external e-mail addresses.Subject—Enter the subject for the e-mail notification.Comment—Enter the comments for the e-mail notification. <p>NOTE: The reports are not sent if a specified recipient does not have permission for a device or domain included in the report configuration when the report is generated.</p>

Related Documentation

- [About the Security Report Definitions Page on page 370](#)
- [Editing and Deleting Log Report Definitions on page 376](#)
- [Editing and Deleting Bandwidth Report Definitions on page 377](#)

Editing and Deleting Log Report Definitions

You can edit and delete log report definitions. This topic contains the following sections:

- [Editing the Log Report Definition on page 376](#)
- [Deleting Log Report Definitions on page 376](#)

Editing the Log Report Definition

To edit the log report definition:

1. Select **Reports > Report Definitions**.

The Report Definitions page appears.

2. Select the check box of the log report definition that you want to modify, and click the edit icon.

The Edit Log Report Definition page appears. The options available on the Create Log Report 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.

Deleting Log 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 log report definitions.



NOTE: You can delete only custom log report definitions.

To delete log report definition:

1. Select **Reports > Report Definitions**.

The Report Definitions page appears.

2. Select the log 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 log report definition or **No** to cancel the deletion.

The log report definition is deleted from the main page.

**Related
Documentation**

- [About the Security Report Definitions Page on page 370](#)
- [Creating Log Report Definition on page 373](#)

Editing and Deleting Bandwidth Report Definitions

You can edit and delete bandwidth report definitions. This topic contains the following sections:

- [Editing the Bandwidth Report Definition on page 377](#)
- [Deleting Bandwidth Report Definitions on page 378](#)

Editing the Bandwidth Report Definition

To edit the bandwidth report definition:

1. Select **Reports > Report Definitions**.

The Report Definitions page appears.

2. Select the check box of the log report definition that you want to modify, and click the edit icon.

The Edit Bandwidth Report Definition page appears. The options available on the create bandwidth report 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.

Deleting Bandwidth 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 log report definitions.



NOTE: You can delete only custom bandwidth report definitions.

To delete bandwidth report definition:

1. Select **Reports > Report Definitions**.

The Report Definitions page appears.

2. Select the bandwidth report definition or right click on the report definition that you want to delete and click the X icon.

The Confirm Delete page appears.

3. Click **Yes** to delete the bandwidth report definition or **No** to cancel the deletion.

The bandwidth report definition is deleted from the main page.

Related Documentation

- [About the Security Report Definitions Page on page 370](#)
- [Creating Bandwidth Report Definition on page 375](#)

CHAPTER 23

SD-WAN Reports

- [About the SD-WAN Report Definitions Page on page 379](#)
- [Editing and Deleting SD-WAN Report Definitions on page 380](#)
- [Creating SD-WAN Tenant Performance Report Definition on page 382](#)
- [Creating SD-WAN Site Performance Report Definition on page 384](#)
- [About the SD-WAN Generated Reports Page on page 386](#)

About the SD-WAN Report Definitions Page

To access this page, click **Customer Portal > Reports > Report Definitions > SD-WAN**.

You can use the SD-WAN Report Definitions page to view a list of predefined and custom report definitions. You can use the predefined report definition as-is, or you can create custom report definitions. You can use SD-WAN reports to view the SLA performance of SD-WAN 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.

You must create a report definition to generate a report. You can generate an SLA performance report for all sites in a tenant or for specific sites in a tenant.

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 Definition” on page 382](#)
- Create SD-WAN site performance report definitions. See [“Creating SD-WAN Site Performance Report Definition” on page 384](#)
- Run a report immediately, edit a schedule, edit e-mail recipients, preview a report in PDF, send reports, and clone reports. See [“Performing Different Actions on Reports” on page 371](#)

Field Descriptions

[Table 179 on page 380](#) provides guidelines on using the fields on the SD-WAN Report Definitions page.

Table 179: 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 and Deleting SD-WAN Report Definitions on page 380](#)
- [Creating SD-WAN Tenant Performance Report Definition on page 382](#)
- [Creating SD-WAN Site Performance Report Definition on page 384](#)

Editing and Deleting SD-WAN Report Definitions

You can edit and delete SD-WAN report definitions from the SD-WAN definitions page. This topic has the following sections:

- [Editing the SD-WAN Report Definition on page 381](#)
- [Deleting SD-WAN Report Definitions on page 381](#)

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.

- Related Documentation**
- [About the SD-WAN Report Definitions Page on page 379](#)

Creating SD-WAN Tenant Performance Report Definition

Use this page to create SD-WAN report definitions for all sites in a tenant and generate the report based on the definitions. You can also schedule a report generation and add one or more recipients to whom you want to send the reports.

The SD-WAN tenant performance report includes SLA performance of the following SLA events:

- Top Applications By Bandwidth
- Top Sites Not Meeting SLA
- Top Sites Meeting SLA with Switching
- Sites Meeting SLA without Switching



NOTE: Only users with the MSP Administrator or Tenant Administrator role can create SD-WAN tenant performance report definitions.

To create SD-WAN tenant report definition:

1. Select **Reports > Report Definitions > SD-WAN**.

The SD-WAN Report Definitions page appears.

2. Click **Create > Performance**.

The Create SD-WAN Tenant Performance Report Definition page appears.

3. Complete the configuration according to the guidelines provided in [Table 180 on page 382](#).

4. Click **OK** to save the report definition.

An SD-WAN tenant performance report definition is created and saved in the report definitions page.

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

Table 180: Fields on the Create Tenant Performance Report Definition

Field	Description
General	
Report Name	Enter a unique name for the report definition. You can use a string of alphanumeric characters, colons, periods, dashes, and underscores. No spaces are allowed and the maximum length is 63 characters.

Table 180: Fields on the Create Tenant Performance Report Definition (continued)

Field	Description
Description	Enter a description for the report definition; maximum length is 1024 characters.
Content	
Duration	Specify the duration (custom, last 24 hours, last 7 hours, or last 30 hours) for which the report is generated. When you select the custom option, you must specify the From and To date (in MM/DD/YYYY and HH:MM:SS formats). The predefined options are Last 24 hours, Last 30 hours, and Last 7 hours.
NOTE: The From and To fields are populated only when you select the Custom 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 that you want to retrieve for each section in the report. The value ranges from 1 to 20 and the maximum value is 20.
Report Content	<p>Select the report content that you want to view in the report.</p> <ul style="list-style-type: none"> • Top Applications By Bandwidth—Displays report on top applications by bandwidth. • Top Sites Not Meeting SLA—Displays report on top sites not meeting the SLA performance. • Top Sites Meeting SLA with Switching—Displays report on top sites meeting SLA performance with link switching. • Sites Meeting SLA without Switching—Displays report on sites meeting SLA performance without switching.
Schedule Report	
Add Schedule	<p>Click Add Schedule 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"> • Run now—Select this option to generate the report immediately • 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).
Email Recipients	
Add Email Recipients	<p>Click Add Email Recipients 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"> • Recipients—Select valid e-mail addresses of the recipients. You can select more than one e-mail address. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters. • Comment—Enter any comments, which will be sent in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.

- Related Documentation**
- [Creating SD-WAN Site Performance Report Definition on page 384](#)
 - [About the SD-WAN Report Definitions Page on page 379](#)
 - [Editing and Deleting SD-WAN Report Definitions on page 380](#)

Creating SD-WAN Site Performance Report Definition

Use this page to create SD-WAN report definitions for specific sites in a tenant and generate the report based on the definitions. You can also schedule a report generation and add one or more recipients to whom you want to send the reports.

The SD-WAN site performance report includes SLA performance of the following SLA events:

- Top 10 Applications for site
- Link Utilization for site
- Top Profiles Not Meeting SLA
- Top Profiles Switching Links



NOTE: Only users with the MSP Administrator or 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 181 on page 384](#).
4. Click **OK** to save the report definition.
A report definition is created and saved in the SD-WAN report definitions page.
Alternatively, if you want to discard your changes, click **Cancel**.

Table 181: Fields on the Site Performance Report Definition Page

Field	Description
General	

Table 181: Fields on the Site Performance Report Definition Page (continued)

Field	Description
Report Name	Enter a unique name for the report definition. You can use 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 report definition; maximum length is 1024 characters.
Content	
Duration	Specify the duration (custom, last 24 hours, or last 7 hours) for which the report is generated. When you select the custom option, you must specify the From and To date (in MM/DD/YYYY and HH:MM:SS formats). The predefined options are Last 24 hours, Last 30 hours, and Last 7 hours.
NOTE: The From and To fields are populated only when you select the Custom 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 that you want to retrieve for each section in the report. The value ranges from 1 to 20 and the maximum value is 20.
Sites	Select one or more sites for which you want to generate the report. You can select up to five sites.
Sections	<p>Select the section for which you want to generate the report up to 5 sites in a tenant. By default, all sections are selected.</p> <ul style="list-style-type: none"> • Top 10 Applications and Link Utilization—Displays report on top 10 applications and link utilization for the selected sites. • Top Profiles Not Meeting SLA—Displays report on top SLA profiles not meeting SLA for the selected sites. • Top Profiles Switching Links—Displays report on top SLA profiles switching links for the selected sites.
Schedule	
Add Schedule	<p>Click Add Schedule 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"> • Run now—Select this option to generate the report immediately • 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).
E-Mail	

Table 181: Fields on the Site Performance Report Definition Page (continued)

Field	Description
Add E-Mail Recipients	<p>Click Add Email Recipients 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"> • Recipients—Select valid e-mail addresses of the recipients. You can select more than one e-mail address. • Subject—Enter the subject line for the e-mail that is sent with the generated report. The maximum length is 2048 characters. • Comment—Enter any comments, which will be sent in the body of the e-mail that is sent with the generated report. The maximum length is 2048 characters.

Related Documentation

- [Creating SD-WAN Tenant Performance Report Definition on page 382](#)
- [About the SD-WAN Report Definitions Page on page 379](#)
- [Editing and Deleting SD-WAN Report Definitions on page 380](#)

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 182 on page 386](#) provides guidelines on using the fields on the SD-WAN Generated Reports page.

Table 182: 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.

Table 182: Fields on the SD-WAN Generated Reports Page (continued)

Field	Description
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 on page 369](#)
 - [About the SD-WAN Report Definitions Page on page 379](#)

PART 8

Administration

- [Managing Tenant Users on page 391](#)
- [Licenses on page 397](#)
- [Signature Database on page 399](#)
- [Managing Certificates on page 403](#)
- [Managing Juniper Identity Management Service on page 409](#)

Managing Tenant Users

- [Role-Based Access Control Overview on page 391](#)
- [About the Tenant Users Page on page 392](#)
- [Adding Tenant Users on page 393](#)
- [Editing and Deleting Tenant Users on page 394](#)

Role-Based Access Control Overview

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

[Table 183 on page 391](#) shows MSP and Tenant roles and their access privileges.

Table 183: Roles and Access Privileges

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

Related Documentation

- [About the Tenant Users Page on page 392](#)

About the Tenant Users Page

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

Use the Users page to add, edit, and delete users for a tenant. You can also assign roles to tenant users. The MSP Administrator, MSP Operator, Tenant Administrator, and Tenant Operator can access the Users page for tenants. The MSP Administrator and the MSP Operator can switch from all-tenants scope to specific-tenant scope. To know more about tenant users roles and access permissions, 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 tenant-specific local users that you can add, edit, and delete.
- **Authentication with SSO Server**—The **Add User** page does not display the password field because you can assign a role only to an external user.
- **Authentication and Authorization with SSO Server**—The **Users** page is not displayed because users are externally managed in the single sign-on (SSO) server.

Tasks You Can Perform

The tenant administrator can perform the following tasks from this page:

- Add a tenant user. See [“Adding Tenant Users” on page 393](#).
- Edit and delete a tenant user. See [“Editing and Deleting Tenant Users” on page 394](#).

Field Descriptions

[Table 184 on page 392](#) provides guidelines on using the fields on the Users page.

Table 184: Fields on the Users Page

Field	Description
Username	Username of the tenant user. Example: <i>abc@example.com</i>
First Name	First name of the tenant user.
Last Name	Last name of the tenant user.
Role	Role assigned to the tenant user. Example: Tenant Operator

Table 184: Fields on the Users Page (continued)

Field	Description
Last Login	Date and time of the last login. The format is MM/DD/YYYY HH:MIN. Example: 07/22/2017 20:07

- Related Documentation**
- [Adding Tenant Users on page 393.](#)
 - [Editing and Deleting Tenant Users on page 394.](#)
 - [Switching the Tenant Scope on page 5](#)

Adding Tenant Users

Use this page to add tenant users and assign roles to users. After the tenant administrator adds the user, the user account is created in the Contrail Service Orchestration (CSO) and the user receives an e-mail with the initial login credentials.



NOTE: Users with the Tenant Operator role have read-only access to Customer Portal and APIs, and they cannot add new users.

To add a tenant user:

1. Select **Administration > Users**.
The Users page appears.
2. Click the add icon (+) or click **Add User**.
The Add User page appears.
3. Complete the configuration as described in [Table 185 on page 394](#).
4. Click **OK** to save the changes. If you want to discard the changes, click **Cancel** instead.
The tenant user account is created in CSO.

To enhance the security related to login credentials, an automatically generated password is sent to the e-mail address that you have specified on the Add User page. You are prompted to change the password 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” on page 7](#).

Table 185: Fields on the Add User Page

Field	Description
First Name	Enter the first name as a string of alphanumeric characters and the special characters space, underscore (_), or period (.). The maximum length is 32 characters.
Last Name	Enter the last name as a string of alphanumeric characters and the special characters space, underscore (_), or period (.). The maximum length is 32 characters.
Username (E-mail)	Enter a valid e-mail address in the <i>user@domain</i> format.
Role	<p>Select the role—Tenant Operator (default) or Tenant Administrator—that you want to assign to the user.</p> <ul style="list-style-type: none"> • Tenant Administrator—Users with the Tenant Administrator role have full access to the Customer Portal UI and APIs. They can add one or more users with Tenant Administrator or Tenant Operator roles. • Tenant Operator—Users with the Tenant Operator role have read-only access to the Customer Portal UI and APIs.

Related Documentation

- [About the Tenant Users Page on page 392](#)
- [Editing and Deleting Tenant Users on page 394](#)

Editing and Deleting Tenant Users

You can edit tenant users' information and delete one or more tenant users.



NOTE: Users with the Tenant Operator role have read-only access to the Customer Portal and APIs, and they cannot edit and delete users.

- [Editing Tenant Users on page 394](#)
- [Deleting Tenant Users on page 395](#)

Editing Tenant Users

To modify a tenant user:

1. Select **Administration > Users**.

The Users page appears.

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

The Edit User page appears. The options available on the Add User page are available for editing.



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

3. Update the configuration as needed.
4. Click **OK** to save the changes. If you want to discard your changes, click **Cancel** instead.
The modified tenant user information is saved in CSO.

Deleting Tenant Users

To delete tenant users:

1. Select **Administration > Users**.

The Users page appears.

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

The Confirm Delete page appears.

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

If you click **Yes**, then the user is deleted and the user account is removed from the CSO.

- Related Documentation**
- [About the Tenant Users Page on page 392](#)
 - [Adding Tenant Users on page 393](#)

CHAPTER 25

Licenses

- [About the Licenses Page on page 397](#)

About the Licenses Page

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

You can use the Licenses page to view information about uploaded 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 license. Click the details icon that appears when you hover over the name of an image or click **More > Details**. See [“Viewing Object Details” on page 17](#).
- Show or hide columns about the license. See [“Sorting Objects” on page 17](#).
- Search an object about the license. See [“Searching for Text in an Object Data Table” on page 18](#).

Field Descriptions

[Table 186 on page 397](#) describes the fields on the License Files page.

Table 186: Fields on the License Files Page

Field	Description
License 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

Table 186: Fields on the License Files Page (continued)

Field	Description
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

Related Documentation • *Viewing Object Details*

CHAPTER 26

Signature Database

- [Signature Database Overview on page 399](#)
- [About the Active Database Page on page 400](#)
- [Installing Signatures on page 401](#)

Signature Database Overview

The Application Firewall signature database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies and quality-of-service (QoS) prioritization.

Contrail Service Orchestration (CSO) enables you to download the signature database. During a download, the complete signature database is downloaded, and the download might take some time to complete. You can track the progress of the download by using job details.

All of the downloaded signatures are created as a default project in read-only mode. The configurations that are downloaded are also saved as a default project.

Related Documentation

- [About the Active Database Page on page 400](#)
- [Installing Signatures on page 401](#)

About the Active Database Page

To access this page, select **Administration > Signature Database**. The **Active Database** page appears.

Use the **Active Database** page to download and install the Application Firewall signature database to security devices. This database includes signature definitions of attacks and applications that can be used to identify applications for tracking firewall policies, SD-WAN flows, and QoS prioritization.

Tasks You Can Perform

You can perform the following task from this page:

- Install signatures. See [“Installing Signatures” on page 401](#).

Field Descriptions

The **Active Database** page provides an overall, high-level view of your signature database settings. The **Latest List of Signatures** table provides a search option that you can use to search for the signature you want. [Table 187 on page 400](#) describes the fields on this page.

Table 187: Fields on the Active Database Page

Field	Description
Active Database	
Database Version	Version of signature database.
Publish Date	Date when the signature database was published.
Update Job	Job ID of the last successful download signatures job.
Installed Device Count	Number of devices installed.
Detectors	Version number of the protocol detector currently running on the device.
Action	Install signature database configuration.
Latest List of Signatures	
Database Version	Version of latest signature database.
Publish Date	Date when the signature database was published.
Update Summary	List of updated signature details for the selected database.
Detectors	Version number of the protocol detector currently running on the device.
Action	Full Download—Download the complete signature database; the download might take a while to complete.

- Related Documentation**
- [Signature Database Overview on page 399](#)
 - [Installing Signatures on page 401](#)

Installing Signatures

After the signature database is downloaded, you can install the active database.

To install the signature database:

1. Select **Administration > Signature Database**.
2. Click **Install Signatures**.

The **Install Signatures** page appears.

3. You can view the summary of active signature database version, which will be installed on your device.
4. Click the check box next to the devices on which you want to install the signature database.

You can also search, sort, or filter this information.

5. Select **Run now** to set the signature database to automatically install immediately.
6. Select **Schedule at a later time** to set the signature database to automatically download at the specified time and to take the following actions:
 - a. Choose a date by clicking the date picker icon.
 - b. Enter the time.
 - c. Select the time format from the drop-down list.

7. Click **OK**.

The signature database installation is complete.

- Related Documentation**
- [Signature Database Overview on page 399](#)
 - [About the Active Database Page on page 400](#)

CHAPTER 27

Managing Certificates

- [Certificates Overview on page 403](#)
- [About the Certificates Page on page 403](#)
- [Importing a Certificate on page 405](#)
- [Installing and Uninstalling Certificates on page 407](#)

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 on page 261](#)
- [About the SSL Proxy Profiles Page on page 274](#)

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 188 on page 404](#).
- Import a certificate—Select **More > Import Certificate**. See “Importing a Certificate” on [page 405](#).
- 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 407](#).
- Uninstall a certificate from a site—Select a certificate and then select **More > Uninstall Certificate**. See “Installing and Uninstalling Certificates” on [page 407](#).
- View details about a certificate—Select a certificate and then select **More > Detailed View**. The Detailed View page appears. See [Table 189 on page 404](#) for an explanation of fields on this page.

Field Descriptions

[Table 188 on page 404](#) displays the fields on the Certificates page.

Table 188: Fields on the Certificates Page

Field	Description
Certificate Name	Name of the certificate.
Type	Type of the certificate: <ul style="list-style-type: none">• Root certificate• Trusted certificate
Description	Description of the certificate.

Table 189: Fields on the Detailed View Page

Field	Description
Certificate Name	See Table 188 on page 404 .
Type	See Table 188 on page 404 .
Valid From	Date and time (UTC) from which the certificate is valid.
Valid Upto	Date and time (UTC) until which the certificate is valid.

Table 189: Fields on the Detailed View Page (continued)

Field	Description
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 on page 274](#)

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 190 on page 406](#).



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 190: Import Certificate Settings

Setting	Guideline
Certificate Name	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.
Certificate Type	Select an option to specify whether the certificate that you are importing is a root certificate (Root CA) or a trusted certificate (Trusted CA).
Passphrase	Enter the passphrase to protect the private key or key pair of the Privacy-Enhanced Mail (PEM) certificate file.
Description	Enter a description for the certificate.
Certificate Content	Select an option to specify whether you want to import the certificate content from a file or whether you want to paste the certificate content.
Paste Certificate Content	<p>Depending on the method you choose in the preceding field, do one of the following:</p> <ul style="list-style-type: none"> Import the certificate content directly from a file—Click Browse, and in the File Upload dialog, select a file and click Open. The filename of the file that you uploaded is displayed. Paste the certificate content directly from a file—Copy the certificate content from the file and paste it in the text box. <p>NOTE:</p> <ul style="list-style-type: none"> The following certificate file extensions are supported: .cert, .pem, and .txt. The certificate content must be in the X.509 ASCII format. If the certificate type is Root CA, then the both the certificate content and private key must be specified.

The following is an example of root certificate content.

```
-----BEGIN PRIVATE KEY-----
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123AbcXyz123A
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456DefQrs456A
-----END CERTIFICATE-----
```

- Related Documentation**
- [Installing and Uninstalling Certificates on page 407](#)
 - [Creating SSL Forward Proxy Profiles on page 276](#)

Installing and Uninstalling Certificates

You can install and uninstall certificates from the Certificates page. This topic has the following sections:

- [Installing a Certificate on page 407](#)
- [Uninstalling a Certificate on page 407](#)

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 on page 405](#)

CHAPTER 28

Managing Juniper Identity Management Service

- [Juniper Identity Management Service Overview on page 409](#)
- [About the Identity Management Page on page 411](#)
- [Configuring CSO and JIMS Connection on page 412](#)
- [Configuring JIMS for an SRX Device on page 414](#)

Juniper Identity Management Service Overview

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 on page 410](#)
- [Batch or Periodic Query on page 410](#)
- [IP Address Query on page 410](#)
- [User Mapping Query on page 411](#)

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 on page 411](#)
 - [Configuring CSO and JIMS Connection on page 412](#)
 - [Configuring JIMS for an SRX Device on page 414](#)

About the Identity Management Page

To access this page, select **Administration > Identity Management**.



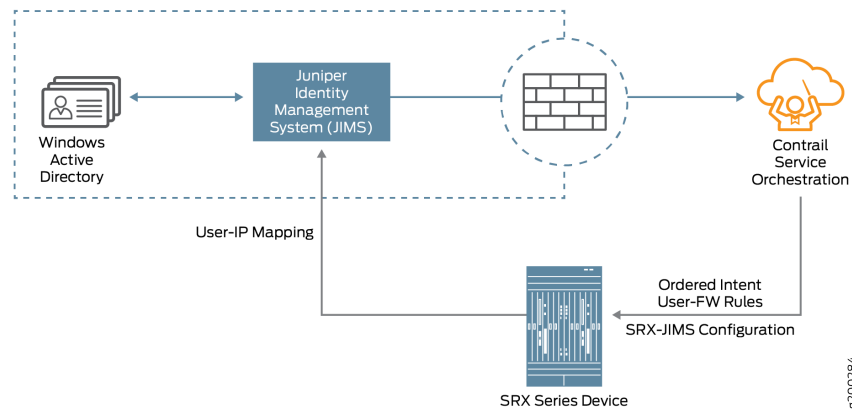
NOTE:

- 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 6 on page 412](#) illustrates the connectivity between, CSO, JIMS, and an SRX Series device.

Figure 6: 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 412.
- Configure the connection between JIMS and an SRX Series device. See [“Configuring JIMS for an SRX Device”](#) on page 414.

Related Documentation

- [Juniper Identity Management Service Overview](#) on page 409
- [Configuring CSO and JIMS Connection](#) on page 412
- [Configuring JIMS for an SRX Device](#) on page 414
- [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**

- [Juniper Identity Management Service Overview on page 409](#)
- [About the Identity Management Page on page 411](#)
- [Configuring JIMS for an SRX Device on page 414](#)

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 Certificate Authority (CA) certificate for 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 191 on page 415](#).

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 191 on page 415](#) provides guidelines on using the fields on the **SRX-to-JIMS Configuration** panel.

Table 191: Fields on the SRX-to-JIMS Configuration Panel

Field	Description
Identity	
IP Address	Enter a valid IPv4 or IPv6 address of the primary JIMS server. SRX Series devices always query the primary JIMS to obtain the user identities.
Secondary Identity	Enable this option to use the secondary JIMS server as a fallback when the primary JIMS server fails. By default, this option is disabled.
Secondary IP Address	Enter a valid IPv4 or IPv6 address of the secondary JIMS server. 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.
Client Credentials	
Client ID	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.
Client Secret	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.

Table 191: Fields on the SRX-to-JIMS Configuration Panel (continued)

Field	Description
Advanced Settings	
Authentication Entry Timeout	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.
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 Add New Address to create a new IP address group, see "Creating Addresses or Address Groups" on page 287.</p>
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 Add New Address to create a new IP address group, see "Creating Addresses or Address Groups" on page 287.</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 on page 409](#)
 - [About the Identity Management Page on page 411](#)
 - [Configuring CSO and JIMS Connection on page 412](#)