



---

# Security Director Application Guide



---

Published: 2015-02-24

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

Copyright © 2015, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

*Security Director Application Guide*  
Copyright © 2015, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	xxxi
	Documentation and Release Notes . . . . .	xxxi
	Documentation Conventions . . . . .	xxxi
	Documentation Feedback . . . . .	xxxiii
	Requesting Technical Support . . . . .	xxxiv
	Self-Help Online Tools and Resources . . . . .	xxxiv
	Opening a Case with JTAC . . . . .	xxxiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Understanding Security Director . . . . .</b>	<b>3</b>
	Security Director Overview . . . . .	3
	Security Director Logging and Reporting Overview . . . . .	6
	Indexing Overview . . . . .	7
	Global Search . . . . .	8
	Security Director User Roles . . . . .	9
	Security Director Dashboard . . . . .	21
<b>Part 2</b>	<b>Configuring Dashboard Monitors</b>	
<b>Chapter 2</b>	<b>Creating and Managing Dashboard Monitors . . . . .</b>	<b>27</b>
	Logging and Reporting Dashboard Overview . . . . .	27
	Understanding Role-Based Access Control for the Dashboard . . . . .	28
	Understanding the Default Dashboard for Logging and Reporting . . . . .	28
	Default Monitors for Default Dashboard . . . . .	28
	Creating a Dashboard Monitor . . . . .	31
	Creating the Event Based Monitor . . . . .	31
	Creating the CPU Utilization Monitor . . . . .	33
	Creating the Memory Utilization Monitor . . . . .	34
	Creating the Device Health Monitor . . . . .	35
	Creating the VPN Status Monitor . . . . .	36
	Managing Dashboard Monitors . . . . .	37
	Using the Dashboard Monitors . . . . .	37

<b>Part 3</b>	<b>Using Event Viewer</b>	
<b>Chapter 3</b>	<b>Understanding Event Viewer Options</b>	<b>41</b>
	Event Viewer Overview	41
	Understanding Role-Based Access Control for the Event Viewer	42
	Using Event Viewer Options	42
	Using the Group By Selection Filter	43
	Using the Column Sets	44
	Selecting Event Viewer Table Columns	45
	Using Time Span	47
	Using the Event Viewer Settings	48
	Using Log View Options	48
	Clearing Filter Settings	49
	Returning to the Previous Page	49
	Creating a Report	49
	Creating an Alert	49
	Creating a Monitor	49
	Using Event Viewer Table Options	51
	Using Event Viewer Table Options in Nongrouped Mode	51
	Creating an Address Object	53
	Using Event Viewer Table Options in Grouped Mode	53
	Example: Using Event Viewer Table Options in Grouped Mode	54
	Using the Detailed Log View	54
	Using the Display Option	56
	Using Event Graphs	57
	Using Comparison Charts	57
	Using the Show Logs Option to Navigate from the Event Viewer to the Policies Page	58
	Using the Show Logs Option to Navigate from Policies to Logs on the Event Viewer Page	59
	Creating an Exempt Rule	59
<b>Chapter 4</b>	<b>Creating and Managing Event Viewer Filters</b>	<b>61</b>
	Filter Management Overview	61
	Understanding Role-Based Access Control for Filter Management	62
	Understanding Advanced Filter Options	62
	Creating an Event Viewer Filter Using Advanced Filter Options	66
	Managing Filters in the Event Viewer	67
	Using Load Filter Selections	68
	Using the Filter Manager	68
	Searching Filters in the Filter Manager	69
	Editing Event Viewer Filters	70
	Saving an Event Viewer Filter	70
	Deleting an Event Viewer Filter	70
	Filtering on Multiple String Values	71

<b>Part 4</b>	<b>Configuring Alerts</b>	
<b>Chapter 5</b>	<b>Creating and Managing Alerts</b>	<b>75</b>
	Alerts and Notifications Overview	75
	Understanding Role-Based Access Control for the Alerts and Alert	
	Definitions	75
	Generating an Alert	76
	Searching Alerts	77
	Deleting an Alert	77
<b>Chapter 6</b>	<b>Creating and Managing Alert Definitions</b>	<b>79</b>
	Using Alert Definitions	79
	Creating Alert Definitions	80
	Managing Alert Definitions	82
	Deleting Alert Definitions	82
	Editing Alert Definitions	82
	Searching Alert Definitions	82
	Hiding or Displaying Alert Definitions Using Quick View	82
<b>Part 5</b>	<b>Configuring Reports</b>	
<b>Chapter 7</b>	<b>Creating and Managing Reports</b>	<b>87</b>
	Reports Overview	87
	Understanding Role-Based Access Control for Reports	87
	Creating a Log Report Definition	88
	Using Reports	92
	Creating a Policy Analysis Report Definition	94
	Managing Reports	96
	Editing a Report	97
	Deleting a Report	97
	Duplicating a Report	98
	Adding Information to All Reports	98
	Performing Different Actions on Reports	99
<b>Part 6</b>	<b>Configuring Security Objects</b>	
<b>Chapter 8</b>	<b>Overview</b>	<b>103</b>
	Object Builder Overview	103
	Domain RBAC Overview	104
	Creation or Addition of an Object or a Service	104
	Reading or Viewing an Object or a Service	105
	Updating or Modifying an Object or a Service	105
	Deleting an Object or a Service	105
	Referencing Objects	105
	Moving Objects Across Domains	106
	Naming the Objects in a Domain	106
	Predefined Objects	106

<b>Chapter 9</b>	<b>Creating and Managing Services and Service Groups . . . . .</b>	<b>107</b>
	Service and Service Group Overview . . . . .	107
	Creating Services . . . . .	108
	Managing Services . . . . .	112
	Modifying a Service . . . . .	112
	Deleting a Service . . . . .	113
	Cloning a Service . . . . .	113
	Find Duplicate Service Objects . . . . .	113
	Find Service Usage . . . . .	114
	Replace Services . . . . .	115
	Show Unused Services . . . . .	117
	Delete All Unused Services . . . . .	117
	Creating Service Groups . . . . .	118
	Managing Service Groups . . . . .	119
	Modifying a Service Group . . . . .	119
	Deleting a Service Group . . . . .	119
	Cloning a Service Group . . . . .	120
<b>Chapter 10</b>	<b>Creating and Managing Addresses and Address Groups . . . . .</b>	<b>121</b>
	Address and Address Groups Overview . . . . .	121
	Global Address Book Overview . . . . .	121
	Differences Between Global and Zone-Based Address Books . . . . .	122
	Nested Address Group Support . . . . .	122
	Mixed-Version Support . . . . .	122
	Migrating from Zone to Global Addressing . . . . .	123
	Example: Configuring Address Book Entries in Global Address Book . . . . .	123
	Creating Addresses . . . . .	124
	Managing Addresses . . . . .	126
	Modifying an Address . . . . .	127
	Deleting an Address . . . . .	128
	Cloning an Address . . . . .	128
	Exporting Addresses . . . . .	128
	Importing Addresses . . . . .	129
	Find Duplicate Address Objects . . . . .	129
	Find Address Usage . . . . .	131
	Replace Addresses . . . . .	132
	Show Unused Addresses . . . . .	134
	Delete All Unused Addresses . . . . .	134
	Assigning Addresses to Domains . . . . .	135
	Creating Address Groups . . . . .	136
	Managing Address Groups . . . . .	137
	Modifying an Address Group . . . . .	137
	Deleting an Address Group . . . . .	138
	Cloning an Address Group . . . . .	138

<b>Chapter 11</b>	<b>Creating and Managing Zone Sets</b>	<b>139</b>
	Creating a Zone Set	139
	Managing Zone Sets	140
	Modifying a Zone Set	140
	Deleting a Zone Set	141
	Cloning a Zone set	141
	Showing Duplicate Zone Sets	141
	Finding Zone Set Usage	141
	Showing Unused Zone Sets	142
	Deleting All Unused Zone Sets	142
<b>Chapter 12</b>	<b>Creating and Managing Variables</b>	<b>143</b>
	Creating Variable Definitions	143
	Managing Variable Definitions	147
	Deleting Variable Definitions	147
	Modifying Variable Definitions	147
	Cloning Variable Definitions	148
<b>Part 7</b>	<b>Configuring Firewall Policies</b>	
<b>Chapter 13</b>	<b>Creating and Managing Firewall Policies</b>	<b>151</b>
	Firewall Policies Overview	151
	Rule Base Overview	153
	Example: UnManaging a Previously Managed Rule Base	153
	Policy Analysis	154
	Custom Column Overview	155
	Custom Column Data Search	155
	Multiple Group Policy Membership Overview	155
	General Rules About Priority and Precedence	156
	Example: New Precedence of a Policy Set to the Same Precedence as an Existing Policy	156
	Sorting of Firewall Policy Left Pane	156
	Creating Firewall Policies	159
	Unlocking Locked Policies	174
	Inline Creation of Objects in Policy	176
	Adding Rules to a Firewall Policy	180
	Ordering the Rules in a Firewall Policy	185
	Policy Priority Precedence Setting	188
	Tracking the Utility Rate of Security Firewall Policies	190
	Publishing Firewall Policies	194
	Managing Firewall Policies	201
	Modifying Firewall Policies	202
	Comparing Firewall Policies	203
	Deleting Firewall Policies	205
	Adding Rules to a Firewall Policy	206
	Cloning Firewall Policies	206
	Promoting a Firewall Policy	207
	Exporting a Firewall Policy	207
	Policy Versioning	208

	Managing Policy Versioning . . . . .	210
	Deleting Rules in a Firewall Policy . . . . .	215
	Cloning a Rule in a Firewall Policy . . . . .	216
	Grouping Rules in a Firewall Policy . . . . .	216
	Enabling/Disabling Rules in a Firewall Policy . . . . .	216
	Expanding/Collapsing All Rules in a Firewall Policy . . . . .	217
	Cutting/Copying and Pasting Rules or Rule Groups in a Firewall Policy . . . . .	217
	Assigning Devices to a Firewall Policy . . . . .	218
	Firewall Policy Rule Hits . . . . .	219
	Generating the Policy Analysis Report . . . . .	221
	Deleting Devices from a Firewall Policy . . . . .	223
	Rule Operations on the Filtered Rules . . . . .	223
	Managing Custom Column Data . . . . .	225
	Modifying Custom Columns Definitions . . . . .	225
	Deleting a Custom Columns Definition . . . . .	226
	Exporting a Custom Columns Definition . . . . .	226
	Showing Firewall Policy for a Corresponding Log . . . . .	226
<b>Chapter 14</b>	<b>Creating and Managing Application Signatures . . . . .</b>	<b>229</b>
	Creating Application Signatures . . . . .	230
	Managing Application Signatures . . . . .	233
	Filtering Application Signatures . . . . .	233
	Modifying Application Signatures . . . . .	234
	Modifying Application Signature Groups . . . . .	234
	Deleting Application Signatures . . . . .	234
	Cloning Application Signatures . . . . .	235
	Cloning Application Signature Groups . . . . .	235
	Viewing Application Signature Details . . . . .	235
<b>Chapter 15</b>	<b>Creating and Managing Schedulers . . . . .</b>	<b>237</b>
	Scheduler Overview . . . . .	237
	Creating a Scheduler . . . . .	238
	Managing Scheduler . . . . .	240
	Modifying a Scheduler . . . . .	240
	Deleting a Scheduler . . . . .	240
	Find Scheduler Usage . . . . .	241
	Show Unused Schedulers . . . . .	241
<b>Chapter 16</b>	<b>Creating and Managing Policy Profiles . . . . .</b>	<b>243</b>
	Security Policy Profiles Overview . . . . .	243
	Creating Policy Profiles . . . . .	244
	Managing Policy Profiles . . . . .	248
	Deleting Policy Profiles . . . . .	248
	Modifying Policy Profiles . . . . .	248
	Cloning Policy Profiles . . . . .	249
	Creating Template Definitions . . . . .	249
	Managing Template Definitions . . . . .	250
	Deleting Template Definitions . . . . .	251
	Modifying Template Definitions . . . . .	251
	Creating Templates . . . . .	252

	Managing Templates . . . . .	253
	Deleting Templates . . . . .	253
	Modifying Templates . . . . .	253
<b>Part 8</b>	<b>Configuring VPNs</b>	
<b>Chapter 17</b>	<b>Creating and Managing IPsec VPNs . . . . .</b>	<b>257</b>
	IPsec VPN Overview . . . . .	257
	Creating IPsec VPNs . . . . .	259
	Creating IPsec VPNs . . . . .	260
	Importing an Existing VPN Environment of SRX Series Devices . . . . .	273
	Publishing IPsec VPNs . . . . .	281
	Managing IPsec VPNs . . . . .	282
	Modifying IPsec VPNs . . . . .	283
	Modifying Endpoint Settings in a VPN . . . . .	284
	Deleting IPsec VPNs . . . . .	285
<b>Chapter 18</b>	<b>Creating and Managing Extranet Devices . . . . .</b>	<b>287</b>
	Creating Extranet Devices . . . . .	287
	Managing Extranet Devices . . . . .	288
	Modifying an Extranet Device . . . . .	288
	Deleting an Extranet Device . . . . .	288
	Cloning an Extranet Device . . . . .	289
<b>Chapter 19</b>	<b>Creating and Managing VPN Profiles . . . . .</b>	<b>291</b>
	VPN Profiles Overview . . . . .	291
	Creating VPN Profiles . . . . .	292
	Managing VPN Profiles . . . . .	297
	Deleting VPN Profiles . . . . .	297
	Modifying VPN Profiles . . . . .	297
	Cloning VPN Profiles . . . . .	298
<b>Part 9</b>	<b>Using Security Intelligence Solution</b>	
<b>Chapter 20</b>	<b>Understanding Security Intelligence Solution . . . . .</b>	<b>301</b>
	Security Intelligence Overview . . . . .	301
<b>Chapter 21</b>	<b>Creating and Managing Spotlight Secure Connectors . . . . .</b>	<b>303</b>
	Creating a Spotlight Secure Connector . . . . .	303
	Managing Spotlight Secure Connectors . . . . .	305
	Adding Spotlight Secure Connector Global Settings . . . . .	305
	Uploading Trusted Server CAs . . . . .	307
	Associating Devices to Spotlight Secure Connectors . . . . .	307
	Updating Spotlight Secure Connector Configuration . . . . .	310
	Deleting Spotlight Secure Connectors . . . . .	310
	Viewing Spotlight Secure Connector Feed Status . . . . .	310
	Upgrading Spotlight Secure Connector Software or Package . . . . .	311

<b>Chapter 22</b>	<b>Creating and Managing Information Sources . . . . .</b>	<b>313</b>
	Creating an Information Source . . . . .	313
	Managing Information Sources . . . . .	315
	Modifying an Information Source . . . . .	315
	Deleting an Information Source . . . . .	316
	Updating Feeds to Connectors . . . . .	316
<b>Chapter 23</b>	<b>Creating and Managing Security Intelligence Profiles . . . . .</b>	<b>317</b>
	Creating Security Intelligence Profiles . . . . .	317
	Managing Security Intelligence Profiles . . . . .	320
	Modifying a Security Intelligence Profile . . . . .	320
	Deleting a Security Intelligence Profile . . . . .	321
	Modifying a Global White List or Global Black List . . . . .	321
<b>Chapter 24</b>	<b>Creating and Managing Security Intelligence Policies . . . . .</b>	<b>323</b>
	Creating Security Intelligence Policies . . . . .	323
	Managing Security Intelligence Policies . . . . .	324
	Modifying a Security Intelligence Policy . . . . .	325
	Deleting a Security Intelligence Policy . . . . .	325
<b>Chapter 25</b>	<b>Creating and Managing Dynamic Address Groups . . . . .</b>	<b>327</b>
	Creating Dynamic Address Groups . . . . .	327
	Managing Dynamic Address Groups . . . . .	328
	Modifying a Dynamic Address Group . . . . .	328
	Deleting an Address from a Dynamic Address Group . . . . .	329
<b>Chapter 26</b>	<b>Creating a Backup of the Connector Configuration . . . . .</b>	<b>331</b>
	Creating a Backup or Restoring the Connector Settings . . . . .	331
<b>Part 10</b>	<b>Configuring UTM Policies</b>	
<b>Chapter 27</b>	<b>Creating and Managing UTM Policies . . . . .</b>	<b>335</b>
	UTM Overview . . . . .	335
	Creating a UTM Policy Using UTM Wizard . . . . .	336
	Creating a Web Filtering Profile . . . . .	339
	Creating an Antivirus Profile . . . . .	341
	Creating an Antispam Profile . . . . .	343
	Creating a Content Filtering Profile . . . . .	345
	Managing UTM Policies . . . . .	346
	Modifying a UTM Policy . . . . .	347
	Deleting a UTM Policy . . . . .	347
	Cloning a UTM Policy . . . . .	347
	Finding UTM Policy Usage . . . . .	347
	Showing Unused UTM Policies . . . . .	348
	Deleting All Unused UTM Policies . . . . .	348
<b>Chapter 28</b>	<b>Creating and Managing Antispam Profiles . . . . .</b>	<b>349</b>
	Creating an Antispam Profile . . . . .	349
	Managing Antispam Profiles . . . . .	351
	Modifying an Antispam Profile . . . . .	351
	Deleting an Antispam Profile . . . . .	351

	Cloning an Antispam Profile . . . . .	352
	Finding Antispam Profile Usage . . . . .	352
	Showing Unused Antispam Profiles . . . . .	352
	Deleting All Unused Antispam Profiles . . . . .	352
<b>Chapter 29</b>	<b>Creating and Managing Antivirus Profiles . . . . .</b>	<b>355</b>
	Creating an Antivirus Profile . . . . .	355
	Managing Antivirus Profiles . . . . .	359
	Modifying an Antivirus Profile . . . . .	360
	Deleting an Antivirus Profile . . . . .	360
	Cloning an Antivirus Profile . . . . .	360
	Finding Antivirus Profile Usage . . . . .	361
	Showing Unused Antivirus Profiles . . . . .	361
	Deleting All Unused Antivirus Profiles . . . . .	361
<b>Chapter 30</b>	<b>Creating and Managing Content Filtering Profiles . . . . .</b>	<b>363</b>
	Creating a Content Filtering Profile . . . . .	363
	Managing Content Filtering Profiles . . . . .	367
	Modifying the Content Filtering Profile . . . . .	367
	Deleting the Content Filtering Profile . . . . .	367
	Cloning the Content Filtering Profile . . . . .	368
	Finding Content Filtering Profile Usage . . . . .	368
	Showing Unused Content Filtering Profiles . . . . .	368
	Deleting All Unused Content Filtering Profiles . . . . .	368
<b>Chapter 31</b>	<b>Creating and Managing Web Filtering Profiles . . . . .</b>	<b>371</b>
	Creating a Web Filtering Profile . . . . .	371
	Managing Web Filtering Profiles . . . . .	379
	Modifying a Web Filtering Profile . . . . .	379
	Deleting a Web Filtering Profile . . . . .	380
	Cloning a Web Filtering Profile . . . . .	380
	Finding Web Filtering Profile Usage . . . . .	380
	Showing Unused Web Filtering Profiles . . . . .	380
	Deleting All Unused Web Filtering Profiles . . . . .	381
<b>Chapter 32</b>	<b>Creating and Managing URL Patterns . . . . .</b>	<b>383</b>
	Creating a URL Pattern . . . . .	383
	Managing URL Patterns . . . . .	385
	Modifying a URL Pattern . . . . .	385
	Deleting a URL Pattern . . . . .	386
	Cloning a URL Pattern . . . . .	386
	Finding URL Pattern Usage . . . . .	386
	Showing Unused URL Patterns . . . . .	386
	Delete All Unused URL Patterns . . . . .	387
<b>Chapter 33</b>	<b>Creating and Managing Custom URL Category Lists . . . . .</b>	<b>389</b>
	Creating a Custom URL Category List . . . . .	389
	Managing Custom URL Category Lists . . . . .	391
	Modifying a Custom URL Category List . . . . .	391
	Deleting a Custom URL Category List . . . . .	391
	Cloning a Custom URL Category List . . . . .	392

	Finding Custom URL Category List Usage . . . . .	392
	Showing Unused Custom URL Category Lists . . . . .	392
	Deleting All Unused Custom URL Category Lists . . . . .	392
<b>Chapter 34</b>	<b>Creating and Managing UTM Device Profiles . . . . .</b>	<b>395</b>
	Creating a UTM Device Profile . . . . .	395
	Managing Device Profiles . . . . .	398
	Modifying a UTM Device Profile . . . . .	399
	Deleting a UTM Device Profile . . . . .	399
	Cloning a UTM Device Profile . . . . .	399
	Showing Unused UTM Device Profiles . . . . .	399
	Deleting All Unused UTM Device Profiles . . . . .	400
<b>Part 11</b>	<b>Configuring NAT Policies</b>	
<b>Chapter 35</b>	<b>Understanding NAT . . . . .</b>	<b>403</b>
	NAT Overview . . . . .	403
	Global Address Book Overview . . . . .	406
	Differences Between Global and Zone-Based Address Books . . . . .	406
<b>Chapter 36</b>	<b>Creating and Managing NAT Policies . . . . .</b>	<b>409</b>
	Creating NAT Policies . . . . .	409
	Unlocking Locked Policies . . . . .	423
	Ordering the Rules in a NAT Policy . . . . .	424
	Adding Rules to a NAT Policy . . . . .	427
	Publishing NAT Policies . . . . .	433
	Managing NAT Policies . . . . .	436
	Modifying NAT Policies . . . . .	437
	Deleting NAT Policies . . . . .	437
	Cloning NAT Policies . . . . .	438
	Exporting a NAT Policy . . . . .	438
	Configuring NAT Rule Sets . . . . .	438
	NAT Policy Versioning . . . . .	439
	Managing NAT Policy Versioning . . . . .	440
	Deleting Rules in a NAT Policy . . . . .	445
	Grouping Rules in a NAT Policy . . . . .	445
	Enabling/Disabling Rules in a NAT Policy . . . . .	445
	Expanding/Collapsing All Rules in a NAT Policy . . . . .	446
	Cutting/Copying and Pasting Rules or Rule Groups in a NAT Policy . . . . .	446
	Assigning Devices to a NAT Policy . . . . .	448
	Deleting Devices from a NAT Policy . . . . .	448
	Rule Operations on the Filtered Rules . . . . .	449
	Showing NAT Policy for a Corresponding Log . . . . .	450
	Viewing Logs Generated by the NAT Rule . . . . .	452
<b>Chapter 37</b>	<b>Creating and Managing NAT Pools . . . . .</b>	<b>455</b>
	Creating NAT Pools . . . . .	456
	Managing NAT Pools . . . . .	459
	Deleting NAT Pools . . . . .	459
	Modifying NAT Pools . . . . .	459

	Cloning NAT Pools . . . . .	460
	Show Duplicate NAT Pools . . . . .	460
	Find NAT Pool Usage . . . . .	462
	Replace Addresses . . . . .	463
	Show Unused NAT Pools . . . . .	464
	Delete All Unused NAT Pools . . . . .	465
<b>Chapter 38</b>	<b>Creating and Managing Port Sets . . . . .</b>	<b>467</b>
	Creating a Port Set . . . . .	467
	Managing Port Sets . . . . .	468
	Modifying a Port Set . . . . .	468
	Deleting a Port Set . . . . .	469
	Cloning a Port Set . . . . .	469
	Showing Duplicate Port Sets . . . . .	469
	Finding a Port Set Usage . . . . .	469
	Showing Unused Port Sets . . . . .	470
	Deleting All Unused Port Sets . . . . .	470
	Assigning Domains to Port Sets . . . . .	470
<b>Part 12</b>	<b>Using IDP Signature Database Downloads</b>	
<b>Chapter 39</b>	<b>Downloading and Installing Signature Database . . . . .</b>	<b>473</b>
	Downloading the Signature Database . . . . .	473
	Installing the Signature Database . . . . .	475
<b>Part 13</b>	<b>Using IPS Management</b>	
<b>Chapter 40</b>	<b>Creating and Managing IPS Signatures and Signature Sets . . . . .</b>	<b>481</b>
	IPS Management Overview . . . . .	481
	Creating IPS Signatures . . . . .	482
	Managing IPS Signatures . . . . .	484
	Filtering IPS Signatures . . . . .	484
	Modifying IPS Signatures . . . . .	485
	Deleting IPS Signatures . . . . .	485
	Cloning IPS Signatures . . . . .	485
	Creating Static Signature Groups . . . . .	486
	Creating Dynamic Signature Groups . . . . .	486
	Creating IPS Signature Sets . . . . .	487
	Creating a Policy Template . . . . .	487
	Adding Rules to a Policy Template . . . . .	488
	Managing Policy Templates . . . . .	489
	Deleting Policy Templates . . . . .	489
	Cloning Policy Templates . . . . .	489
	Enable or Disable Rules in a Policy Templates . . . . .	490
	Grouping Rules in a Policy Templates . . . . .	490
	Expanding/Collapsing All Rules in a Policy Template . . . . .	491
	Cutting/Copying And Pasting Rules or Rule Groups in a Policy Template . . . . .	491
	Adding Rules to a Policy Template . . . . .	492

<b>Chapter 41</b>	<b>Creating and Managing IPS Policies . . . . .</b>	<b>493</b>
	Creating IPS Policies . . . . .	494
	Managing Policy Locks . . . . .	503
	Ordering the Rules in a IPS Policy . . . . .	504
	Adding Rules to an IPS Policy . . . . .	507
	Publishing IPS Policies . . . . .	509
	Managing IPS Policies . . . . .	513
	Deleting IPS Policy Rules . . . . .	514
	Enabling or Disabling Rules in an IPS Policy . . . . .	514
	Cloning a Rule in an IPS Policy . . . . .	514
	Grouping Rules in an IPS Policy . . . . .	515
	Expanding/Collapsing All Rules in an IPS Policy . . . . .	515
	Cutting/Copying And Pasting Rules or Rule Groups in an IPS Policy . . . . .	515
	Adding Rules to an IPS Policy . . . . .	516
	Rule Operations on the Filtered Rules . . . . .	516
 <b>Part 14</b>	 <b>Configuring Network Devices</b>	
<b>Chapter 42</b>	<b>Creating and Managing Security Zones . . . . .</b>	<b>521</b>
	Creating a Security Zone for a Device . . . . .	521
	Managing Security Zones . . . . .	524
	Modifying a Security Zone . . . . .	524
	Deleting a Security Zone . . . . .	525
	Deactivating a Security Zone . . . . .	526
	Activating a Security Zone . . . . .	526
 <b>Chapter 43</b>	 <b>Creating and Managing Screens . . . . .</b>	 <b>527</b>
	Creating a Screen for a Device . . . . .	527
	Managing Screens . . . . .	531
	Modifying a Screen . . . . .	531
	Deleting a Screen . . . . .	532
	Deactivating a Screen . . . . .	533
	Activating a Screen . . . . .	533
 <b>Chapter 44</b>	 <b>Configuring Security Logs . . . . .</b>	 <b>535</b>
	Creating Security Logs . . . . .	535
 <b>Chapter 45</b>	 <b>Creating and Managing Static Routes . . . . .</b>	 <b>541</b>
	Creating a Static Route for a Device . . . . .	541
	Managing Static Routes . . . . .	545
	Modifying a Static Route . . . . .	545
	Deleting a Static Route . . . . .	546
	Deactivating a Static Route . . . . .	547
	Activating a Static Route . . . . .	547
 <b>Chapter 46</b>	 <b>Creating and Managing Routing Instances . . . . .</b>	 <b>549</b>
	Creating a Routing Instance for a Device . . . . .	549
	Managing Routing Instances . . . . .	552
	Modifying a Routing Instance . . . . .	552
	Deleting a Routing Instance . . . . .	553

	Deactivating a Routing Instance . . . . .	554
	Activating a Routing Instance . . . . .	554
<b>Chapter 47</b>	<b>Managing Physical Interfaces and Syslog . . . . .</b>	<b>555</b>
	Managing Physical Interfaces . . . . .	555
	Modifying a Syslog . . . . .	560
<b>Chapter 48</b>	<b>Updating Security Director Devices . . . . .</b>	<b>565</b>
	Security Director Devices Workspace Overview . . . . .	565
	Updating Devices with Pending Services . . . . .	567
	Importing Firewall, NAT, and IPS Policies from a Device to Security Director . . .	573
	NSM Migration . . . . .	580
	Managing Consolidated Configurations . . . . .	586
	Generating a Consolidated Configuration . . . . .	586
	Managing Commit Confirm . . . . .	587
<b>Part 2</b>	<b>Index</b>	
	Index . . . . .	593



# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Understanding Security Director</b>	<b>3</b>
	Figure 1: Security Director Homepage	4
	Figure 2: Junos OS Schema Mismatch Warning Message	5
	Figure 3: Indexing Status Message	7
	Figure 4: Global Search Results	8
	Figure 5: Object Count Gadget	23
	Figure 6: Address Types Gadget	23
	Figure 7: Security Director Dashboard with Logging and Reporting	24
<b>Part 2</b>	<b>Configuring Dashboard Monitors</b>	
<b>Chapter 2</b>	<b>Creating and Managing Dashboard Monitors</b>	<b>27</b>
	Figure 8: Security Director Logging and Reporting Dashboard	27
<b>Part 6</b>	<b>Configuring Security Objects</b>	
<b>Chapter 8</b>	<b>Overview</b>	<b>103</b>
	Figure 9: Variable Objects: Concurrent Edit Save Warning Message	104
<b>Chapter 9</b>	<b>Creating and Managing Services and Service Groups</b>	<b>107</b>
	Figure 10: Create Service: Basic View Page	109
	Figure 11: Create Service: Advanced Settings Page	110
	Figure 12: Window Showing Duplicate Services	114
	Figure 13: Window Showing Service Usage	115
	Figure 14: Replace Services Window	116
	Figure 15: Service: Confirm Replace Warning Message	116
	Figure 16: Service Replace Successful Message	117
	Figure 17: Create Service Group Page	118
<b>Chapter 10</b>	<b>Creating and Managing Addresses and Address Groups</b>	<b>121</b>
	Figure 18: Create Address Page	125
	Figure 19: Page Showing Duplicate Address Objects	129
	Figure 20: Merge Address Page	130
	Figure 21: Merge Operation Confirmation Message	130
	Figure 22: Duplicate Objects Delete Confirmation Page	131
	Figure 23: Window Showing Address Usage	132
	Figure 24: Replace Addresses Window	133
	Figure 25: Address: Confirm Replace Warning Message	133
	Figure 26: Address Replace Success Message	134
	Figure 27: Addresses-Assign to Domain	135

	Figure 28: Create Address Group Page . . . . .	136
<b>Chapter 11</b>	<b>Creating and Managing Zone Sets . . . . .</b>	<b>139</b>
	Figure 29: Create Zone Set . . . . .	139
<b>Chapter 12</b>	<b>Creating and Managing Variables . . . . .</b>	<b>143</b>
	Figure 30: Create Polymorphic Object Page . . . . .	144
	Figure 31: Inline Address Group Creation for a Polymorphic Object . . . . .	145
	Figure 32: Create Address Object-Inline Address Group Creation Page . . . . .	146
<b>Part 7</b>	<b>Configuring Firewall Policies</b>	
<b>Chapter 13</b>	<b>Creating and Managing Firewall Policies . . . . .</b>	<b>151</b>
	Figure 33: Custom Column Data Search . . . . .	155
	Figure 34: Sorting Order in the Firewall Policy Left Pane . . . . .	156
	Figure 35: Policy View Setting . . . . .	158
	Figure 36: Firewall Policy Tabular View . . . . .	159
	Figure 37: Create Firewall Policy . . . . .	160
	Figure 38: Turning an IPS Policy On or Off . . . . .	162
	Figure 39: Policy with Error Saved as Draft . . . . .	163
	Figure 40: Lock Failure Error Message for the Second User . . . . .	164
	Figure 41: Inactivity Timeout Error . . . . .	164
	Figure 42: Policy Lock Expired Message . . . . .	164
	Figure 43: Save the Edited Policy with a Different Name . . . . .	165
	Figure 44: Unsaved Changes Warning Message . . . . .	165
	Figure 45: Policy Unlock by Admin Message . . . . .	165
	Figure 46: Policy Lock Release Message . . . . .	166
	Figure 47: Creating Custom Column . . . . .	167
	Figure 48: Creating Custom Column Page . . . . .	167
	Figure 49: Create Custom Column Confirm Page . . . . .	167
	Figure 50: Source Identity Page . . . . .	168
	Figure 51: Select Devices Page . . . . .	169
	Figure 52: Tooltip Showing Object Information . . . . .	170
	Figure 53: Advanced Search Dialog for Firewall Policies . . . . .	171
	Figure 54: Firewall Policy: Manage Policy Locks . . . . .	175
	Figure 55: Modify Security Director Settings . . . . .	175
	Figure 56: Inline Address Object Creation in the Source Address Window . . . . .	176
	Figure 57: Inline Address Object Create Page . . . . .	177
	Figure 58: Address Selector Page Showing the New Inline Object . . . . .	178
	Figure 59: Inline Address Group Creation . . . . .	178
	Figure 60: Inline Service Object Creation in the Service List . . . . .	179
	Figure 61: Inline Service Object Creation Page . . . . .	179
	Figure 62: Service Selector Page Showing the New Object . . . . .	180
	Figure 63: Tunnel Option for Device Rule . . . . .	182
	Figure 64: TCP-Session Options . . . . .	183
	Figure 65: Concurrent Policy Edit Error Message . . . . .	184
	Figure 66: Firewall Policy Landing Page . . . . .	186
	Figure 67: Firewall Policy-Drag and Drop Objects Window . . . . .	186
	Figure 68: Policy: Priority And Precedence Page . . . . .	188
	Figure 69: Setting Priority And Precedence Value Page . . . . .	189

	Figure 70: Firewall Policy with Rule Hits . . . . .	190
	Figure 71: Firewall Policy Hit Levels . . . . .	192
	Figure 72: Hits Per Device . . . . .	193
	Figure 73: Hit Level Filter . . . . .	193
	Figure 74: Policy Publish Page . . . . .	195
	Figure 75: Devices on Which the Policies Will Be Published . . . . .	196
	Figure 76: Policy Publish-CLI Configuration . . . . .	196
	Figure 77: Device Validation Warning Message . . . . .	197
	Figure 78: Policy Publish-LSYS Device CLI Configuration . . . . .	197
	Figure 79: Policy Publish-XML Configuration . . . . .	198
	Figure 80: Modify Policy Page . . . . .	202
	Figure 81: Compare Policy . . . . .	204
	Figure 82: Compare Policy Result . . . . .	205
	Figure 83: Clone Policy Page . . . . .	206
	Figure 84: Promote Policy Page . . . . .	207
	Figure 85: Snapshot Policy Window . . . . .	209
	Figure 86: Modify Security Director Settings . . . . .	210
	Figure 87: Rollback Service Summary Page . . . . .	211
	Figure 88: Object Conflict Resolution Window . . . . .	211
	Figure 89: Rollback OCR Summary Report . . . . .	212
	Figure 90: Rollback Snapshot Policy Report . . . . .	212
	Figure 91: Manage Versions Window . . . . .	213
	Figure 92: Compare Versions Window . . . . .	213
	Figure 93: Compare Versions-Results Window . . . . .	214
	Figure 94: Confirm Delete Operation Message . . . . .	215
	Figure 95: Expand All Warning Message for More Than 1,000 Rules . . . . .	217
	Figure 96: Nested Rule Group Paste Operation Warning Message . . . . .	218
	Figure 97: Variable Objects Rule Paste Error . . . . .	218
	Figure 98: Reset Hit Confirm . . . . .	220
	Figure 99: Probe Latest Hits Job Details . . . . .	221
	Figure 100: Policy Analysis Progress Bar . . . . .	222
	Figure 101: Policy Analysis Report . . . . .	222
	Figure 102: Policy Analysis Report-Shadowed . . . . .	222
	Figure 103: Policy Analysis-Redundant . . . . .	223
	Figure 104: Modifying a Custom Column . . . . .	226
	Figure 105: Deleting a Custom Column . . . . .	226
	Figure 106: Jumping to the Current Policy Rule . . . . .	227
<b>Chapter 14</b>	<b>Creating and Managing Application Signatures . . . . .</b>	<b>229</b>
	Figure 107: Application Signatures Page . . . . .	230
	Figure 108: Create Application Signature . . . . .	231
	Figure 109: Application Signature Details . . . . .	236
<b>Chapter 15</b>	<b>Creating and Managing Schedulers . . . . .</b>	<b>237</b>
	Figure 110: Scheduler Main Page . . . . .	238
	Figure 111: Create Scheduler . . . . .	239
	Figure 112: Scheduler Find Usage Window . . . . .	241
<b>Chapter 16</b>	<b>Creating and Managing Policy Profiles . . . . .</b>	<b>243</b>
	Figure 113: New Policy Profile Page . . . . .	245

	Figure 114: Create Policy Profile-Advanced Settings . . . . .	247
	Figure 115: Create Template Definition Page . . . . .	250
	Figure 116: Create Template Page . . . . .	252
<b>Part 8</b>	<b>Configuring VPNs</b>	
<b>Chapter 17</b>	<b>Creating and Managing IPsec VPNs . . . . .</b>	<b>257</b>
	Figure 117: VPN Landing Page . . . . .	260
	Figure 118: Create VPN Page . . . . .	260
	Figure 119: VPN Profile Tooltip . . . . .	262
	Figure 120: Create VPN: Add as Endpoint Page . . . . .	263
	Figure 121: Create VPN: Hub and Spoke Configuration . . . . .	265
	Figure 122: Create VPN Page Showing Custom Routing Instance Option . . . . .	266
	Figure 123: Create VPN Policy-Based—Add as Endpoint Page . . . . .	267
	Figure 124: Create VPN Page—External Interface Selection . . . . .	268
	Figure 125: VPN: Concurrent Save Error Message . . . . .	269
	Figure 126: Inline Address Object Creation Page . . . . .	270
	Figure 127: Inline Address Group Creation for VPN Object . . . . .	270
	Figure 128: Import VPN . . . . .	274
	Figure 129: Select Devices . . . . .	275
	Figure 130: VPN Configuration Progress Bar . . . . .	275
	Figure 131: VPN Import—Conflicting EndPoints . . . . .	276
	Figure 132: Select EndPoints Page . . . . .	277
	Figure 133: Summary Page . . . . .	278
	Figure 134: VPN Import Job Details . . . . .	279
	Figure 135: VPN Import from Security Director Devices . . . . .	280
<b>Chapter 18</b>	<b>Creating and Managing Extranet Devices . . . . .</b>	<b>287</b>
	Figure 136: Create Extranet Device Page . . . . .	287
<b>Chapter 19</b>	<b>Creating and Managing VPN Profiles . . . . .</b>	<b>291</b>
	Figure 137: VPN Profile: Phase 1 . . . . .	292
	Figure 138: VPN Profile: Phase 2 . . . . .	295
	Figure 139: Create Phase 2 Proposal . . . . .	295
<b>Part 9</b>	<b>Using Security Intelligence Solution</b>	
<b>Chapter 20</b>	<b>Understanding Security Intelligence Solution . . . . .</b>	<b>301</b>
	Figure 140: Security Intelligence Solution . . . . .	301
	Figure 141: Security Intelligence Page . . . . .	302
<b>Chapter 21</b>	<b>Creating and Managing Spotlight Secure Connectors . . . . .</b>	<b>303</b>
	Figure 142: Spotlight Secure Connector Landing Page . . . . .	303
	Figure 143: Add Connector Page . . . . .	304
	Figure 144: Global Connector Settings . . . . .	306
	Figure 145: Confirm Device Association . . . . .	308
	Figure 146: Connector-Device List . . . . .	309
	Figure 147: Security Device Feed Status . . . . .	309
	Figure 148: Spotlight Secure Connector Feed Status . . . . .	311
<b>Chapter 22</b>	<b>Creating and Managing Information Sources . . . . .</b>	<b>313</b>

	Figure 149: Information Sources Landing Page . . . . .	313
	Figure 150: Add Information Source . . . . .	314
<b>Chapter 23</b>	<b>Creating and Managing Security Intelligence Profiles . . . . .</b>	<b>317</b>
	Figure 151: Profiles Page . . . . .	317
	Figure 152: Create Security Intelligence Profile Page . . . . .	318
	Figure 153: Create Security Intelligence Profile-Custom Values . . . . .	319
<b>Chapter 24</b>	<b>Creating and Managing Security Intelligence Policies . . . . .</b>	<b>323</b>
	Figure 154: Policies Page . . . . .	323
	Figure 155: Create Policy Page . . . . .	324
<b>Chapter 25</b>	<b>Creating and Managing Dynamic Address Groups . . . . .</b>	<b>327</b>
	Figure 156: Dynamic Address Groups Main Page . . . . .	327
	Figure 157: Create Dynamic Address Page . . . . .	328
	Figure 158: Modify Dynamic Address Page . . . . .	329
<b>Part 10</b>	<b>Configuring UTM Policies</b>	
<b>Chapter 27</b>	<b>Creating and Managing UTM Policies . . . . .</b>	<b>335</b>
	Figure 159: UTM Policies Landing Page . . . . .	337
	Figure 160: UTM Policy Wizard . . . . .	337
	Figure 161: Different UTM Policy Profiles . . . . .	338
	Figure 162: Web Filtering Wizard . . . . .	339
	Figure 163: Web Filtering Profile Summary . . . . .	340
	Figure 164: Antivirus Wizard . . . . .	341
	Figure 165: Antivirus Profile Summary . . . . .	342
	Figure 166: Antispam Profile Wizard . . . . .	343
	Figure 167: Antispam Profile Summary . . . . .	344
	Figure 168: Content Filtering Profile Wizard . . . . .	345
<b>Chapter 28</b>	<b>Creating and Managing Antispam Profiles . . . . .</b>	<b>349</b>
	Figure 169: Anti-Spam Profiles Page . . . . .	349
	Figure 170: Create Anti-Spam Profile Page . . . . .	350
<b>Chapter 29</b>	<b>Creating and Managing Antivirus Profiles . . . . .</b>	<b>355</b>
	Figure 171: Anti-Virus Profiles Main Page . . . . .	355
	Figure 172: Create Anti-Virus Profile Page . . . . .	356
	Figure 173: Antivirus Profile-General Information . . . . .	356
<b>Chapter 30</b>	<b>Creating and Managing Content Filtering Profiles . . . . .</b>	<b>363</b>
	Figure 174: Content Filtering Profiles Main Page . . . . .	363
	Figure 175: Create Content Filtering Profile Page . . . . .	364
	Figure 176: Content Filtering Profile Wizard . . . . .	364
<b>Chapter 31</b>	<b>Creating and Managing Web Filtering Profiles . . . . .</b>	<b>371</b>
	Figure 177: Web Filtering Profiles Main Page . . . . .	371
	Figure 178: Create Web Filtering Profile . . . . .	372
	Figure 179: Create Web Filtering Profile . . . . .	373
	Figure 180: Select URL Categories . . . . .	374
	Figure 181: Inline Creation of a New URL Category . . . . .	375
	Figure 182: Inline Creation of a New URL Pattern . . . . .	376

<b>Chapter 32</b>	<b>Creating and Managing URL Patterns . . . . .</b>	<b>383</b>
	Figure 183: URL Patterns Main Page . . . . .	383
	Figure 184: Create URL Pattern Page . . . . .	384
<b>Chapter 33</b>	<b>Creating and Managing Custom URL Category Lists . . . . .</b>	<b>389</b>
	Figure 185: Custom URL Category Lists Main Page . . . . .	389
	Figure 186: Create Custom URL Category List Page . . . . .	390
<b>Chapter 34</b>	<b>Creating and Managing UTM Device Profiles . . . . .</b>	<b>395</b>
	Figure 187: Device Profiles Main Page . . . . .	396
	Figure 188: Create UTM Device Profile Page . . . . .	397
<b>Part 11</b>	<b>Configuring NAT Policies</b>	
<b>Chapter 36</b>	<b>Creating and Managing NAT Policies . . . . .</b>	<b>409</b>
	Figure 189: NAT Tabular View . . . . .	409
	Figure 190: Create NAT Policy Page . . . . .	410
	Figure 191: Lock Failure Error Message for the Second User . . . . .	412
	Figure 192: Inactivity Timeout Error . . . . .	412
	Figure 193: Policy Lock Expired Message . . . . .	412
	Figure 194: NAT Locked Policy-Save As Window . . . . .	413
	Figure 195: NAT Policy-Unsaved Changes Message . . . . .	413
	Figure 196: NAT Policy- Policy Unlock by Admin Message . . . . .	413
	Figure 197: NAT Policy Lock Release Message . . . . .	413
	Figure 198: Setting Source NAT Pool Page . . . . .	415
	Figure 199: Create Source NAT Pool Page . . . . .	415
	Figure 200: Setting the Destination Pool Page . . . . .	416
	Figure 201: Create Destination NAT Pool Page . . . . .	416
	Figure 202: Create Inline NAT Address Object . . . . .	416
	Figure 203: Create NAT Address Page . . . . .	417
	Figure 204: Inline Address Group Creation for NAT Policy . . . . .	417
	Figure 205: Advanced Search Box for NAT Policies . . . . .	419
	Figure 206: Policy View Settings . . . . .	422
	Figure 207: NAT Policy-Manage Policy Locks . . . . .	423
	Figure 208: Modify Security Director Settings . . . . .	424
	Figure 209: NAT Policies Landing Page . . . . .	425
	Figure 210: NAT Policies-Drag and Drop Objects Window . . . . .	426
	Figure 211: Destination Traffic Match Type Selector Page . . . . .	429
	Figure 212: Port Configuration for Static NAT . . . . .	431
	Figure 213: Concurrent NAT Policy Editing Error . . . . .	433
	Figure 214: NAT Policy CLI Configuration . . . . .	434
	Figure 215: Snapshot Policy . . . . .	439
	Figure 216: Modify Security Director Settings . . . . .	440
	Figure 217: Rollback Service Summary Report . . . . .	441
	Figure 218: Object Conflict Resolution Window . . . . .	441
	Figure 219: Rollback OCR Summary Report . . . . .	442
	Figure 220: Rollback Policy Summary Report . . . . .	442
	Figure 221: Compare Versions with Swap Option . . . . .	443
	Figure 222: Versions Comparing Summary Report . . . . .	443
	Figure 223: Snapshot Delete Confirm Window . . . . .	444

	Figure 224: Expand All Warning Message for More Than 1,000 Rules . . . . .	446
	Figure 225: Nested Rule Group Operation Warning Message . . . . .	447
	Figure 226: Destination NAT Rule Paste Error . . . . .	447
	Figure 227: Static NAT Rule Paste Error . . . . .	447
	Figure 228: Group Policy Paste Error . . . . .	448
	Figure 229: Jumping to the Current NAT Rule . . . . .	451
	Figure 230: Changes in Rule View Window . . . . .	451
	Figure 231: Policy Comparison . . . . .	452
	Figure 232: Log Displayed in the Event Viewer . . . . .	453
<b>Chapter 37</b>	<b>Creating and Managing NAT Pools . . . . .</b>	<b>455</b>
	Figure 233: Create NAT Pool Page . . . . .	456
	Figure 234: Inline Address Group Creation for NAT Pool . . . . .	458
	Figure 235: Show Duplicates of NAT Pool . . . . .	461
	Figure 236: Merge NAT Pool . . . . .	461
	Figure 237: Delete Duplicate NAT Pool Objects . . . . .	462
	Figure 238: Confirm Merge Operation . . . . .	462
	Figure 239: NAT Pool Usage Window . . . . .	463
	Figure 240: Replace NAT Pools . . . . .	464
<b>Chapter 38</b>	<b>Creating and Managing Port Sets . . . . .</b>	<b>467</b>
	Figure 241: Create PortSet . . . . .	467
<b>Part 12</b>	<b>Using IDP Signature Database Downloads</b>	
<b>Chapter 39</b>	<b>Downloading and Installing Signature Database . . . . .</b>	<b>473</b>
	Figure 242: Signature Download Logs . . . . .	473
	Figure 243: Signature Database Page . . . . .	474
	Figure 244: Download Configuration Page . . . . .	474
	Figure 245: Install Configuration Page . . . . .	476
<b>Part 13</b>	<b>Using IPS Management</b>	
<b>Chapter 40</b>	<b>Creating and Managing IPS Signatures and Signature Sets . . . . .</b>	<b>481</b>
	Figure 246: View All IPS Signatures Page . . . . .	482
	Figure 247: Create IPS Signature Page . . . . .	483
	Figure 248: Nested Rule Group Paste Warning Message . . . . .	491
<b>Chapter 41</b>	<b>Creating and Managing IPS Policies . . . . .</b>	<b>493</b>
	Figure 249: IPS Policies Tabular View . . . . .	495
	Figure 250: Policy View Settings . . . . .	497
	Figure 251: IPS Advance Search Window . . . . .	498
	Figure 252: Lock Failure Error Message for the Second User . . . . .	500
	Figure 253: Inactivity Timeout Error . . . . .	501
	Figure 254: Policy Lock Expired Message . . . . .	501
	Figure 255: Unsaved Changes Warning Message . . . . .	501
	Figure 256: Policy Unlock by Admin Message . . . . .	501
	Figure 257: Policy Lock Release Message . . . . .	502
	Figure 258: IPS Policy-Manage Policy Locks . . . . .	503
	Figure 259: Modify Security Director Settings . . . . .	504
	Figure 260: IPS Policies Landing Page . . . . .	505

	Figure 261: IPS Policie-Drag and Drop Objects Window . . . . .	506
	Figure 262: IPS Policy Publish Page . . . . .	509
	Figure 263: Policy Publish-Affected Devices Page . . . . .	510
	Figure 264: Policy Publish-CLI Configuration . . . . .	510
	Figure 265: Policy Publish-XML Configuration . . . . .	511
	Figure 266: Nested Rule Groups Paste Operation Warning Message . . . . .	516
<b>Part 14</b>	<b>Configuring Network Devices</b>	
<b>Chapter 42</b>	<b>Creating and Managing Security Zones . . . . .</b>	<b>521</b>
	Figure 267: Device Configuration-Zones Main Page . . . . .	522
	Figure 268: Device Configuration-Create Zone Page . . . . .	523
	Figure 269: Modify Zone Page . . . . .	525
<b>Chapter 43</b>	<b>Creating and Managing Screens . . . . .</b>	<b>527</b>
	Figure 270: Device Configuration-Create Screen Page . . . . .	528
	Figure 271: Modify Screen Page . . . . .	532
<b>Chapter 44</b>	<b>Configuring Security Logs . . . . .</b>	<b>535</b>
	Figure 272: Device Configuration-Create Security Logging Page . . . . .	535
	Figure 273: Security Logging-Stream Configuration Page . . . . .	536
	Figure 274: Security Logging-Exclude Configuration Page . . . . .	538
<b>Chapter 45</b>	<b>Creating and Managing Static Routes . . . . .</b>	<b>541</b>
	Figure 275: Device Configuration-Static Routes Main Page . . . . .	542
	Figure 276: Static Routes-Create Static Route Page . . . . .	543
	Figure 277: Modify Static Route Page . . . . .	546
<b>Chapter 46</b>	<b>Creating and Managing Routing Instances . . . . .</b>	<b>549</b>
	Figure 278: Device Configuration-Routing Instances Main Page . . . . .	550
	Figure 279: Create Routing Instance Page . . . . .	551
	Figure 280: Modify Routing Instance Page . . . . .	553
<b>Chapter 47</b>	<b>Managing Physical Interfaces and Syslog . . . . .</b>	<b>555</b>
	Figure 281: Device Configuration-Physical Interfaces Main Page . . . . .	556
	Figure 282: Modify Physical Interface Page . . . . .	557
	Figure 283: Create Logical Interface Page . . . . .	558
	Figure 284: Device Configuration-Modify Syslog Page . . . . .	560
	Figure 285: Modify Syslog-Host Configuration Page . . . . .	561
	Figure 286: Modify Syslog-File Configuration Page . . . . .	562
	Figure 287: Modify Syslog-User Configuration Page . . . . .	563
<b>Chapter 48</b>	<b>Updating Security Director Devices . . . . .</b>	<b>565</b>
	Figure 288: Security Director Devices Page . . . . .	567
	Figure 289: Update Window . . . . .	567
	Figure 290: Device Changes Page Showing Device Comments . . . . .	569
	Figure 291: Sync Device Status Page . . . . .	570
	Figure 292: Manage Security Devices Page . . . . .	574
	Figure 293: Service Import Summary Page . . . . .	575
	Figure 294: Object Conflict Resolution Page . . . . .	575
	Figure 295: Same Action Applied to Two Conflicting Objects . . . . .	576
	Figure 296: Policy Import Status Page . . . . .	576

Figure 297: Firewall Policy Final Import Status Page . . . . .	577
Figure 298: High-Level Device Import Workflow . . . . .	581
Figure 299: NSM Xdiff File Upload Page . . . . .	582
Figure 300: NSM Migration Devices Page . . . . .	582
Figure 301: Service Import Summary Page . . . . .	583
Figure 302: NSM-Object Conflict Resolution Page . . . . .	583
Figure 303: NSM Migration Status Page . . . . .	584
Figure 304: NSM Migration Final Status Report Page . . . . .	585
Figure 305: Consolidated Config Status from Security Director . . . . .	586
Figure 306: Job Details Window . . . . .	590
Figure 307: Confirmed Commit Warning Message . . . . .	590



# List of Tables

	<b>About the Documentation</b> . . . . .	<b>xxxi</b>
	Table 1: Notice Icons . . . . .	xxxii
	Table 2: Text and Syntax Conventions . . . . .	xxxii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Understanding Security Director</b> . . . . .	<b>3</b>
	Table 3: Security Director Global Search . . . . .	8
	Table 4: Predefined Roles for Security Director . . . . .	11
	Table 5: Security Director Workspaces . . . . .	22
<b>Part 2</b>	<b>Configuring Dashboard Monitors</b>	
<b>Chapter 2</b>	<b>Creating and Managing Dashboard Monitors</b> . . . . .	<b>27</b>
	Table 6: Default Dashboard Monitor Parameters . . . . .	29
<b>Part 3</b>	<b>Using Event Viewer</b>	
<b>Chapter 3</b>	<b>Understanding Event Viewer Options</b> . . . . .	<b>41</b>
	Table 7: Event Viewer Columns . . . . .	45
	Table 8: Event Viewer Table Options . . . . .	52
	Table 9: Detailed Log View . . . . .	54
	Table 10: Compare Time Period . . . . .	57
<b>Chapter 4</b>	<b>Creating and Managing Event Viewer Filters</b> . . . . .	<b>61</b>
	Table 11: Advanced Filter Options . . . . .	63
	Table 12: Operators Supported in the Group By Column fields . . . . .	65
<b>Part 4</b>	<b>Configuring Alerts</b>	
<b>Chapter 5</b>	<b>Creating and Managing Alerts</b> . . . . .	<b>75</b>
	Table 13: Alert Columns . . . . .	76
<b>Chapter 6</b>	<b>Creating and Managing Alert Definitions</b> . . . . .	<b>79</b>
	Table 14: Alert Generation Columns . . . . .	79
	Table 15: Alert Definitions Options . . . . .	80
<b>Part 5</b>	<b>Configuring Reports</b>	
<b>Chapter 7</b>	<b>Creating and Managing Reports</b> . . . . .	<b>87</b>
	Table 16: Report Options . . . . .	88
	Table 17: Report Columns . . . . .	93

	Table 18: Report Options . . . . .	94
<b>Part 6</b>	<b>Configuring Security Objects</b>	
<b>Chapter 10</b>	<b>Creating and Managing Addresses and Address Groups . . . . .</b>	<b>121</b>
	Table 19: Migration Matrix . . . . .	123
<b>Part 7</b>	<b>Configuring Firewall Policies</b>	
<b>Chapter 13</b>	<b>Creating and Managing Firewall Policies . . . . .</b>	<b>151</b>
	Table 20: Sorting Order for Firewall Policies . . . . .	157
	Table 21: IPS Configuration Mode . . . . .	162
	Table 22: Firewall policy Right Pane Search Options . . . . .	170
	Table 23: Specific Security Director Search Behavior . . . . .	173
	Table 24: Examples of Different Advanced Search Parameters . . . . .	173
	Table 25: Priority and Precedence for Firewall Policies . . . . .	189
	Table 26: Policy Rule Hit Level . . . . .	191
	Table 27: Hits Detail View . . . . .	192
	Table 28: Setting Precedence Values for Different Priorities . . . . .	202
	Table 29: Various Rule Operation on the Filtered Rules . . . . .	224
<b>Part 8</b>	<b>Configuring VPNs</b>	
<b>Chapter 17</b>	<b>Creating and Managing IPsec VPNs . . . . .</b>	<b>257</b>
	Table 30: Select End-Points Columns . . . . .	277
<b>Part 11</b>	<b>Configuring NAT Policies</b>	
<b>Chapter 35</b>	<b>Understanding NAT . . . . .</b>	<b>403</b>
	Table 31: Persistent NAT Support . . . . .	404
	Table 32: Translated Address Pool Selection for Source NAT . . . . .	405
	Table 33: Translated Address Pool Selection for Destination NAT And Static NAT . . . . .	405
<b>Chapter 36</b>	<b>Creating and Managing NAT Policies . . . . .</b>	<b>409</b>
	Table 34: Junos OS Protocol Names . . . . .	418
	Table 35: Specific Security Director Search Behavior . . . . .	420
	Table 36: Example: Different Advanced Search Parameters for NAT . . . . .	420
	Table 37: Example: Rule Set Names for Different Ingress And Egress Values of Source NAT Rules . . . . .	431
	Table 38: Example: Rule Set Names for Destination NAT and Static NAT . . . . .	432
	Table 39: Various Rule Operation on the Filtered Rules . . . . .	449
<b>Part 12</b>	<b>Using IDP Signature Database Downloads</b>	
<b>Chapter 39</b>	<b>Downloading and Installing Signature Database . . . . .</b>	<b>473</b>
	Table 40: App-Sig-Package Details . . . . .	478
<b>Part 13</b>	<b>Using IPS Management</b>	
<b>Chapter 41</b>	<b>Creating and Managing IPS Policies . . . . .</b>	<b>493</b>

	Table 41: IPS Configuration Mode . . . . .	494
	Table 42: Specific Security Director Search Behavior . . . . .	499
	Table 43: Examples of Different Advanced Search Parameters . . . . .	499
	Table 44: Various Rule Operation on the Filtered Rules . . . . .	517
<b>Chapter 48</b>	<b>Updating Security Director Devices . . . . .</b>	<b>565</b>
	Table 45: Security Director Devices Workspace Columns . . . . .	565
	Table 46: Different Status of Candidate Configuration . . . . .	587



# About the Documentation

- Documentation and Release Notes on page xxxi
- Documentation Conventions on page xxxi
- Documentation Feedback on page xxxiii
- Requesting Technical Support on page xxxiv

## 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 <http://www.juniper.net/techpubs/>.

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 <http://www.juniper.net/books>.

## Documentation Conventions

---

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

Table 2: Text and Syntax Conventions

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

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"><li>To configure a stub area, include the <b>stub</b> statement at the <b>[edit protocols ospf area area-id]</b> hierarchy level.</li><li>The console port is labeled <b>CONSOLE</b>.</li></ul>
< > (angle brackets)	Encloses optional keywords or variables.	<b>stub &lt;default-metric <i>metric</i>&gt;;</b>
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <b>(<i>string1</i>   <i>string2</i>   <i>string3</i>)</b>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	<b>community name members [ <i>community-ids</i> ]</b>
Indentation and braces ( { } )	Identifies a level in the configuration hierarchy.	<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"><li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li><li>To cancel the configuration, click <b>Cancel</b>.</li></ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

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

- Online feedback rating system—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.

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

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC 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 <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://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: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

## 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 <http://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 <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Overview

- [Understanding Security Director on page 3](#)



## CHAPTER 1

# Understanding Security Director

- [Security Director Overview on page 3](#)
- [Security Director Logging and Reporting Overview on page 6](#)
- [Indexing Overview on page 7](#)
- [Global Search on page 8](#)
- [Security Director User Roles on page 9](#)
- [Security Director Dashboard on page 21](#)

## Security Director Overview

---

Security Director is a Junos Space application that you can use to design your network security using a quick and easy approach. With Security Director, you can create IPsec VPNs, firewall policies, NAT policies, and IPS configurations and push them to your security devices. These configurations use objects such as addresses, services, NAT pools, application signatures, policy profiles, VPN profiles, template definitions, and templates. These objects can be shared across multiple security configurations. You can create these objects prior to creating security configurations.

Firewall policy, NAT policy, and IPS policy can be created and managed in Tabular view. You can easily add new rules to the policies and choose to override policy-inherited settings by customizing the settings at a per-rule level. After you have added the rules to the policy, you can reorder these rules based on priority, or group these rules for easy identification and modify them at a later time. A unified user interface approach for firewall, NAT, and IPS policies helps you reduce the learning time required to create different security configurations.

Security Director allows you to create site-to-site, hub-and-spoke, and full-mesh IPsec VPNs. The IPsec VPN creation interface allows you to define the Phase 1 and Phase 2 settings of the VPN. All VPNs created using Security Director can be viewed in Tabular view. You can also modify the settings at a per-VPN level or per-device level in a VPN.

You can periodically download the latest version of application signatures and IPS signatures from a URL provided by Juniper Networks. You can install these signatures on security devices that have an IPS-related license installed. You can then use application signatures and IPS signatures when creating firewall policy configurations. Security Director also lets you create your own customized signature sets. All application firewall

and IPS configurations are pushed to the devices when the firewall policy in which they are used is pushed to the devices.

When you finish creating and verifying your security configurations, you can publish these configurations and keep them ready to be pushed to the security devices. Security Director helps you push all the security configurations to the devices all at once by providing a single interface that is intuitive. You can select all security devices that you are using on the network and push all security configurations to these devices.

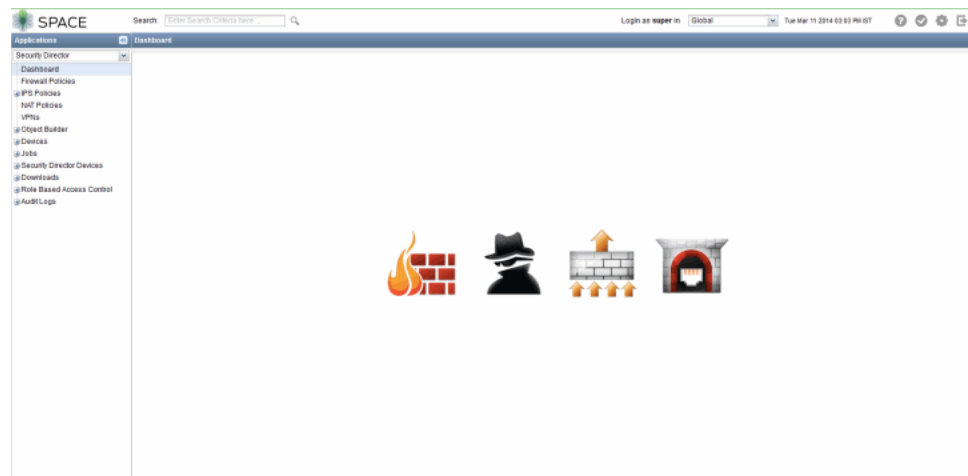
A set of gadgets displayed on the dashboard graphically illustrates the critical elements related to your security configurations. These gadgets help you keep track of the objects created and their usage across security configurations.

The Security Director application is divided into seven workspaces, which include Object Builder, Firewall Policy, NAT Policy, VPN, Downloads, IPS Management, and Security Director Devices.

- Object Builder—A workspace to created objects used for firewall policy, NAT policy, and VPN configurations.
- Firewall Policy— A workspace to create and publish firewall policies on supported devices.
- NAT Policy—A workspace to create and publish NAT policies on supported devices.
- VPN—A workspace to create site-to-site, hub-and-spoke, and full-mesh IPsec VPNs.
- Downloads—A workspace to download and install signatures.
- IPS Management—A workspace to create and manage IPS signatures, signature sets, and IPS policies.
- Security Director Devices—A workspace to update the configurations on the devices.

Figure 1 on page 4 displays the Security Director homepage.

Figure 1: Security Director Homepage



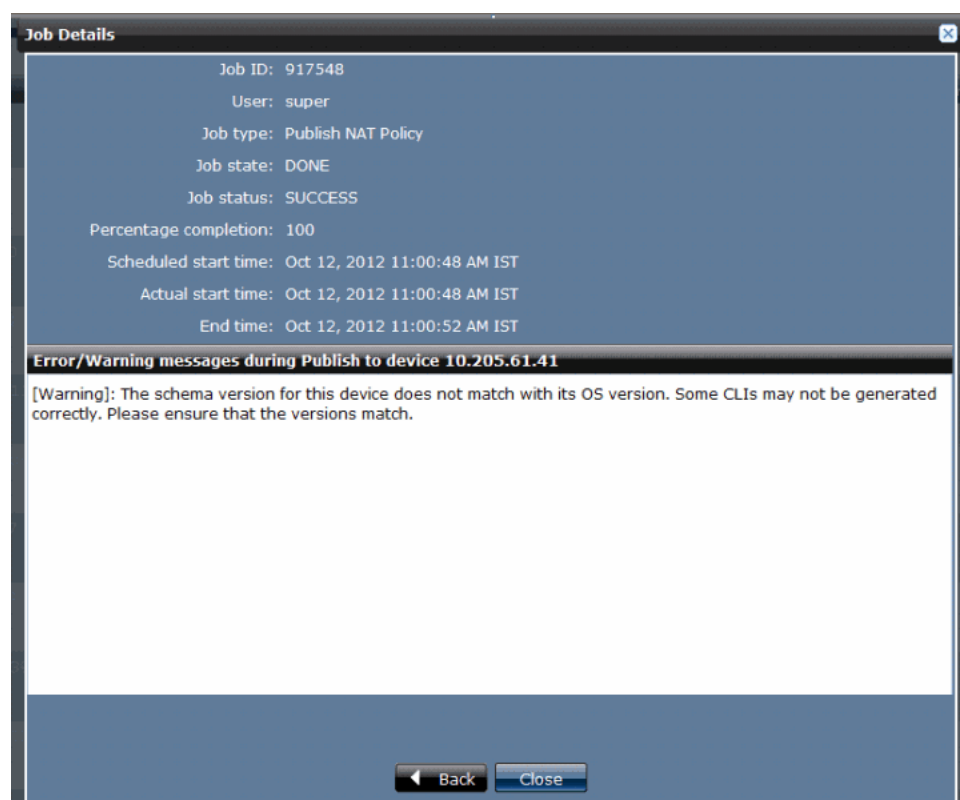
Some of the global features available with Security Director include:

- Create unique labels for objects and security configurations using the Tagging feature for easier identification.
- Search objects and security configurations from a single search interface.
- Verify and tweak your security configurations before pushing them to the device by viewing the CLI and XML version of the configuration in the Publish workflow. This approach helps you keep the configurations ready and push these configurations to the devices during the maintenance window.
- Quickly clone objects and policy-related security configurations to save time and effort in creating new objects and configurations.



**NOTE:** Ensure that the exact matching of Junos OS schema is installed on the Junos Space Platform before you start using Security Director features. If there is a mismatch, the following warning message is displayed during the publish preview workflow, as shown in [Figure 2 on page 5](#).

**Figure 2: Junos OS Schema Mismatch Warning Message**



**Related  
Documentation**

- [Security Director User Roles on page 9](#)
- [Security Director Dashboard on page 21](#)

## Security Director Logging and Reporting Overview

---

The Junos Space Security Director Logging and Reporting module enables log collection across multiple SRX Series Services Gateways and enables log visualization.

The Logging and Reporting module provides:

- Device health and events monitoring.
- Visualization of security events resulting from complex and dynamic firewall policies using the dashboard and the Event Viewer. The dashboard is customizable: you can add, modify, or edit the monitors.
- Device health monitoring of CPU and memory.
- Alert notifications about specific events or when a threshold limit is reached.

Logs, also called event logs, provide vital information for managing network security incident investigation and response.

Logs allow you to monitor devices for issues to ensure that all services are up and running, and to check on the device usage trends to allow you make decisions about potential issues and upgrades.

Security traffic monitoring helps to ensure that the security practices and controls are in place, are being adhered to, and are effective. You can view traffic logs generated from security policies using the dashboard and the Event Viewer.

Logging provides the following features:

- Receives events from SRX Series Services Gateways and application logs
- Stores events for a defined period of time or a set volume of data
- Parses and indexes logs to help speed up searching
- Provides queries and helps in data analysis and historical events investigation

The system collects the following key logs:

- Firewall—Captures events generated by one or more firewall rules to validate whether the rules configured are producing the desired impact on actual traffic.
- IDP—Captures events when the system is attacked. If the configuration is enabled, the log captures the volume of messages transferred to an application. For example: from an IP address, to an IP address, and so on. It also logs details of the traffic permitted and dropped according to the IDP rule set.
- VPN—Captures the status of the VPNs and enables VPN monitoring.
- UTM—Captures all UTM-related log messages. For example: Antivirus records of virus incidents in Web, FTP, and e-mail traffic.
- System—Captures the control plane logs generated and stored on the local SRX Series Services Gateways.

Logging and reporting is divided into three workspaces, which include Alerts, Reports, and Event Viewer.

- **Event Viewer**—Event Viewer is used to view traffic logs generated from security policies.
- **Alerts**—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 occurs. An alert trigger threshold is reached when a number of network traffic events crosses a predefined threshold within a period of time.

- **Reports**—Reports are used to schedule reports daily, weekly, or monthly, and to configure them to include multiple criteria. You can also personalize the reports by adding company logo, a footer, and so on. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail. Reports enable you to perform trend analysis of your network activities.

#### Related Documentation

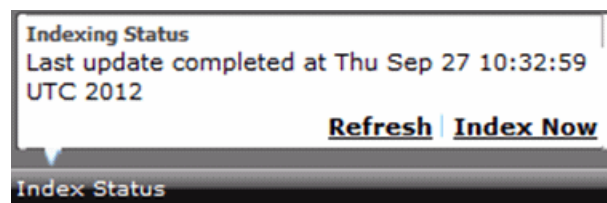
- [Logging and Reporting Dashboard Overview on page 27](#)
- [Alerts and Notifications Overview on page 75](#)
- [Reports Overview on page 87](#)
- [Event Viewer Overview on page 41](#)

## Indexing Overview

Index Now option is a manual override option to completely re-index the Security Director database for search functionality. However, Security Director does this process automatically when you add, delete, or update the objects. Therefore, this option should only be used in scenarios when you notice that objects are not searchable. One such scenario is database restore or other unknown failure conditions, in which the search indexes might have gone out of sync with Security Director.

[Figure 3 on page 7](#) shows the indexing status for Security Director.

**Figure 3: Indexing Status Message**



To get the Indexing Status, go to Object Builder workspace and click either Addresses or Services option. In the Addresses or Services page, right-click any address or service and select **Find Usage**. You can see the Indexing Status option at the bottom of the Usage window.



**NOTE:** After the Junos Space database is restored, a manual re-index of the Security Director database is required.

#### Related Documentation

- [Global Search on page 8](#)

## Global Search

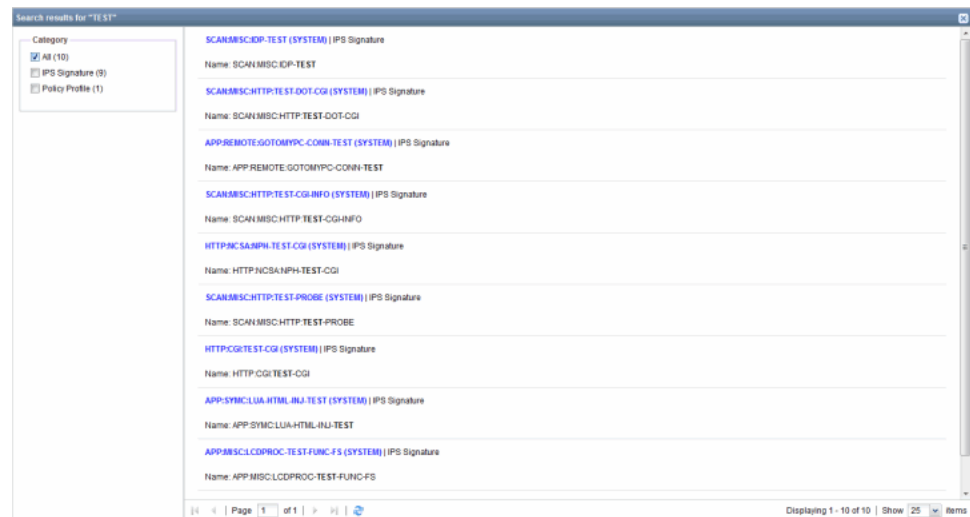
The Security Director homepage provides a global search option to find objects and security configurations. You can also click a search result and navigate to its page.

To search for objects or configurations using the Global search:

1. Enter the search criteria in the Search field and click the magnifying glass icon.

All objects and configurations matching the search criteria appear in the search results page. The area on the left displays the search results with appropriate filters and the area on the right displays the detailed search results with a short description as shown in [Figure 4 on page 8](#).

**Figure 4: Global Search Results**



2. Click a detailed search result URL to navigate to its respective page.

The search results for Global search are based on how the Security Director objects and configurations are indexed. [Table 3 on page 8](#) specifies the objects and configurations that you can search using Global search.

**Table 3: Security Director Global Search**

Security Director Object/Configuration	Attributes by which Global search is possible.
Firewall Policy	Name, profile name, description, source address, destination address, service, and zone.

Table 3: Security Director Global Search (*continued*)

Address	Addresses that are IP, subnet, range, and hostname type.
Address Group	All address parts of the group after expanding address groups within the group.
Service	Services that include ports, ICMP, RPC, and UUID searches.
Service Group	All service parts of the group.
VPN	All addresses used in VPN or protected resources of the VPN.
NAT	All addresses used in NAT, NAT pools, and Match Type (zone, interface).
IPS	IPS signature name, signature CVE ID, bug ID, and IPS policy names.

You cannot search objects such as device name, policy profile, and template using Global search. If you type a valid IPv4 address, subnet or range search results return all addresses that include that specific valid IPv4 address. For example, if you type 1.1.1.1 and if there is an subnet address 1.1.1.0/24, the search result will match the subnet and return the result.

With Global search, the search is free-text based. You can search for phrases and multiple terms. The default value for multiple terms is the OR operator. You can also search for multiple terms using the AND operator. By default, the search query looks at name, IP, port, category, ICMP code, ICMP type, subnets, and IP ranges. All search results are highlighted as part of the result, and the search results have a URL to jump to the corresponding object in its ILP. The IP address searches looks for an IP address, within ranges and subnets as long as the user gives a valid IP address. In range-based searches for IP addresses; you would need to add the – for range; for example, 1.1.1.1/24 and 10.204.76.56-10.204.76.80. The subnet searches should be provided with valid subnets. All port-specific searches will only search for ports. The source port uses the keyword “srcPort” and the destination port uses the keyword “dstPort”.

SD Search supports wildcard searches if you use the “\*” character in the search query. Names of objects will be broken down into one or more terms if the name has a nonletter character or a number. For example, a name like “enet\_dest12” will be broken into “enet” “dest” and “12”. You can search on “enet” “dest” or 112 or type “ene\*” “des\*” and so on.

**Related Documentation**

- [Indexing Overview on page 7](#)

## Security Director User Roles

The Junos Space administrator creates users and assigns roles (permissions) that allow you to permissions for and perform different tasks. You cannot view the tasks that you do not have access to. While Junos Space allows creating users with custom permissions, it also has a set of predefined user roles. These predefined roles cannot be modified or

deleted. See [Table 4 on page 11](#) for the list of predefined user roles available in Security Director.

For the latest predefined roles, see **Network Management Platform > Role Based Access Control > Roles**.

Table 4: Predefined Roles for Security Director

Predefined Role	Task Group and Tasks	Application > Workspace
Security Analyst	<ul style="list-style-type: none"> <li>Event Viewer               <ul style="list-style-type: none"> <li>Edit Dashboard</li> <li>Create Filter</li> <li>Modify Filter</li> <li>Delete Filter</li> </ul> </li> </ul>	Security Director > Event Viewer
	<ul style="list-style-type: none"> <li>Firewall Policies               <ul style="list-style-type: none"> <li>View Policy</li> <li>Policy Profiles                   <ul style="list-style-type: none"> <li>Manage Template Definitions                       <ul style="list-style-type: none"> <li>Create Template Definition</li> <li>Modify Template Definition</li> <li>Delete Template Definitions</li> </ul> </li> <li>Manage SD Templates                       <ul style="list-style-type: none"> <li>Create Policy Template</li> <li>Modify Policy Template</li> <li>Delete policy Templates</li> </ul> </li> </ul> </li> <li>Assign Policy Profile to Domain</li> <li>Schedulers               <ul style="list-style-type: none"> <li>Assign Scheduler to Domain</li> </ul> </li> <li>Publish Policy</li> <li>Delete Policy</li> <li>Export Policy</li> <li>Create Policy</li> <li>Modify Policy</li> <li>Prioritize Policies</li> <li>Application Signatures</li> <li>Assign Devices</li> <li>Create/Modify/Delete Custom Column</li> <li>Manage Policy Locks</li> <li>Assign FWPolicy to Domain</li> </ul> </li> </ul>	Security Director > Firewall Policies
	<ul style="list-style-type: none"> <li>Reports               <ul style="list-style-type: none"> <li>View Report</li> <li>Create Report</li> <li>Modify Report</li> <li>Delete Report</li> <li>Send Report</li> </ul> </li> </ul>	Security Director > Reports
		Security Director > Alerts

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>Alerts               <ul style="list-style-type: none"> <li>Delete Generated Alert</li> <li>Alert Definitions                   <ul style="list-style-type: none"> <li>Create Alert Definition</li> <li>Modify Alert Definition</li> <li>Delete Alert Definition</li> </ul> </li> </ul> </li> </ul>	
	<ul style="list-style-type: none"> <li>UTM Policies               <ul style="list-style-type: none"> <li>UTM Policies                   <ul style="list-style-type: none"> <li>Assign UTM Policy to Domain</li> </ul> </li> <li>Anti-Spam Profiles                   <ul style="list-style-type: none"> <li>Assign AntiSpam Profile to Domain</li> </ul> </li> <li>Anti-Virus Profiles                   <ul style="list-style-type: none"> <li>Assign AntiVirus Profile to Domain</li> </ul> </li> <li>Content Filtering Profiles                   <ul style="list-style-type: none"> <li>Assign Content Filtering Profile to Domain</li> </ul> </li> <li>Web Filtering Profiles                   <ul style="list-style-type: none"> <li>Assign Web Filtering Profile to Domain</li> </ul> </li> <li>Device Profiles                   <ul style="list-style-type: none"> <li>Assign UTM Device Profile to Domain</li> </ul> </li> <li>URL Patterns                   <ul style="list-style-type: none"> <li>Assign URL Pattern to Domain</li> </ul> </li> <li>Custom URL Category Lists                   <ul style="list-style-type: none"> <li>Assign URL Category List to Domain</li> </ul> </li> </ul> </li> </ul>	Security Director > UTM Policies
	<ul style="list-style-type: none"> <li>IPS Policies               <ul style="list-style-type: none"> <li>IPS Signature</li> <li>Policy Templates</li> <li>View IPS Policy</li> <li>Create IPS Policy</li> <li>Modify IPS Policy</li> <li>Publish IPS Policy</li> <li>Manage Policy Locks</li> </ul> </li> </ul>	Security Director > IPS Policies
		Security Director > Object Builder

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>Object Builder               <ul style="list-style-type: none"> <li>Zone Sets                   <ul style="list-style-type: none"> <li>Create ZoneSet</li> <li>Modify ZoneSet</li> <li>Delete ZoneSets</li> </ul> </li> <li>Addresses                   <ul style="list-style-type: none"> <li>Assign Address to Domain</li> </ul> </li> <li>Variables                   <ul style="list-style-type: none"> <li>Create Variable Definition</li> <li>Modify Variable Definition</li> <li>Delete Variables</li> <li>Assign Variable to Domain</li> </ul> </li> <li>Services                   <ul style="list-style-type: none"> <li>Assign Service Domain</li> </ul> </li> </ul> </li> </ul>	
	<ul style="list-style-type: none"> <li>Security Director Devices               <ul style="list-style-type: none"> <li>View Security Director Devices</li> <li>Update Device</li> <li>NSM Migration</li> <li>Import Device</li> </ul> </li> </ul>	Security Director > Security Director Devices
	<ul style="list-style-type: none"> <li>VPNs               <ul style="list-style-type: none"> <li>Create VPN</li> <li>View VPN</li> <li>Modify VPN</li> <li>Delete VPN</li> <li>VPN Profiles                   <ul style="list-style-type: none"> <li>Assign VPN Profile to Domain</li> </ul> </li> <li>Publish VPN</li> <li>Extranet Devices                   <ul style="list-style-type: none"> <li>Create Extranet Device</li> <li>Delete Extranet Device</li> <li>Modify Extranet Device</li> </ul> </li> <li>Assign IPSec VPN to Domain</li> </ul> </li> </ul>	Security Director > VPNs
		Security Director > Security Intelligence

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>• Security Intelligence           <ul style="list-style-type: none"> <li>• Profiles               <ul style="list-style-type: none"> <li>• Create Security Intelligence Profile</li> <li>• Modify Security Intelligence Profile</li> <li>• Delete Security Intelligence Profiles</li> </ul> </li> <li>• Policies               <ul style="list-style-type: none"> <li>• Create Security Intelligence Policy</li> <li>• Modify Security Intelligence Policy</li> <li>• Delete Security Intelligence Policies</li> </ul> </li> <li>• Dynamic Address Groups               <ul style="list-style-type: none"> <li>• Create Dynamic Address</li> <li>• Modify Dynamic Address</li> <li>• Delete Dynamic Addresses</li> </ul> </li> <li>• Backup / Restore               <ul style="list-style-type: none"> <li>• Create Backup</li> <li>• Delete Backups</li> <li>• Restore</li> </ul> </li> <li>• Information Sources               <ul style="list-style-type: none"> <li>• Update Feed Now</li> <li>• Create Information Source</li> <li>• Modify Information Source</li> <li>• Delete Information Sources</li> </ul> </li> <li>• Spotlight Connectors               <ul style="list-style-type: none"> <li>• Global Connector Settings</li> <li>• Trusted Server CAs</li> <li>• Associate Devices</li> <li>• Update connector Configurations</li> </ul> </li> </ul> </li> </ul>	
		Security Director > NAT Policies

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>NAT Policies               <ul style="list-style-type: none"> <li>View NAT Policy</li> <li>Create NAT Policy</li> <li>Modify NAT Policy</li> <li>Delete NAT Policy</li> <li>Publish NAT Policy</li> </ul> </li> <li>NAT Pools               <ul style="list-style-type: none"> <li>Create NAT Pool</li> <li>Modify NAT Pool</li> <li>Delete NAT Pools</li> <li>Assign Nat Pool to Domain</li> </ul> </li> <li>Port Sets               <ul style="list-style-type: none"> <li>Create PortSet</li> <li>Modify PortSet</li> <li>Delete PortSet</li> <li>Assign PortSet to Domain</li> </ul> </li> <li>Assign Devices To NAT Policy</li> <li>Manage Policy Locks</li> <li>Assign NAT Policy To Domain</li> </ul>	

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
Security Architect	<ul style="list-style-type: none"> <li>Event Viewer               <ul style="list-style-type: none"> <li>Edit Dashboard</li> <li>Create Filter</li> <li>Modify Filter</li> <li>Delete Filter</li> </ul> </li> </ul>	Security Director > Event Viewer
	<ul style="list-style-type: none"> <li>Firewall Policies               <ul style="list-style-type: none"> <li>View Policy</li> <li>Policy Profiles                   <ul style="list-style-type: none"> <li>Create Policy Profile</li> <li>Delete Policy Profiles</li> <li>Modify Policy Profile</li> </ul> </li> <li>Manage Template Definitions                   <ul style="list-style-type: none"> <li>Create Template Definition</li> <li>Modify Template Definition</li> <li>Delete Template Definitions</li> </ul> </li> <li>Manage SD Templates                   <ul style="list-style-type: none"> <li>Create Policy Template</li> <li>Modify Policy Template</li> <li>Delete policy Templates</li> </ul> </li> <li>Assign Policy Profile to Domain</li> </ul> </li> <li>Schedulers               <ul style="list-style-type: none"> <li>Create Scheduler</li> <li>Modify Scheduler</li> <li>Delete Schedulers</li> <li>Assign Scheduler to Domain</li> </ul> </li> <li>Publish Policy</li> <li>Delete Policy</li> <li>Export Policy</li> <li>Create Policy</li> <li>Modify Policy</li> <li>Prioritize Policies</li> <li>Application Signatures               <ul style="list-style-type: none"> <li>Create Application Signature</li> <li>Modify Application Signature</li> <li>Delete Application Signature</li> </ul> </li> <li>Assign Devices</li> <li>Create/Modify/Delete Custom Column</li> <li>Manage Policy Locks</li> <li>Unlock Firewall</li> <li>Assign FWPolicy to Domain</li> </ul>	Security Director > Firewall Policies
		Security Director > Reports

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>• Reports               <ul style="list-style-type: none"> <li>• View Report</li> <li>• Create Report</li> <li>• Modify Report</li> <li>• Delete Report</li> <li>• Send Report</li> </ul> </li> </ul>	
	<ul style="list-style-type: none"> <li>• Alerts               <ul style="list-style-type: none"> <li>• Delete Generated Alert</li> <li>• Alert Definitions                   <ul style="list-style-type: none"> <li>• Create Alert Definition</li> <li>• Modify Alert Definition</li> <li>• Delete Alert Definition</li> </ul> </li> </ul> </li> </ul>	Security Director > Alerts
		Security Director > UTM Policies

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>UTM Policies           <ul style="list-style-type: none"> <li>UTM Policies               <ul style="list-style-type: none"> <li>Create UTM Policy</li> <li>Modify UTM Policy</li> <li>Delete UTM Policies</li> <li>Assign UTM Policy to Domain</li> </ul> </li> <li>Anti-Spam Profiles               <ul style="list-style-type: none"> <li>Create Anti-Spam Profile</li> <li>Modify Anti-Spam Profile</li> <li>Delete Anti-Spam Profiles</li> <li>Assign AntiSpam Profile to Domain</li> </ul> </li> <li>Anti-Virus Profiles               <ul style="list-style-type: none"> <li>Create Anti-Virus Profile</li> <li>Modify Anti-Virus Profile</li> <li>Delete Anti-Virus Profiles</li> <li>Assign AntiVirus Profile to Domain</li> </ul> </li> <li>Content Filtering Profiles               <ul style="list-style-type: none"> <li>Create Content Filtering Profile</li> <li>Modify Content Filtering Profile</li> <li>Delete Content Filtering Profiles</li> <li>Assign Content Filtering Profile to Domain</li> </ul> </li> <li>Web Filtering Profiles               <ul style="list-style-type: none"> <li>Create Web Filtering Profile</li> <li>Modify Web Filtering Profile</li> <li>Delete Web Filtering Profiles</li> <li>Assign Web Filtering Profile to Domain</li> </ul> </li> <li>Device Profiles               <ul style="list-style-type: none"> <li>Create UTM Device Profile</li> <li>Modify UTM Device Profile</li> <li>Delete UTM Device Profiles</li> <li>Assign UTM Device Profile to Domain</li> </ul> </li> <li>URL Patterns               <ul style="list-style-type: none"> <li>Create URL Pattern</li> <li>Modify URL Pattern</li> <li>Delete URL Patterns</li> <li>Assign URL Pattern to Domain</li> </ul> </li> <li>Custom URL Category Lists               <ul style="list-style-type: none"> <li>Create Custom URL Category List</li> <li>Modify Custom URL Category List</li> <li>Delete Custom URL Category Lists</li> <li>Assign URL Category List to Domain</li> </ul> </li> </ul> </li> </ul>	

Security Director > IPS  
Policies

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>IPS Policies               <ul style="list-style-type: none"> <li>IPS Signature                   <ul style="list-style-type: none"> <li>Create IPS Signature</li> <li>Modify IPS Signature</li> <li>Delete IPS Signature</li> <li>Create Policy Template</li> </ul> </li> <li>Policy Templates                   <ul style="list-style-type: none"> <li>Create Policy Template</li> <li>Modify Policy Template</li> <li>Delete Policy Template</li> </ul> </li> <li>View IPS Policy</li> <li>Create IPS Policy</li> <li>Modify IPS Policy</li> <li>Publish IPS Policy</li> <li>Manage Policy Locks</li> <li>Unlock IPS</li> </ul> </li> </ul>	
	<ul style="list-style-type: none"> <li>Object Builder               <ul style="list-style-type: none"> <li>Zone Sets                   <ul style="list-style-type: none"> <li>Create ZoneSet</li> <li>Modify ZoneSet</li> <li>Delete ZoneSets</li> </ul> </li> <li>Addresses                   <ul style="list-style-type: none"> <li>Create Address</li> <li>Modify Address</li> <li>Delete Addresses</li> <li>Assign Address to Domain</li> </ul> </li> <li>Variables                   <ul style="list-style-type: none"> <li>Create Variable Definition</li> <li>Modify Variable Definition</li> <li>Delete Variables</li> <li>Assign Variable to Domain</li> </ul> </li> <li>Services                   <ul style="list-style-type: none"> <li>Create Service</li> <li>Modify Service</li> <li>Delete Services</li> <li>Assign Service Domain</li> </ul> </li> </ul> </li> </ul>	Security Director > Object Builder
	<ul style="list-style-type: none"> <li>Security Director Devices               <ul style="list-style-type: none"> <li>View Security Director Devices</li> <li>Update Device</li> <li>NSM Migration</li> <li>Import Device</li> </ul> </li> </ul>	Security Director > Security Director Devices

Table 4: Predefined Roles for Security Director (*continued*)

Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>VPNs               <ul style="list-style-type: none"> <li>Create VPN</li> <li>View VPN</li> <li>Modify VPN</li> <li>Delete VPN</li> <li>VPN Profiles                   <ul style="list-style-type: none"> <li>Create VPN Profile</li> <li>Delete VPN Profiles</li> <li>Modify VPN Profile</li> <li>Assign VPN Profile to Domain</li> </ul> </li> <li>Publish VPN</li> <li>Extranet Devices                   <ul style="list-style-type: none"> <li>Create Extranet Device</li> <li>Delete Extranet Device</li> <li>Modify Extranet Device</li> </ul> </li> <li>Assign IPSec VPN to Domain</li> </ul> </li> </ul>	Security Director > VPNs
	<ul style="list-style-type: none"> <li>Security Intelligence               <ul style="list-style-type: none"> <li>Profiles                   <ul style="list-style-type: none"> <li>Create Security Intelligence Profile</li> <li>Modify Security Intelligence Profile</li> <li>Delete Security Intelligence Profiles</li> </ul> </li> <li>Policies                   <ul style="list-style-type: none"> <li>Create Security Intelligence Policy</li> <li>Modify Security Intelligence Policy</li> <li>Delete Security Intelligence Policies</li> </ul> </li> <li>Dynamic Address Groups                   <ul style="list-style-type: none"> <li>Create Dynamic Address</li> <li>Modify Dynamic Address</li> <li>Delete Dynamic Addresses</li> </ul> </li> <li>Backup / Restore                   <ul style="list-style-type: none"> <li>Create Backup</li> <li>Delete Backups</li> <li>Restore</li> </ul> </li> <li>Information Sources                   <ul style="list-style-type: none"> <li>Update Feed Now</li> <li>Create Information Source</li> <li>Modify Information Source</li> <li>Delete Information Sources</li> </ul> </li> <li>Spotlight Connectors                   <ul style="list-style-type: none"> <li>Global Connector Settings</li> <li>Trusted Server CAs</li> <li>Associate Devices</li> <li>Update connector Configurations</li> </ul> </li> </ul> </li> </ul>	Security Director > Security Intelligence

Table 4: Predefined Roles for Security Director (*continued*)


Predefined Role	Task Group and Tasks	Application > Workspace
	<ul style="list-style-type: none"> <li>Downloads               <ul style="list-style-type: none"> <li>Signature Database                   <ul style="list-style-type: none"> <li>Download Configuration</li> </ul> </li> <li>Install Configuration</li> </ul> </li> </ul>	Security Director > Downloads
	<ul style="list-style-type: none"> <li>NAT Policies               <ul style="list-style-type: none"> <li>View NAT Policy</li> <li>Create NAT Policy</li> <li>Modify NAT Policy</li> <li>Delete NAT Policy</li> <li>Publish NAT Policy</li> </ul> </li> <li>NAT Pools               <ul style="list-style-type: none"> <li>Create NAT Pool</li> <li>Modify NAT Pool</li> <li>Delete NAT Pools</li> </ul> </li> <li>Port Sets               <ul style="list-style-type: none"> <li>Create PortSet</li> <li>Modify PortSet</li> <li>Delete PortSet</li> </ul> </li> <li>Assign Devices To NAT Policy</li> <li>Manage Policy Locks</li> <li>Unlock NAT</li> <li>Assign NAT Policy To Domain</li> </ul>	Security Director > NAT Policies

**Related Documentation** • [Security Director Overview on page 3](#)

## Security Director Dashboard

[Table 5 on page 22](#) lists the workspaces on the Security Director dashboard. This is the default dashboard of Security Director.

Table 5: Security Director Workspaces

Icons	Workspace Name	Tasks
	Firewall Policy	Create, manage, and publish firewall policies.
	IPS Policy	Create and manage IPS signatures, IPS signature sets, and IPS policies.
	NAT Policy	Create, manage, and publish NAT policies.
	VPN	Create, manage, and publish VPNs.
—	Object Builder	Create, modify, delete, and clone addresses, services, policy profiles, VPN profiles, application signatures, templates, template definitions, templates, and NAT pools.
—	Devices	Manage, discover, and add devices.
—	Job Management	Manage and view job status.
—	Security Director Devices	Update the devices with firewall policies, NAT policies, and VPN configurations.
—	Downloads	Download AppFirewall and IPS signatures.
—	Audit Logs	View audit logs by task, user, workspace, and application.

The Security Director dashboard has gadgets with information that is updated automatically and immediately. You can move gadgets on the dashboard and resize them. These changes persist when you log out and log in to the Security Director application. The gadgets displayed on the Security Director dashboard are shown in the figures that follow.

[Figure 5 on page 23](#) shows the Object Count gadget. This gadget shows the number of objects that are created from the Object Builder workspace. You can use this gadget to keep track of the objects available to create a security topology, IPsec VPNs, or security policies.

Figure 5: Object Count Gadget

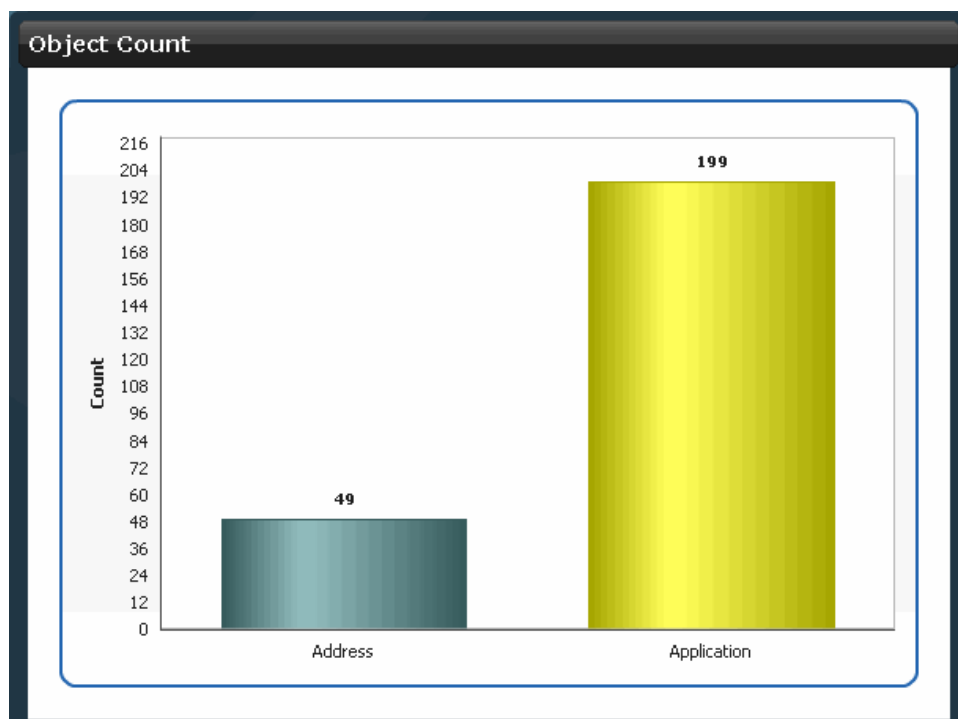
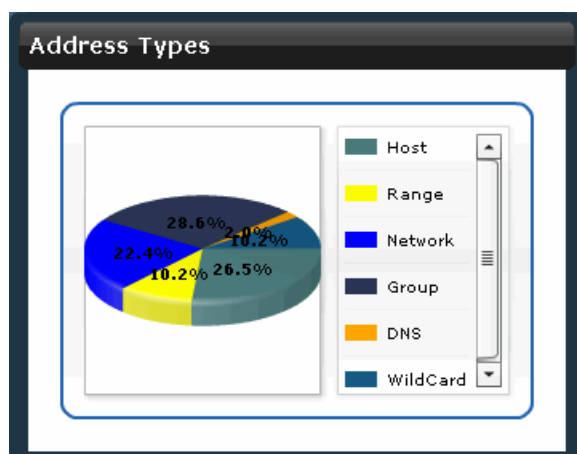


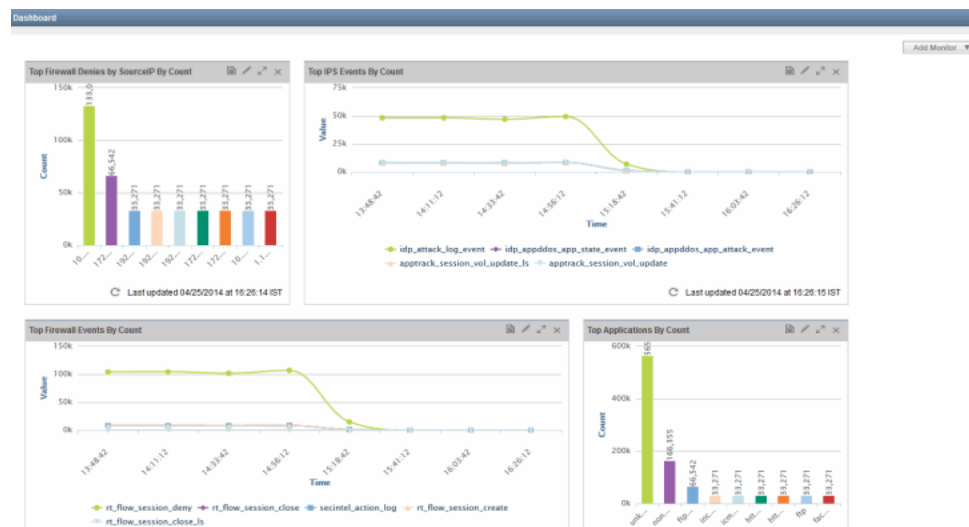
Figure 6 on page 23 shows the Address Types gadget. This gadget shows the different address types created using the Address Creation Wizard.

Figure 6: Address Types Gadget



If Security Director is installed with Junos Space Log Director application, the Security Director dashboard is replaced with the logging and reporting, as shown in Figure 7 on page 24.

Figure 7: Security Director Dashboard with Logging and Reporting



The new dashboard provides a unified view of the system and network status as retrieved from SRX Series Services Gateway firewalls. In addition to a default logging and reporting dashboard, you can define supported monitoring graphs that can be part of a dashboard. You can customize the dashboard as per the domain Role Based Access Control and changes are reflected to all users with in the domain.

## PART 2

# Configuring Dashboard Monitors

- [Creating and Managing Dashboard Monitors on page 27](#)



## CHAPTER 2

# Creating and Managing Dashboard Monitors

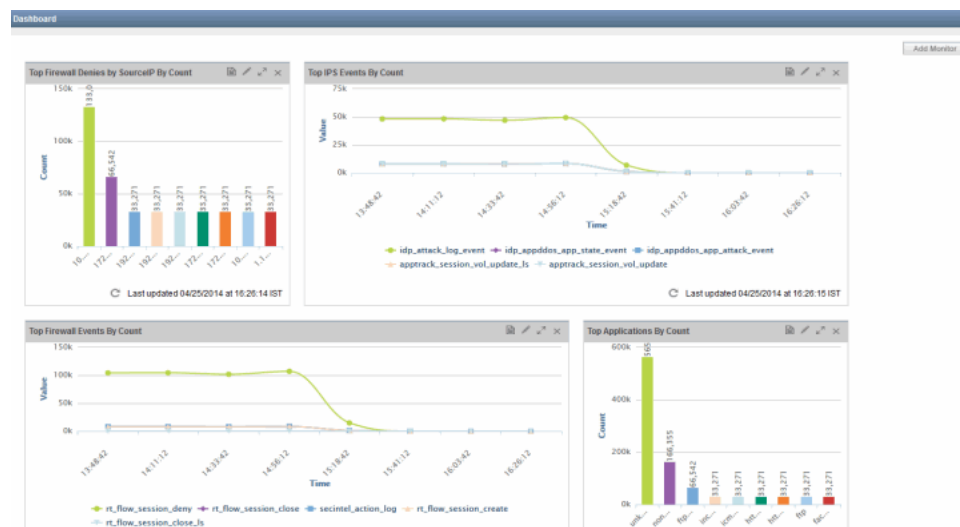
- [Logging and Reporting Dashboard Overview on page 27](#)
- [Understanding the Default Dashboard for Logging and Reporting on page 28](#)
- [Creating a Dashboard Monitor on page 31](#)
- [Managing Dashboard Monitors on page 37](#)

## Logging and Reporting Dashboard Overview

The Junos Space Security Director Logging and Reporting dashboard provides a unified overview of the system and network status retrieved from SRX Series Services Gateway firewalls.

When you install the Junos Space Security Director with Junos Space Log Director application, the new Junos Space Log Director dashboard is displayed, as shown in [Figure 8 on page 27](#).

**Figure 8: Security Director Logging and Reporting Dashboard**



To display the dashboard, select **Security Director > Dashboard** on the Security Director application tree on the left hand side.

You can create a dashboard monitor to meet your requirements. For example, a monitor can display a graph with top 10 applications accessed using VPN in the last 3 hours or the number of logins to devices in the last 10 minutes.

Using the dashboard, you can:

- Refresh monitors independently
- Edit monitors
- Delete monitors
- Maximize the monitors to provide a full-screen view
- Navigate to the event viewer page from an event-based monitor.

The dashboard page automatically adjusts the placement of the monitors to dynamically fit on the browser window without changing the order of the monitors. You can manually reorder the monitors using the drag and drop option. The monitors that you create are automatically placed at the end of the default monitors on the dashboard page.

## Understanding Role-Based Access Control for the Dashboard

Role-based access control (RBAC) has the following impact on the dashboard:

- You can create or edit monitors within a dashboard only if you have **EditDashboard** permissions.

### Related Documentation

- [Understanding the Default Dashboard for Logging and Reporting on page 28](#)
- [Creating a Dashboard Monitor on page 31](#)
- [Managing Dashboard Monitors on page 37](#)

## Understanding the Default Dashboard for Logging and Reporting

---

Junos Space Security Director Logging and Reporting provides a default dashboard. Dashboard monitors that you create are automatically added under Add Monitor.

### Default Monitors for Default Dashboard

The default dashboard provides five default monitors:

- Event-based
- CPU utilization
- Memory utilization
- Device health
- VPN status

Table 6 on page 29 provides the details of the default dashboard monitor parameters.

**Table 6: Default Dashboard Monitor Parameters**

Parameter	Value
<b>Top Firewall Denies by SourceIP by Count</b>	
Target	All firewalls denied
Group by	Source IP
Time Range	3 hours
Chart Type	Bar
Comparison	Disabled
Number to Display	Top 10
Interval	10 minutes
<b>Top IPS Events by Count</b>	
Target	All IPS events—Event category = IPS
Group by	Event type
Time Range	3 hours
Chart Type	Time series
Comparison	Disabled
Number to Display	Top 5
Interval	10 minutes
<b>Top Firewall Events by Count</b>	
Target	All firewall events—Event category=FIREWALL
Group by	Event type
Time Range	3 hours
Chart Type	Time series
Comparison	Disabled
Number to Display	Top 5
Interval	10 minutes

Table 6: Default Dashboard Monitor Parameters (*continued*)

Parameter	Value
<b>Top Applications by Count</b>	
Target	All events
Group by	Application
Time Range	3 hours
Chart Type	Bar
Comparison	Disabled
Number to Display	Top 10
Interval	10 minutes
<b>Top Destination IPs by Count</b>	
Target	All events
Group by	Destination IP
Time Range	3 hours
Chart Type	Bar
Comparison	Disabled
Number to Display	Top 10
Interval	10 minutes
<b>Top Source IPs by Count</b>	
Target	All events
Group by	Source IP
Time Range	3 hours
Chart Type	Bar
Comparison	Disabled
Number to Display	Top 10
Interval	10 minutes

- Related Documentation**
- [Logging and Reporting Dashboard Overview on page 27](#)
  - [Creating a Dashboard Monitor on page 31](#)
  - [Managing Dashboard Monitors on page 37](#)

## Creating a Dashboard Monitor

You can create a dashboard monitor using the option Add Monitor. This topic covers the following sections:

- [Creating the Event Based Monitor on page 31](#)
- [Creating the CPU Utilization Monitor on page 33](#)
- [Creating the Memory Utilization Monitor on page 34](#)
- [Creating the Device Health Monitor on page 35](#)
- [Creating the VPN Status Monitor on page 36](#)

### Creating the Event Based Monitor

To create an event-based monitor:

1. On the right side of the dashboard, click **Add Monitor > Event Based**.
2. Enter the following details:

Parameters	Description	Action
<b>General</b>		
Name	Specifies the unique name of the monitor.	Enter the monitor name.
Description	Specifies the short description of the monitor.	Enter the monitor description.
<b>Data</b>		

Parameters	Description	Action
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>The details of the filters displayed are:</p> <ul style="list-style-type: none"> <li>• <b>Select</b>—Specifies the check boxes for selecting the filter.</li> <li>• <b>Filter Name</b>—Specifies the name of the filter.</li> <li>• <b>Filter Description</b>—Specifies a description of the filter.</li> <li>• <b>Group By</b>—Specifies the selected group by option.</li> <li>• <b>Time Span</b>—Specifies the duration for which the data is displayed.</li> </ul> <p><b>NOTE:</b> The default value is last 3 hours.</p> <ul style="list-style-type: none"> <li>• <b>Filter By</b>—Specifies the list of default and user-created filters.</li> <li>• <b>Created</b>—Specifies the date on which the filter was created.</li> </ul>	<p>To add saved filters:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add Saved Filters</b>.</li> <li>2. Select the filters to be added.</li> <li>3. Click <b>Add Filter(s) to Monitor</b>.</li> </ol>
Add Data Criteria	Specify the data criteria based on the Time period, Group By, and Filter By option.	<p>To add data criteria:</p> <ol style="list-style-type: none"> <li>1. Select the data criteria.</li> <li>2. Click <b>Add Data Criteria</b>.</li> </ol>
Auto refresh interval	<p>Specifies the auto-refresh interval. The available options are:</p> <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 10 minutes</li> <li>• 15 minutes</li> <li>• 20 minutes</li> <li>• 25 minutes</li> <li>• 30 minutes</li> </ul>	Select the refresh time interval by scrolling the scroll bar.

## Display

Parameters	Description	Action
Chart Type	Specifies the chart used to display the data. The available options are: <ul style="list-style-type: none"> <li>• Time series</li> <li>• Bar</li> <li>• List</li> </ul>	Select the chart type for the monitor.
Number to display	Specifies the number of logs to be displayed. The available options are: <ul style="list-style-type: none"> <li>• Top 1</li> <li>• Top 5</li> <li>• Top 10</li> </ul>	Select the number of logs to be displayed.

3. Click **Create**.

The event-based monitor is created.

## Creating the CPU Utilization Monitor

To create the CPU utilization monitor:

1. On the right side of the dashboard, click **Add Monitor > CPU Utilization**.
2. Enter the following details:

Parameters	Description
<b>General</b>	
Name	Specifies the unique name of the monitor.
Description	Specifies the short description of the monitor.
<b>Data</b>	
Available/Selected	Specifies the devices that are available and can be added. The number of devices you can add is 10.
Time range	Specifies how long the data is displayed. The available options are: <ul style="list-style-type: none"> <li>• 15 mins</li> <li>• 30 mins</li> <li>• 1 hour</li> <li>• 3 hours</li> <li>• 12 hours</li> <li>• 1 day</li> <li>• 7 days</li> </ul>

Parameters	Description
Auto refresh interval	<p>Specifies the auto-refresh interval. The available options are:</p> <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 10 minutes</li> <li>• 15 minutes</li> <li>• 20 minutes</li> <li>• 25 minutes</li> <li>• 30 minutes</li> </ul>

3. Click **Create**.

The CPU utilization monitor is created.

## Creating the Memory Utilization Monitor

To create the memory utilization monitor:

1. On the right side of the dashboard, click **Add Monitor>Memory Utilization**.
2. Enter the following details:

Parameters	Description
<b>General</b>	
Name	Specifies the unique name of the monitor.
Description	Specifies the short description of the monitor.
<b>Data</b>	
Available/Selected	Specifies the devices that are available and can be added. The number of devices you can add is 10.
Time range	<p>Specifies how long the data is displayed. The available options are:</p> <ul style="list-style-type: none"> <li>• 15 mins</li> <li>• 30 mins</li> <li>• 1 hour</li> <li>• 3 hours</li> <li>• 12 hours</li> <li>• 1 day</li> <li>• 7 days</li> </ul>

Parameters	Description
Auto refresh interval	<p>Specifies the auto-refresh interval. The available options are:</p> <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 10 minutes</li> <li>• 15 minutes</li> <li>• 20 minutes</li> <li>• 25 minutes</li> <li>• 30 minutes</li> </ul>

3. Click **Create**.

The CPU utilization monitor is created.

## Creating the Device Health Monitor

To create the device health monitor:

1. On the right side of the dashboard, click **Add Monitor > Device Health**.
2. Enter the following details:

Parameters	Description
General	
Name	Specifies the unique name of the monitor.
Description	Specifies the short description of the monitor.
Data	
Available/Selected	Specifies the devices that are available and can be added. The number of devices you can add is 25.
Time range	<p>Specifies how long the data is displayed. The available options are:</p> <ul style="list-style-type: none"> <li>• 15 mins</li> <li>• 30 mins</li> <li>• 1 hour</li> <li>• 3 hours</li> <li>• 12 hours</li> <li>• 1 day</li> <li>• 7 days</li> </ul>

Parameters	Description
Auto refresh interval	<p>Specifies the auto-refresh interval. The available options are:</p> <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 10 minutes</li> <li>• 15 minutes</li> <li>• 20 minutes</li> <li>• 25 minutes</li> <li>• 30 minutes</li> </ul>

3. Click **Create**.

The device health monitor is created.



**NOTE:** Device health monitors, will always display the latest CPU/memory information available in the selected time range for a particular device. For Example: If the selected range is 30 minutes, the latest CPU/memory data point for that device in 30 minutes.

## Creating the VPN Status Monitor

To create the VPN status monitor:

1. On the right side of the dashboard, click **Add Monitor > VPN Status**.
2. Enter the following details:

Parameters	Description
<b>General</b>	
Name	Specifies the unique name of the monitor.
Description	Specifies the short description of the monitor.
<b>Data</b>	
Time range	<p>Specifies how long the data is displayed. The available options are:</p> <ul style="list-style-type: none"> <li>• 15 mins</li> <li>• 30 mins</li> <li>• 1 hour</li> <li>• 3 hours</li> <li>• 12 hours</li> <li>• 1 day</li> <li>• 7 days</li> </ul>

Parameters	Description
Auto refresh interval	<p>Specifies the auto-refresh interval. The available options are:</p> <ul style="list-style-type: none"> <li>• 5 minutes</li> <li>• 10 minutes</li> <li>• 15 minutes</li> <li>• 20 minutes</li> <li>• 25 minutes</li> <li>• 30 minutes</li> </ul>

3. Click **Create**.

The VPN status monitor is created.

#### Related Documentation

- [Logging and Reporting Dashboard Overview on page 27](#)
- [Understanding the Default Dashboard for Logging and Reporting on page 28](#)
- [Managing Dashboard Monitors on page 37](#)

## Managing Dashboard Monitors

You can edit, save, delete the dashboard monitors and the dashboard.

- [Using the Dashboard Monitors on page 37](#)

### Using the Dashboard Monitors

To use the monitors on the dashboard:

1. From the left navigation tree on the dashboard, select **Security Director > Dashboard**.

The Dashboard is displayed.

2. Click one of the following options:

- Jump to:
  - Event Viewer—Navigates to the Event Viewer page.
  - Device Management—Navigates to the Device Management page from the CPU utilization, memory utilization, and device health monitors.
  - VPN Management—Navigates to the VPN Management page.
- Edit monitor—Edits the dashboard monitor.



**NOTE:** The Edit Monitor page contains all available options for creating monitors.

- Maximize monitor—Maximizes the dashboard monitor.

- Delete monitor—Deletes the dashboard monitor.
- Refresh monitor—Refreshes the dashboard monitor.

## PART 3

# Using Event Viewer

- [Understanding Event Viewer Options on page 41](#)
- [Creating and Managing Event Viewer Filters on page 61](#)



## CHAPTER 3

# Understanding Event Viewer Options

- [Event Viewer Overview on page 41](#)
- [Using Event Viewer Options on page 42](#)
- [Using Event Viewer Table Options on page 51](#)

### Event Viewer Overview

---

When you install the Junos Space Security Director with the Junos Space Log Director application, the Event Viewer is displayed. You can select **Security Director > Event Viewer** from the Security Director application tree on the left side to view the Event Viewer. Using the Event Viewer, you can view information for event logs.

The Event Viewer provides:

- Event grouping and nongrouping— You can group events based on all columns. When you use the Group By option, for every distinct value of that field, one record is displayed and other columns in the row display MULTIPLE(n) for multiple values. If you do not use the Group By option, all the events are displayed.
- Event filtering based on user-defined filter conditions—You can apply specific filter conditions to view logs.
- Navigation among the Firewall Policies page, the IPS Policies page, and the logs—You can navigate to the policy that generated the events using the option **Jump to Policy**.
- Navigation among the NAT log and NAT policies page—You can navigate to the policy that generated the events using the option **Show Source NAT Policy** and **Show Destination NAT Policy**.
- Statistical overview of the events using charts—You can view charts that display top events by using Group By on all columns.
- Comparison charts—You can compare the number of events of a particular type for the current time period to the number of events of that type for the previous time period using a bar chart.
- Security Director address object resolution—You can resolve IP addresses in log fields, such as source IP, destination IP, NAT source IP and NAT destination IP, source IPv6 and destination IPv6 with Security Director address objects.

You can access the Event Viewer page using:

- **Security Director > Event Viewer** on the left navigation tree.
- **Firewall Rule > Firewall rule table > Show Log** on the Firewall Policies and IPS Policies pages.
- **Security Director > Dashboard > Jump to Event Viewer** in the dashboard monitor window.

## Understanding Role-Based Access Control for the Event Viewer

Role-Based Access Control (RBAC) has the following impact on the Event Viewer:

- You cannot view event logs created in other domains. However, a super user or any user with an appropriate role who can access a global domain can view logs in a subdomain, if a subdomain is created with visibility to the parent domain.
- You can only view logs from the devices that you can access and that belong to your domain.
- You can only view, not edit, a policy if you do not have edit permissions.

You must have the following permission under Role Based Access Controls > Roles:

- Event Viewer

### Related Documentation

- [Using Event Viewer Options on page 42](#)
- [Using Event Viewer Table Options on page 51](#)

---

## Using Event Viewer Options

This topic contains the following sections:

- [Using the Group By Selection Filter on page 43](#)
- [Using the Column Sets on page 44](#)
- [Selecting Event Viewer Table Columns on page 45](#)
- [Using Time Span on page 47](#)
- [Using the Event Viewer Settings on page 48](#)
- [Using Log View Options on page 48](#)
- [Clearing Filter Settings on page 49](#)
- [Returning to the Previous Page on page 49](#)
- [Creating a Report on page 49](#)
- [Creating an Alert on page 49](#)
- [Creating a Monitor on page 49](#)

## Using the Group By Selection Filter

To filter using the Group By selection:

1. On the Event Viewer page, select a Group By option. The available options are:

- None
- Event Category
- Event Name
- Source Zone
- Destination Zone
- Source IP
- Destination IP
- Source Port
- Destination Port
- Log Source
- Service
- User Name
- Event
- URL
- UTM Category or Virus Name
- Application
- Action
- Attack Name
- Policy Name
- Profile Name
- Source IPv6
- Destination IPv6
- Nested Application
- Reason
- Roles
- Rule Name
- NAT Source IP
- NAT Destination IP
- NAT Source Port

- NAT Destination Port
- NAT Source Rule
- NAT Destination Rule
- Attack Severity
- Category Name
- Sub Category Name
- Action Detail
- Feed Name
- Protocol ID
- Traffic Session ID
- Host Name
- Object Name
- Logical System Name



**NOTE:** The default option is **None**. Select **None** to list all events in the Event Viewer table.

---

2. Click **Filter**.

Event logs based on the Group By selection are displayed.

The Event Viewer table header displays the updated time duration for which the data was requested.

## Using the Column Sets

You can use the column set option to filter the logs based on the type such as firewall, UTM, security intelligence, and so on.

To filter using the column sets, select any or multiple options from the column set on the Event Viewer page.

The available options are:

- Default
- Firewall
- Screen
- IPS
- VPN
- UTM
- Control

- Security Intelligence
- All Columns

## Selecting Event Viewer Table Columns

To select Event Viewer table columns:

1. Click a column header.
2. Select the Column option.

Columns—Provides a list of columns with check boxes to add or remove columns from the Event Viewer table. [Table 7 on page 45](#) lists the columns that you can add to the Event Viewer table.

**Table 7: Event Viewer Columns**

Column Name	Description
Log ID	Displays a unique event log ID.
Time	Displays the time that the log was received.
Event name	Displays the event name.
Source Zone	Displays the source zone.
Destination Zone	Displays the destination zone.
Source IP	Displays the source IP address.
Destination IP	Displays the destination IP address.
Source Port	Displays the source port.
Destination Port	Displays the destination port.
Log source	Displays the IP address of the log source.
Service	Displays the service in the log.
User Name	Displays the username in the log.
URL	Displays the URL in the log.
UTM Category or Virus Name	Displays the UTM category in the log.
Application	Display the application in the log.
Action	Displays the action in the log.

Table 7: Event Viewer Columns (*continued*)

Column Name	Description
Attack Name	Displays the attack name in the log.
Policy Name	Displays the policy name in the log.
Profile Name	Displays the profile name in the log.
Source IPv6	Displays the source IPv6 IP address.
Destination IPv6	Displays the destination IPv6 address.
Nested Application	Displays the nested application in the log.
Reason	Displays the reason for the log generation.
Roles	Displays the roles in the log.
Rule Name	Displays the rule name in the log.
NAT Source IP	Displays the NAT source IP address.
NAT Source Port	Displays the NAT source port.
NAT Destination IP	Displays the NAT destination IP address.
NAT Destination Port	Displays the NAT destination port.
NAT Source Rule	Displays the NAT source rule.
NAT Destination Rule	Displays the NAT destination rule.
Attack Severity	Displays the severity of the log.
Category Name	Displays the category name in the log.
Sub Category Name	Displays the subcategory name in the log.
Action Detail	Displays the action details in the log.
Feed Name	Displays the feed name in the log.
Protocol ID	Displays the protocol ID in the log.
Traffic Session ID	Displays the security intelligence session ID in the log.
Event Category	Displays the event category of the log.
Host Name	Displays the host name in the log.

Table 7: Event Viewer Columns (*continued*)

Column Name	Description
Object Name	Displays the object name in the log.
Logical System Name	Displays the logical system name in the log.

To view a list of event logs in the Event Viewer table:

1. Select a Group By option in the drop-down list and select the time span.  
For example: Select **None** and the time span as **Last 3 Hours**.
2. Click **Filter**.  
  
The Event Viewer table header displays the time duration for which the data was requested.  
  
The Event Viewer table is empty if no logs match the filter condition. The table footer displays the number of logs that match the filter. If there are more than 5,000 events. You must refine your filter criteria to see those logs.
3. Change the time span and click **Filter** or press **Enter** to refresh the Event Viewer table.
4. Select a log displayed in the Event Viewer table.  
  
A detailed view of the log is displayed in the detailed log view section at the bottom of the page.

## Using Time Span

To use time span:

1. Specify the time period to check the logs.

The available options are:

- Hour(s)
- Day(s)
- Week(s)
- Month(s)
- Custom



**NOTE:** The default value is Last 5 minutes.

Logs for the selected time span are displayed in the Event Viewer table.

2. Click **Filter**.

All logs are displayed.

A detailed view of the log is displayed in the detailed log view section at the bottom of the Event Viewer page.

You can customize the time span to meet your requirements.

To customize the time span:

1. Select **Custom** from the time period.
2. Select the from and to date using the calendar option and time from the drop-down.
3. Click **Filter**.

## Using the Event Viewer Settings

You can choose log display time and Security Director object settings that meet your requirements.

To use the Event Viewer settings:

1. Select the log display time:
  - Local time zone—Displays logs in the local time zone.
  - UTC time zone—Displays logs in the UTC time zone.



**NOTE:** By default, the Local time zone option is enabled.

2. Show SD Object—Select to display Security Director address objects.

By default, the Show SD Object option is enabled.



**NOTE:** If there is no corresponding Security Director address for a specific IP address, only the IP address is displayed.

3. Security Events Only—Select to display security events.
4. Page size—Key in the number of events that you want to display. The range is 200 through 10,000 events.
5. Click **Save** to save the changes.

## Using Log View Options

The icons on the upper right side of the Event Viewer table enable you to switch between the split view or grid view.

1. Select an icon:
  - Split view—Displays logs as graphs and tables when logs are grouped by log field. When the logs are not grouped, the Event Viewer table and the details window are displayed.

- Grid view—Displays logs in a table when event logs are not grouped.



**NOTE:** By default, the grid view mode is enabled.

## Clearing Filter Settings

To clear filter settings, click **Clear Filter Settings**.

## Returning to the Previous Page

To move back to the previous page, click **Back**.

## Creating a Report

You can create a report from the Event Viewer.

1. Select **Security Director > Event Viewer**. Note that every report must have an aggregation point.
2. Select a **Group By** option to create a report.
3. Select **Create > Create Report**.
4. Enter the report definition options in Use Data to Create Report window.
5. Click **Create Report**.

## Creating an Alert

You can create an alert from the Event Viewer.

1. Select **Security Director > Event Viewer**.
2. Select a **Group By** option to create an alert.
3. Select **Create > Create Alert**.
4. Enter the alert definition options in Use Data to Create Alert window.
5. Click **Create Alert**.

## Creating a Monitor

You can create a monitor from the Event Viewer.

1. Select **Security Director > Event Viewer**.
2. Select a **Group By** option to create a monitor.
3. Select **Create > Create Monitor**.
4. Enter the alert definition options in Use Data to Create Monitor window.
5. Click **Create Monitor**.

- Related Documentation**
- [Event Viewer Overview on page 41](#)
  - [Using Event Viewer Table Options on page 51](#)

## Using Event Viewer Table Options

---

This section covers the following topics:

- [Using Event Viewer Table Options in Nongrouped Mode on page 51](#)
- [Creating an Address Object on page 53](#)
- [Using Event Viewer Table Options in Grouped Mode on page 53](#)
- [Example: Using Event Viewer Table Options in Grouped Mode on page 54](#)
- [Using the Detailed Log View on page 54](#)
- [Using the Display Option on page 56](#)
- [Using Event Graphs on page 57](#)
- [Using Comparison Charts on page 57](#)
- [Using the Show Logs Option to Navigate from the Event Viewer to the Policies Page on page 58](#)
- [Using the Show Logs Option to Navigate from Policies to Logs on the Event Viewer Page on page 59](#)
- [Creating an Exempt Rule on page 59](#)

### Using Event Viewer Table Options in Nongrouped Mode

To use the Event Viewer table options in nongrouped mode:

1. Select and right-click a cell.

Table 8 on page 52 describes the Event Viewer table options.

**Table 8: Event Viewer Table Options**

Option	Description	Example
Show policy	Navigates to the Firewall Policies or IPS Policies page that generates the logs.	–
Filter on Cell Data	Updates the logs in the Event Viewer table with field values matching the selected cell value.  The value selected is appended to the existing filter.	For example: If you select an srcip column with the value 2.2.2.2 and click <b>Filter on cell data</b> , then the filter string will be updated with <b>srcip equals 2.2.2.2</b> .
Exclude Cell Data	Updates the logs in the Event Viewer table without the field values matching the selected cell value.  <b>NOTE:</b> The option Exclude cell data is not available in the <b>Time</b> column.	For example: If you select an srcip column with the value 2.2.2.2 and click <b>Exclude cell data</b> , then the filter string will be updated with <b>srcip not equals 2.2.2.2</b> .
Show Raw Log	Displays the actual logs received from the SRX Series devices.	For example: Log ID 147696: 1 2014-04-08T11:00:03.917Z - snmpd 1099 SNMPD_AUTH_FAILURE [junos@2636.1.1.1.2.96 function-name="nsa_log_community" message="unauthorized SNMP community" source-address="10.207.99.91" destination-address="10.207.99.72" index1="public"] nsa_log_community: unauthorized SNMP community from 10.207.99.91 to 10.207.99.72 (public)
Create Address Object	Allows you to create address objects in Security Director.  <b>NOTE:</b> This option is available only on source IP address, destination IP address, NAT source IP, NAT destination IP, source IPv6, and destination IPv6.	–
Create Exempt Rule	Allows you to exempt the rule.	--
Hide Column	Allows you to hide a column.	–
Show Exact Match	Allows you to see the exact match of the logs for the selected log based on the column excluding the time and log ID.	For example: "EventName equals RT_FLOW_SESSION_CREATE AND SrcIP equals 1.1.1.1 AND DstIP equals 172.19.51.235 AND SrcPort equals 56752 AND DstPort equals 1025 AND LogSource equals 10.207.99.43 AND UserName equals fabien AND AttackName notexists"

Table 8: Event Viewer Table Options (*continued*)

Option	Description	Example
Show Source NAT Policy	<p>Navigates to the corresponding NAT policy in the NAT Policies page.</p> <p>For a log that was generated by the NAT source rule, src-nat-rule-name will be populated with rule name and NAT destination rule will be None.</p>	--
Show Destination NAT Policy	<p>Navigates to the corresponding NAT policy in the NAT Policies page.</p> <p>For a log that was generated by the NAT destination rule, dst-nat-rule-name will be populated with rule name and NAT source rule will be None.</p>	--

## Creating an Address Object

To create a Security Director address object:

1. Right-click the cell and select **Create Address Object** and then enter the following details:
  - Name—Name of the address object.
  - Description—Description of the address object.
2. Click **Save** to save the address object.

The host address is created, and the Security Director address object name is displayed in the address or destination address column.

## Using Event Viewer Table Options in Grouped Mode

When you use the Group By option to combine logs based on a specific field, for every distinct value of that field, one record is displayed. Other columns in the row display MULTIPLE(n) for multiple values. By default, Group By tables are always sorted by count. The Group By column is the first column in the table and is followed by the count column. The count column is not displayed when the table is not grouped.

To see more information on Group By logs:

1. Click **Multiple**.
 

The Event Viewer table displays the grouped log details associated with multiple values.
2. Select a row and click **Show All Logs**.
 

The Event Viewer table view is switched to nongrouped view.

The Group By drop-down list is reset to **None**.

## Example: Using Event Viewer Table Options in Grouped Mode

In this sample scenario, assume that the logs are grouped based on event name and that there are multiple destination IP addresses for a specific event name.

To see more information on grouped logs:

1. Click **Multiple** in the Destination IP column of the row for which you want to see more details.

The Event Viewer table displays the grouped log details.

The filter string displays the expression **SrcIP equals 1.1.1.1**. The logs are grouped based on source IP with the filter **SrcIP equals 1.1.1.1**.

2. Click **Multiple** in the Event Name column of the row to see more information.

The Event Viewer table displays the grouped log details.

The filter string displays the expression **SrcIP equals 1.1.1.1 AND DstIP equals 2.1.1.1**. The logs are grouped based on service with the filter **SrcIP equals 1.1.1.1 AND DstIP equals 2.1.1.1**.

3. Select a row, right-click, and select **Show all Logs**.

The Event Viewer table view is switched to nongrouped view with the filter **SrcIP equals 1.1.1.1 AND DstIP equals 2.1.1.1 AND EventName equals rt\_screen\_ip**.

The Group By drop-down list is reset to **None**.

## Using the Detailed Log View

To use the detailed log view:

1. Select a log in the Event Viewer table.

The details of the log selected on the Event Viewer page are displayed in the detailed log view section at the bottom of the Event Viewer page. [Table 9 on page 54](#) lists the details of the logs.

**Table 9: Detailed Log View**

Option	Description
<b>General Information</b>	
Log ID	Displays the unique log ID.
Log Source	Displays the IP address of the log source.
Local Time	Displays the time at which the log was received.
UTC Time	Displays logs in the UTC time zone.
Category	Displays the category of the logs.

Table 9: Detailed Log View (*continued*)

Option	Description
Severity	Displays the severity of the logs.
Reason	Displays the reason the log was generated.
Host Name	Displays the host name in the log.
<b>Source Information</b>	
Source IP	Displays the source IP address.
Source Port	Displays the source port.
Source Address	Displays the source port address.
Source Zone	Displays the source zone.
NAT Source IP	Displays the NAT source IP address.
NAT Source Port	Displays the NAT source port.
NAT Source Rule	Displays the NAT source rule.
<b>Destination Information</b>	
Destination IP	Displays the destination IP address.
Destination Port	Displays the destination port.
Destination Address	Displays the destination port address.
Destination Zone	Displays the destination zone.
NAT Destination IP	Displays the NAT destination IP address.
NAT Destination Port	Displays the NAT destination port.
NAT Destination Rule	Displays the NAT destination rule.
<b>Log Information</b>	
Attack Name	Displays the attack name in the log.
Policy Name	Displays the policy name.
Username	Displays the username in the log.
Logical System Name	Displays the logical system name in the log.
Application	Display the application in the log.

Table 9: Detailed Log View (*continued*)

Option	Description
Service	Displays the service in the log.
Nest Application	Displays the nested application in the log.
Rule Name	Displays the rule name in the log.
Session ID	Displays the session ID in the log.
<b>Security Information</b>	
UTM Category	Displays the UTM category in the log.
Action Details	Displays the action details.
Roles	Displays the roles.
URL	Displays the URL in the log.
Profile Name	Displays the profile name in the log.
Path Name	Displays the pathname in the log.
Object Name	Displays the object name in the log.
<b>Security Intelligence Information</b>	
Category	Displays the category name in the log.
Sub Category	Displays the subcategory name in the log.
Action Details	Displays the action details in the log.
Feed Name	Displays the feed name in the log.
Protocol ID	Displays the protocol ID in the log.

## Using the Display Option

To use the display option:

1. Select a Group By option.
2. Click **Filter** or press **Enter**.

The Group By logs are displayed in the Event Viewer table, and the Display option is enabled.

3. Click **Display > Display Number**.
4. Select an option to display the top (n) results.

## Using Event Graphs

To use event graphs:

1. Select a **Group By** option.
2. Click **Filter** or press **Enter**.

The grouped logs are displayed in the Event Viewer table.

3. Select **Split View**.

The Event Viewer displays a bar graph and a table for the top (n) grouped items.

4. Select a row in the table below the graph.

The corresponding bar in the graph is highlighted.

5. Click an item in the bar graph.

You will be switched to nongrouped view, which displays all logs related to the filter criteria.

## Using Comparison Charts

Using comparison charts, you can compare log data based on different time periods. You can also see the log data distribution at different time intervals.

To view the comparison charts:

1. Select the event category from the **Column Sets**.
2. Select a **Group By** option.

The events related to the specific column are displayed.

3. Select the **Chart Type** as bar chart.
4. Select the **Compare Time Period To** option.

[Table 10 on page 57](#) lists the options for compare time period.

**Table 10: Compare Time Period**

Option	Description
None	Compares the current time period with the same time period in the past.
Previous Period	Compares the current time period with the last occurrence of the same time period.
One hour ago	Compares the current time period with the same time period one hour earlier.
One week ago	Compares the current time period with the same time period one week earlier.
One month ago	Compares the current time period with the same time period one month earlier.

Table 10: Compare Time Period (*continued*)

Option	Description
Custom	<p>Compares the current time period with the custom time period that you specify.</p> <p>You can select the start time; the end time is selected automatically based on the selected time period.</p> <p>For example, if your selected time period is last 5 minutes, an equivalent time period is automatically selected in the calendar on the compare to Start Date and Start Time fields, usually the period immediately before the Current Period. You can also specify your custom start date and time and the end date and end time is selected automatically for the selected time period.</p>

**NOTE:**

- By default, the top row in the event table is selected and the graph is displayed. You can compare events based on only one event name at a time.
- You can drill down to the event by clicking the bar or time graph.
- You cannot perform the time comparison if the system has no data available for comparison.

### Using the Show Logs Option to Navigate from the Event Viewer to the Policies Page

You can navigate from the Event Viewer page to the Firewall Policies page or IPS Policies page that displays the policy associated with the logs. To navigate from the Event Viewer page to the Firewall Policies page or IPS Policies page:

1. Launch Event Viewer, and query Firewall or IPS logs.

The firewall and IPS logs are displayed.

2. Right-click a log and select **Show Policy**.

The current rule associated with the logs displays the changes on the IPS Policies page.

3. For the Firewall policy, click one of the options:

- Changes in the Rule—Displays the changes in the rule.

The previous rule and the current rule are displayed. You have the options to either **Go to the current rule** or **Go to Policy Comparison**. The Go To Policy Compare option allows you to compare versions.

- Go to Current Rule—Navigates to the current rule.

## Using the Show Logs Option to Navigate from Policies to Logs on the Event Viewer Page

You can navigate from the Firewall Policies page or IPS Policies to view logs. To navigate from logs to a policies page:

1. Select a Firewall Policy and select a rule.
2. Right-click **Show Events Generated by Rule**.

The event logs that contain the rule name associated with the policy are displayed on the Event Viewer page.

## Creating an Exempt Rule

To create an exempt rule. Filter the IPS category logs, right-click, and select **Create an exempt rule**. An IPS rule is added at the beginning of the Rule Type Exempt list on the IPS policy page.

- Related Documentation**
- [Event Viewer Overview on page 41](#)
  - [Using Event Viewer Options on page 42](#)



## CHAPTER 4

# Creating and Managing Event Viewer Filters

- [Filter Management Overview on page 61](#)
- [Understanding Advanced Filter Options on page 62](#)
- [Creating an Event Viewer Filter Using Advanced Filter Options on page 66](#)
- [Managing Filters in the Event Viewer on page 67](#)

### Filter Management Overview

---

Filters are used to search logs and view information about filter condition, time, or fields in the logs. You can configure basic and advanced filters to match the filtering conditions. You can either load existing filters or define a new filter.

A filter allows you to enter specific information that must be displayed on the Event Viewer page; for example, the columns in the Event Viewer table, the type of graph, the time period, and the aggregation point. When you change an existing filter or create a new filter, the Event Viewer table and event graph are updated automatically. If filters contain time details, the time control in Event Viewer is updated with the time specified in the filter.

Filters provide:

- Quick access to critical information—If you are a firewall administrator, you might have to regularly deny traffic from a specific application or a specific set of addresses. You might also have to allow or deny specific application access to some users. To achieve these conditions, you must set user search criteria, scan through the firewall logs that match that criteria, and display the matching logs.
- Filter sharing among users—Other users in your domain can use the filters you create without modifying or deleting the filters.
- Filter usage across multiple functional areas—Filters can be used across multiple functional areas such as the Event Viewer, dashboard monitor, alerts, and reports.

## Understanding Role-Based Access Control for Filter Management

Role-based access control (RBAC) has the following impact on filter management:

- You cannot view filters that are created in other domains.
- When you create or edit a filter, you must use devices in the same domain. If a filter contains devices from different domains, logs are not displayed even if they match the filter condition.
- You can create or edit a filter only if you have create and edit permissions.

You must have the following permissions under Role Based Access Controls > Roles:

- **Event Viewer** to view Event Viewer.
- **Create Filter** to create filters.
- **Modify Filter** to modify filters.
- **Delete Filter** to delete filters.

### Related Documentation

- [Creating an Event Viewer Filter Using Advanced Filter Options on page 66](#)
- [Managing Filters in the Event Viewer on page 67](#)
- [Understanding Advanced Filter Options on page 62](#)

---

## Understanding Advanced Filter Options

The Filter Manager provides advanced filtering options. You can filter values for any field in the log.

To use advanced filter options:

- Click the plus sign (+) next to the Filter By option.

[Table 11 on page 63](#) lists the advanced filter options and includes a description and example of each option. [Table 12 on page 65](#) shows the operators supported on the Group By column fields.

Table 11: Advanced Filter Options

Filter Options	Description	Example
Filter String	<p>The options available are:</p> <ul style="list-style-type: none"> <li>• IP—Specifies the IP address.</li> <li>• Name—Specifies the string name. The string name can include uppercase or lowercase letters (a-z) or (A-Z), numbers 0-9, underscores (_), single quotes ('), double quotes ("), hyphens, or (+) indicating that the preceding options can occur one or more times.</li> <li>• Expression—Specifies the key operator value.</li> </ul>	<ul style="list-style-type: none"> <li>• IP—1.2.3.4, 1.2.3.5</li> <li>• Name—<b>Joseph Lagrange</b>.</li> <li>• Expression—dstip = 1.2.3.4 and srcip = 1.2.3.5.</li> </ul>
Term Operator	<p>The options available are:</p> <ul style="list-style-type: none"> <li>• AND—Specifies that two filter strings must be combined.</li> <li>• OR—Specifies that either of the two filters strings can be used.</li> </ul>	<ul style="list-style-type: none"> <li>• AND—Firewall = Deny and srcip = 1.2.3.4.</li> <li>• OR—Firewall = Deny or srcip = 1.2.3.4.</li> </ul>

Table 11: Advanced Filter Options (*continued*)

Filter Options	Description	Example
Key	<p>The options available are:</p> <ul style="list-style-type: none"> <li>Log ID—Specifies the log ID.</li> <li>EventName—Specifies the event name.</li> <li>SrcIP—Specifies the source IP address.</li> </ul> <p><b>NOTE:</b> You can type either src or srcip to indicate the source address.</p> <ul style="list-style-type: none"> <li>DstIP—Specifies the destination IP address.</li> <li>SrcPort—Specifies the source port address.</li> <li>DstPort—Specifies the destination port address.</li> <li>LogSource—Specifies the source from which the logs are generated.</li> <li>UserName—Specifies the user name.</li> <li>AttackName—Specifies the attack name.</li> <li>Application—Specifies the type of application.</li> <li>AttackSeverity—Specifies the attack severity.</li> <li>DstIPv6—Specifies the destination IPv6.</li> <li>DstZone—Specifies the destination zone.</li> <li>EventCategory—Specifies the event category.</li> <li>NatDstIP—Specifies the NAT destination IP.</li> <li>NatSrcIP—Specifies the NAT source IP.</li> <li>NatDstPort—Specifies the NAT destination port.</li> <li>NatSrcPort—Specifies the NAT source port.</li> <li>NestedApp—Specifies the nested application.</li> <li>PolicyName—Specifies the policy name.</li> <li>Reason—Specifies the reason.</li> <li>RuleName—Specifies the rule name.</li> <li>Service—Specifies the service.</li> <li>SrcIPv6—Specifies the source IPv6 address.</li> <li>SrcZone—Specifies the source zone.</li> <li>TrafficSessionID—Specifies the traffic session ID.</li> <li>HostName—Specifies the host name.</li> <li>ObjectName—Specifies the object name.</li> <li>LogicalSystemName—Specifies the logical system name.</li> </ul>	<ul style="list-style-type: none"> <li>LogID—LogID equals 17492896</li> <li>EventName—EventName equals IDP_APPDDOS_APP_STATE_EVENT</li> <li>SrcIP—SrcIP equals 1.3.4.5,1.3.4.6,1.3.4.26</li> </ul> <p>In this example, multiple IP addresses or values are to be matched. A comma indicates the logical <b>OR</b> operator.</p> <ul style="list-style-type: none"> <li>DstIP—DstIP equals 192.167.2.1</li> <li>SrcPort—SrcPort equals 1.3.4.5,1.3.4.6,1.3.4.26</li> <li>DstPort—DstPort equals 23,35,67</li> <li>LogSource—logsource srx</li> <li>UserName—UserName equals matt</li> <li>AttackName—AttackName equals 'No TCP flag'</li> <li>Application—application = aol,http,yahoo and srcip = 2.3.4.5</li> <li>AttackSeverity—AttackSeverity equals INFO</li> <li>DstIPv6—DstIPv6 equals 2000::1</li> <li>DstZone—DstZone equals Exploit</li> <li>EventCategory—EventCategory equals IPS</li> <li>NatDstIP—NatDstIP equals 172.19.51.235</li> <li>NatSrcIP—NatSrcIP equals 1.1.1.1</li> <li>NatDstPort—NatDstPort equals 1025</li> <li>NatSrcPort—NatSrcPort equals 56752</li> <li>NestedApp—NestedApp equals INCONCLUSIVE</li> <li>PolicyName—PolicyName equals AppDDOS</li> <li>Reason—Reason equals policy deny</li> <li>RuleName—RuleName equals DDOS</li> <li>Service—Service equals HTTP</li> <li>SrcIPv6—HTTPSrcIPv6 equals 2000::2</li> <li>SrcZone—SrcZone equals trust</li> <li>TrafficSessionID—TrafficSessionID equals 1024</li> <li>HostName—Hostname equals srx99_74</li> <li>ObjectName—ObjectName equals www.bet365.com</li> <li>LogicalSystemName—LogicalSystemName equals AP7</li> </ul>

Table 11: Advanced Filter Options (*continued*)

Filter Options	Description	Example
Operator	<p>The options available are:</p> <ul style="list-style-type: none"> <li>= — Specifies that the key is equal to the value provided.</li> <li>!= — Specifies that the key is not equal to the value provided.</li> <li>&gt; — Specifies that the key is greater than the value provided.</li> <li>&lt; — Specifies that the key is less than the value provided.</li> <li>&lt;= — Specifies that the key is less than or equal to the value provided.</li> <li>&gt;= — Specifies that the key is greater than or equal to the value provided.</li> <li>startswith — Specifies that the key starts with the value provided.</li> <li>endswith — Specifies that the key ends with the value provided.</li> <li>exists — Specifies that the key exists.</li> <li>notexists — Specifies that the key does not exist.</li> </ul>	<ul style="list-style-type: none"> <li>= — <b>srcip = 1.2.3.4</b></li> <li>!= — <b>dstZone != 1.2.3.4</b></li> <li>&gt; — <b>LogSource &gt; 1.2.3.4</b></li> <li>&lt; — <b>LogSource &lt; 1.2.3.4</b></li> <li>&lt;= — <b>LogSource &lt;= 1.2.3.4</b></li> <li>&gt;= — <b>LogSource &gt;= 1.2.3.4</b></li> <li>startswith — <b>EventName startswith KMD</b></li> <li>endswith — <b>EventName endswith PHASE</b></li> <li>exists — <b>EventName exists</b></li> <li>notexists — <b>EventName notexists</b></li> </ul>
Value	<p>The options available are:</p> <ul style="list-style-type: none"> <li>IP — Specifies the IP address.</li> <li>String — Specifies the event names, event categories, or any user-defined strings.</li> </ul>	<ul style="list-style-type: none"> <li>IP — <b>10.204.49.43, 10.203.49.5</b></li> <li>String — <b>Joseph Lagrange</b>.</li> </ul>

Table 12: Operators Supported in the Group By Column fields

Column Name	Usable Operators	Unusable Operators
Src IP	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
Dst IP	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
Src IPv6	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
Dst IPv6	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
NAT Src IP	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
NAT Dst IP	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=

Table 12: Operators Supported in the Group By Column fields (*continued*)

Column Name	Usable Operators	Unusable Operators
Log Source	equals, notequals, exists, notexists, =, !=	startswith, endswith, contains, <, <=, >, >=
Src Port	equals, notequals, exists, notexists, =, !=, <, <=, >, >=	startswith, endswith, contains
Dst Port	equals, notequals, exists, notexists, =, !=, <, <=, >, >=	startswith, endswith, contains
NAT Src Port	equals, notequals, exists, notexists, =, !=, <, <=, >, >=	startswith, endswith, contains
NAT Dst Port	equals, notequals, exists, notexists, =, !=, <, <=, >, >=	startswith, endswith, contains
Log ID	equals, notequals, exists, notexists, =, !=, <, <=, >, >=	startswith, endswith, contains



**NOTE:** While creating the filters, if you use invalid or unsupported operators (as described in the table), the result displayed will ignore the invalid filter condition.

**Related Documentation**

- [Creating an Event Viewer Filter Using Advanced Filter Options on page 66](#)
- [Managing Filters in the Event Viewer on page 67](#)

## Creating an Event Viewer Filter Using Advanced Filter Options

To create an Event Viewer filter:

1. Select **Security Director > Event Viewer**.

The Event Viewer filter management tabular view is displayed.

The Event Viewer page is divided into the following sections:

- Filter options
- Event view
- Event details

2. Click the plus sign (+) next to the Filter By option.

The filter keys available are displayed alphabetically in a drop-down list.

3. Type the exact key in the filter text field, or select the key from the drop-down key list.

The key appears in the filter bar. While typing in the values, you are prompted with suggestions in the drop-down list whenever possible.

For example: **EventName =**

4. Continue to add filter expressions *<key> space <operator> space <value>*.

The key appears, along with the value combination in the filter bar.

For example: **EventName = LOGIN\_FAILED**

5. Repeat the Step 3 and Step 4 to add additional filter expressions.

The available filter keys are displayed alphabetically in the drop-down list.

For example: **EventName = LOGIN\_FAILED AND SrcIP =**

6. Type in the required IP address.

For example: **EventName = LOGIN\_FAILED SrcIP = 192.168.45.350**

The term operator **AND** is included in the filter bar automatically.

For example: **EventName = LOGIN\_FAILED AND SrcIP = 192.168.45.350**

7. Click **Filter** or press **Enter**.

The event logs for **EventName = LOGIN\_FAILED AND SrcIP = 192.168.45.350** are displayed.



**NOTE:** The filters that you have typed will appear in the filter history until the next session.

---

**Related  
Documentation**

- [Understanding Advanced Filter Options on page 62](#)
- [Managing Filters in the Event Viewer on page 67](#)

---

## Managing Filters in the Event Viewer

---

You can edit, save, delete, or search filters on the Event Viewer page. To open the filter options, select **Security Director > Event Viewer > Load Filters** on the Event Viewer page.

You can perform the following tasks:

- [Using Load Filter Selections on page 68](#)
- [Using the Filter Manager on page 68](#)
- [Searching Filters in the Filter Manager on page 69](#)
- [Editing Event Viewer Filters on page 70](#)
- [Saving an Event Viewer Filter on page 70](#)
- [Deleting an Event Viewer Filter on page 70](#)
- [Filtering on Multiple String Values on page 71](#)

## Using Load Filter Selections

To use load filters:

1. On the right side of the Event Viewer page, select **Security Director > Load Filter**.  
The drop-down list displays the available filters.
2. Select one of the filters available in the drop-down list.  
The Event Viewer page displays the filter details.
3. To search filters, type the filter name in the Load Filter search bar and click **Search**.  
Filters matching your search criteria are displayed.

## Using the Filter Manager

To use the Filter Manager:

1. Select **Security Director > Load Filters**.  
The saved filters are listed. Only 10 filters are displayed in the Load Filter drop-down list.
2. To view more filters, select **Load Filters > More Filters**.  
The Filter Management window appears.
3. Under **Actions**, select one of the following:
  - Duplicate—Creates a copy of the filter.
  - Rename—Provides the option to rename and save the filter.
  - Edit Description—Provides the option to edit the filter description and save the filter.
4. To view existing filters, select one of the following:
  - All Saved Filters—Displays all the saved filters.
  - My Filters—Displays the filters you created.
  - Default Filters—Displays the default filters.  
The requested filters are displayed.

The following are the default filters that are available:

- Top Web Apps
- Top Applications Blocked
- Top URL's Detected
- Top URL's Blocked
- Top Viruses Detected
- Top Spam Sources

- Top Screen Attackers
- Top Screen Victims
- Top Screen Hits
- Top Firewall Rules
- Top Firewall Deny Sources
- Top Firewall Deny Destinations
- Top Firewall Service Deny
- Top IPS Attack Detected
- Top IPS Attack Blocked
- Top IPS Attacks by Severity
- Top IPS Attack Sources
- Top IPS Attack Destinations
- Top IPS Rules
- Top Activities By User
- Top Roles
- Top FW Denies
- Top IPS Event
- Top Source IPs
- Top Security Intelligence
- Top Security Intelligence Action Blocked

### Searching Filters in the Filter Manager

To search an Event Viewer filter:

1. Select **Security Director > Load Filters > More Filters**.

The Filter Management window is displayed.

2. In the search bar, type one of the following:

- Name
- Description
- Created by
- Date Last Modified

The requested filters are displayed.

## Editing Event Viewer Filters

To edit an Event Viewer filter:

1. Select a filter.

The filter details are displayed in the filter bar.

2. Edit the filter string.
3. Click **Save**.

The filter is saved and the database is updated.

## Saving an Event Viewer Filter

To save an Event Viewer filter:

1. Select a filter.

The Filter Management window is displayed.

2. Edit the filter string.
3. Click **Save**.

The filter is saved and the database is updated.

## Deleting an Event Viewer Filter

To delete an Event Viewer filter:

1. Select **Security Director > Load Filters > More Filters**.

The Filter Management window appears.

2. Select the filter.
3. On the left side of the Filter Management page window, click the delete button (-).

The delete confirmation window displays the message. **Do you wish to permanently delete the selected filter?**

4. Click **Yes** to confirm the deletion.

The selected filter is deleted.



**NOTE:** To delete multiple filters, select the filters using the check box and click the delete icon (-).

You can delete filters only if you are the administrator of the domain or have created the filter.

---

## Filtering on Multiple String Values

You can select multiple string values for filtering by selecting the required column cell from the Event Viewer. This feature enables you to create a filter string to view specific information.

To create a filter based on multiple string values:

1. Select **Security Director > Event Viewer** and then click **Construct Filter String**.
2. Select one or more column cells by clicking the column cell.

The filter conditions appear as a comma-delimited string at the top of the filter by list.

3. Click **Ctrl now**.

### Related Documentation

- [Creating an Event Viewer Filter Using Advanced Filter Options on page 66](#)
- [Understanding Advanced Filter Options on page 62](#)



## PART 4

# Configuring Alerts

- [Creating and Managing Alerts on page 75](#)
- [Creating and Managing Alert Definitions on page 79](#)



## CHAPTER 5

# Creating and Managing Alerts

- [Alerts and Notifications Overview on page 75](#)
- [Generating an Alert on page 76](#)
- [Searching Alerts on page 77](#)
- [Deleting an Alert on page 77](#)

### Alerts and Notifications Overview

---

Alerts and notifications provide options for:

- Defining alert criteria based on a set of predefined filters. You can use the filters defined in the Filter Management window on the Event Viewer page to generate alerts.
- Generating an alert message and notifying you when an alert criteria are met.
- Searching for specific alerts on the Generate Alerts page based on alert ID, description, alert definition, alert type, or recipient e-mail address.
- 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 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.

### Understanding Role-Based Access Control for the Alerts and Alert Definitions

Role-Based Access Control (RBAC) has the following impact on the alerts:

You must have the following permission under Role Based Access Controls > Roles:

- **Create Alert** to create alerts.
- **Modify Alert** to modify alerts.

- **Delete Alert** to delete alerts.
- **User account** under Role Based Access Control to search for user accounts in alert definitions.

**Related Documentation**

- [Using Alert Definitions on page 79](#)
- [Creating Alert Definitions on page 80](#)
- [Managing Alert Definitions on page 82](#)
- [Deleting an Alert on page 77](#)
- [Searching Alerts on page 77](#)
- [Generating an Alert on page 76](#)

---

## Generating an Alert

To generate an alert:

1. Select **Security Director > Alerts**.  
The Alert page is displayed.
2. Click a column header.
3. Select an option. The available options are:
  - Sort Ascending—Sorts logs in the ascending order.
  - Sort Descending—Sorts logs in the descending order.
  - Columns—Provides a list of columns with check boxes to add or remove columns from the Alert Generation table. [Table 13 on page 76](#) lists the columns that you can add to the Alerts table.

**Table 13: Alert Columns**

Column Name	Description
Time	Specifies the date and time the alert was generated.
Alert ID	Specifies the alert ID.
Description	Specifies the description of the alert.
Severity	Specifies the severity of the alert.
Alert Definition	Specifies the alert definition.
Source	Specifies the source generating the alert.
Recipients	Specifies the recipients of the alerts generated from the alert definitions.

Table 13: Alert Columns (*continued*)

Column Name	Description
Alert Type	Specifies the alert type.

**Related  
Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Creating Alert Definitions on page 80](#)
- [Managing Alert Definitions on page 82](#)
- [Deleting an Alert on page 77](#)
- [Searching Alerts on page 77](#)

## Searching Alerts

To quickly locate an alert, use the search option on the upper right side of the Alert page:

1. Enter the alert ID, description, alert definition, alert type, or recipient e-mail address in the search box.
2. Click the search icon.

**Related  
Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Creating Alert Definitions on page 80](#)
- [Managing Alert Definitions on page 82](#)
- [Deleting an Alert on page 77](#)
- [Searching Alerts on page 77](#)

## Deleting an Alert

To delete an alert or multiple alerts:

1. Select **Security Director > Alerts**.
  2. Select an alert or multiple alerts for deletion.
  3. On the upper left side of the Alerts page, click the delete button (-).
- The delete alert notification is displayed.
4. Click **OK**.
- The alert is deleted.

**Related  
Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Creating Alert Definitions on page 80](#)

- [Managing Alert Definitions on page 82](#)

## CHAPTER 6

# Creating and Managing Alert Definitions

- [Using Alert Definitions on page 79](#)
- [Creating Alert Definitions on page 80](#)
- [Managing Alert Definitions on page 82](#)

### Using Alert Definitions

---

To create an alert definition:

1. Select **Security Director > Alert Definition**.  
The Alert Definitions page is displayed.
2. Click a column header.
3. Select an option. The available options are:
  - Sort Ascending—Sorts logs in the ascending order.
  - Sort Descending—Sorts logs in the descending order.
  - Columns—Provides a list of columns with check boxes you use to add or remove columns from the Alert Generation table. [Table 14 on page 79](#) lists the columns that you can add to the Alert Generation table.

**Table 14: Alert Generation Columns**

Column Name	Description
Select	Provides the option to select the available alerts.
Name	Specifies the name of the alert.
Description	Specifies the description of the alert.
Filter	Specifies the filter generating the alerts.
Recipients	Specifies the recipients of the alerts generated from the alert definitions.
Active	Specifies the active alerts.

Table 14: Alert Generation Columns (*continued*)

Column Name	Description
Alert Type	Specifies the alert type.

**NOTE:**

To see the logs in Event Viewer:

1. Select **Security Director > Alert Definition**.
2. Right-click on the cell and select **Show Logs**.

Logs are displayed in Event viewer which triggered that alert.

**Related  
Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Generating an Alert on page 76](#)
- [Creating Alert Definitions on page 80](#)
- [Managing Alert Definitions on page 82](#)

## Creating Alert Definitions

To create an alert definition:

1. Select **Security Director > Alerts > Alert Definitions**.

The Alert Definitions page is displayed.

2. On the upper left side of the Alert Definitions page, click the add button (+).

The alert definitions options are displayed. [Table 15 on page 80](#) lists the available options.

Table 15: Alert Definitions Options

Options	Description	Action
<b>General</b>		
Name	Specifies the name of the alert.	Enter the alert definition name.
Description	Specifies the description of the alert.	Enter the alert description.
Alert Type	Specifies the type of alert.	Displays the alert type.
Status	Specifies the status of the alert.	Click the <b>Active</b> check box to view active alerts.

Table 15: Alert Definitions Options (*continued*)

Options	Description	Action
Severity	Specifies the severity of the alert definition.	Select the severity of the alert.  The available options are: <ul style="list-style-type: none"> <li>• Critical</li> <li>• Warning</li> <li>• Info</li> </ul>
<b>Trigger</b>		
Use Data Criteria from Filters	Specifies the data criteria from the list of default and user-created filters that are saved from the Event Viewer.	To add saved filters: <ol style="list-style-type: none"> <li>1. Click <b>Add Saved Filters</b>.</li> <li>2. Select the filters to be added.</li> <li>3. Click <b>Add Filter(s) to Alert</b>.</li> </ol>
Add Data Criteria	Specifies the data criteria based on the Time period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.	Select the data criteria to filter the content.  To add data criteria: <ol style="list-style-type: none"> <li>1. Select the data criteria.</li> <li>2. Click <b>Add Data Criteria</b>.</li> </ol>
<b>Recipient(s)</b>		
Email address(es)	Specifies the recipients of the alerts generated from the alert definition.  By default, you can search by first name and add registered Junos Space Network Platform users. You can also type in external e-mail addresses.	Enter the recipients email address.
Custom Message	Specifies the custom message that is included in the e-mail message.	Enter the custom message.

3. Select **Create**.

**Related Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Using Alert Definitions on page 79](#)
- [Managing Alert Definitions on page 82](#)

## Managing Alert Definitions

---

- [Deleting Alert Definitions on page 82](#)
- [Editing Alert Definitions on page 82](#)
- [Searching Alert Definitions on page 82](#)
- [Hiding or Displaying Alert Definitions Using Quick View on page 82](#)

### Deleting Alert Definitions

To delete an alert definition:

1. Select **Security Director > Alerts > Alert Definitions**.
2. Select an alert.

You can also select multiple alerts for deletion.

3. On the upper left side of the Alert Definitions page, click the delete button (-).

The delete alert notification is displayed.

4. Click **OK**.

The alert definition is deleted.

### Editing Alert Definitions

To edit an alert definition:

1. Select **Security Director > Alerts > Alert Definitions**.
2. Select the alert.

3. On the upper left side of the Alert Definitions page, click the Edit button.

The alert definitions options are displayed. The options available on the Create Alert Definitions page are available for editing.

4. Click **Update**.

### Searching Alert Definitions

To quickly locate an alert definition, use the search option on the upper right side of the Alert Definition page:

1. Enter the alert name, description, or recipient name in the search box.
2. Click the search icon.

### Hiding or Displaying Alert Definitions Using Quick View

To hide or delete alert definitions using quick view:

1. Select **Security Director > Alerts > Alert Definitions**.

2. Select an alert.
3. On the upper left side of the Alert Definitions page, click the eye icon to hide or display quick view.

The alert definitions quick view pane with the details of the alert is displayed on the right-hand side of the Alert Definitions page.

**Related  
Documentation**

- [Alerts and Notifications Overview on page 75](#)
- [Using Alert Definitions on page 79](#)
- [Creating Alert Definitions on page 80](#)



## PART 5

# Configuring Reports

- [Creating and Managing Reports on page 87](#)



## CHAPTER 7

# Creating and Managing Reports

- [Reports Overview on page 87](#)
- [Creating a Log Report Definition on page 88](#)
- [Using Reports on page 92](#)
- [Creating a Policy Analysis Report Definition on page 94](#)
- [Managing Reports on page 96](#)

### Reports Overview

---

Reports are generated based on the summary of network activity and overall network status. Using reports, you can:

- Schedule reports based on the filters defined.
- Schedule reports based on the available default reports.
- Generate daily, weekly, and monthly reports, and send e-mail notifications to defined recipients.
- Generate reports with multiple sections, each section having its own criterion.

For example, If you are an administrator, you can schedule reports daily, weekly, or monthly, and configure them to include multiple criteria. You can also personalize the reports by adding the company logo, footer, and so on. When the system generates a report, you and other designated recipients receive the report in PDF format through e-mail. Reports enable you to perform trend analysis of your network's activities.

### Understanding Role-Based Access Control for Reports

Role-Based Access Control (RBAC) defines the user roles that control access to and permissions for using report functions.

Administrators must have the following permissions under Role Based Access Controls > Security Analyst or Security Architect:

- **View Report** to view generated reports.
- **Create Report** to create reports.
- **Modify Report** to modify generated reports.

The user role must have the following job permissions enabled for modifying the report.

- Cancel My Job
- Cancel Any Job
- **Delete Report** to delete generated reports.
- **Send Report** to send the generated reports.

**Related  
Documentation**

- [Using Reports on page 92](#)
- [Creating a Log Report Definition on page 88](#)
- [Managing Reports on page 96](#)

---

## Creating a Log Report Definition

---

To create a report:

1. Select **Security Director > Reports**.

The Reports page is displayed.

2. On the upper left side of the Reports page, click the add button (+).

The reports options are displayed. [Table 16 on page 88](#) lists the available options.

**Table 16: Report Options**

Options	Description	Action
General		
Report Name	Specifies the name of the report.	Enter the report name.
Report Description	Specifies the description of the report.	Enter the report description.
Content		

Table 16: Report Options (*continued*)

Options	Description	Action
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>The details of the filters displayed are:</p> <ul style="list-style-type: none"> <li>• Select—Specifies the check boxes for selecting the filter.</li> <li>• Filter Name—Specifies the name of the filter.</li> <li>• Filter Description—Specifies a description of the filter.</li> <li>• Group By—Specifies the selected group by option.</li> <li>• Time Span—Specifies the duration for which the data is displayed.</li> </ul> <p><b>NOTE:</b> The default value is last 3 hours.</p> <ul style="list-style-type: none"> <li>• Filter By—Specifies the list of default and user-created filters.</li> <li>• Created—Specifies the date on which the filter was created.</li> </ul>	<p>To add saved filters:</p> <ol style="list-style-type: none"> <li>1. Click <b>Add Saved Filters</b>.</li> <li>2. Select the filters to be added.</li> <li>3. Click <b>Add Filter(s) to Reports</b>.</li> </ol>
Add Data Criteria	<p>Specify the data criteria based on the Time period, Group By, and Filter By option. Filtered data only displays the subset of data that meets the criteria that you specify.</p>	<p>Select the data criteria to filter the content.</p> <p>To add data criteria:</p> <ol style="list-style-type: none"> <li>1. Select the data criteria.</li> <li>2. Click <b>Add Data Criteria</b>.</li> </ol>
<b>Add Filter(s) to Report</b>		
Section	Specifies the sections in the PDF report.	Select the section number.
Action	Specifies the option to delete the section from the report.	Click <b>Delete</b> to delete the section.
Section Title	Specifies the section title in the PDF report.	Enter the section title.
Section Description	Specifies the description of the section in the PDF report.	Enter the section description.

Table 16: Report Options (*continued*)

Options	Description	Action
Data Criteria	<p>Specifies the filter criteria used for the report. The details displayed are:</p> <ul style="list-style-type: none"> <li>Group by—Specifies the aggregation parameters based on the filter. This option overrides the Group By option specified in the filter.</li> <li>Time Span—Specifies the time range used for the data.</li> <li>Filter by—Specifies the list of default and user-created filters.</li> </ul>	—
Chart	<p>Specifies the chart used to display the data in the report. The available options are:</p> <ul style="list-style-type: none"> <li>Bar</li> <li>Timeline</li> </ul>	Select the chart type for the report.
Number To Display	<p>Specifies the number of top logs. The available options are:</p> <ul style="list-style-type: none"> <li>Top 5</li> <li>Top 10</li> </ul>	Select the number of logs to be displayed.
<b>Schedule</b>		
Add Schedule	<p>Specifies the option to add a schedule.</p> <p><b>NOTE:</b> Report is not generated if the report is not scheduled.</p>	Click <b>Add schedule</b> .

Table 16: Report Options (*continued*)

Options	Description	Action
Recurrence	<p>The available options are:</p> <ul style="list-style-type: none"> <li>• Repeats—Specifies the option to generate recurring reports. Repeats provides the following options: <ul style="list-style-type: none"> <li>• Daily—Specifies the option to generate reports daily.</li> <li>• Weekly—Specifies the options to generate reports weekly. You are provided with the option to select the day of the week the recurring report will be generated.</li> <li>• Monthly—Specifies the options to generate reports monthly. You are provided with the option to select the day of the month the recurring report will be generated.</li> </ul> </li> <li>• Every—Specifies the number of days, weeks, or months for which the recurring report will be generated.</li> </ul>	—
Start Date	<p>The available options are:</p> <ul style="list-style-type: none"> <li>• Date—Specifies the start date of report generation.</li> <li>• Time—Specifies the start time of the report generation.</li> </ul>	—
End Date	<p>The available options are:</p> <ul style="list-style-type: none"> <li>• Date—Specifies the end date of report generation.</li> <li>• Time—Specifies the end time of the report generation.</li> </ul>	After entering the end date options, Click <b>Schedule report</b> .
<b>Add Email Recipients</b>		
Email address(es)	<p>Specifies the recipients of the report.</p> <p>By default, you can search by first name and select registered Junos Space Network Platform users. You can also type in external e-mail addresses.</p>	Enter the e-mail address.
Subject	Specifies the subject of the e-mail.	Enter the subject line.

Table 16: Report Options (*continued*)

Options	Description	Action
Comment	Specifies the section to add comments.	<ol style="list-style-type: none"> <li>1. Enter comments.</li> <li>2. Click <b>Add Email Recipients</b>.</li> </ol>

3. Click one of the following options:

- Save Report Definition—Saves the report definition.
- Send Report Now—Sends the report through e-mail to the recipient immediately.



**NOTE:** If you add e-mail recipients while using Send Report Now, then the recipients receive the actual report for the selected time period. If it is a scheduled report, then the recipients receive the report according to the scheduled date.

- Preview as PDF—Provides the PDF preview of the report.
- Cancel—Cancels the user operation.

#### Related Documentation

- [Reports Overview on page 87](#)
- [Using Reports on page 92](#)
- [Creating a Log Report Definition on page 88](#)
- [Managing Reports on page 96](#)

## Using Reports

To use reports:

1. Select **Security Director > Reports**.

The Reports Page is displayed.

2. Click a column header.
3. Select an option. The available options are:
  - Sort Ascending—Sorts reports in ascending order.
  - Sort Descending—Sorts reports in descending order.
  - Columns—Provides a list of columns with check boxes to add or remove columns from the reports table. [Table 17 on page 93](#) lists the columns that you can add to the reports table.

Table 17: Report Columns

Column Name	Description
Select	Specifies the check boxes to use to select the type of report.
Name	Specifies the name of the report (user-created or default).
Description	Specifies the description of the report.
Type	Specifies the type of report. For example, log reports or policy analysis reports.
Report Content	Specifies the details of the sections in the report.
Schedule	Specifies the report generation schedule (daily, weekly, or monthly).
Recipients	Specifies the recipients of the generated reports.
Last Generated	Specifies the time the last report was generated, along with the status.

- Rows—Provides a list of default reports.

The following are the default reports that are available:

- Top Screen Attackers
- Top Screen Victims
- Top Screen Hits
- Top Firewall Rules
- Top Firewall Deny Sources
- Top Firewall Deny Destinations
- Top Firewall Service Deny
- TopFWDenies
- TopIPSEvent
- TopSourceIPs
- TopFirewallEvents
- TopDestinationIPs
- TopApplication
- Top URLs Detected
- Top URLs Blocked

- Top Viruses Detected
- Top Anti Spam Detected
- Top Screen Attacked
- Top Screen Victims
- Top Screen Hits
- Top Firewall Rules
- Top Attacks Detected
- Top Attacks Blocked
- Top Applications Blocked
- Top Web Apps
- Top Activities By User
- Top Roles

- Related Documentation**
- [Reports Overview on page 87](#)
  - [Creating a Log Report Definition on page 88](#)
  - [Managing Reports on page 96](#)

---

## Creating a Policy Analysis Report Definition

---

To create a policy analysis report definition:

1. Select **Security Director > Reports**.

The Reports page is displayed.

2. On the upper left side of the Reports page, click the add button (+) and then select **Create Policy Analysis Report Definition**.

The reports options are displayed. [Table 18 on page 94](#) lists the available options.

**Table 18: Report Options**

Options	Description	Action
General		
Report Name	Specifies the name of the report.	Enter the report name.
Report Description	Specifies the description of the report.	Enter the report description.
Content		

Table 18: Report Options (*continued*)

Options	Description	Action
Firewall Policy	Specifies the firewall policy data criteria from the list of default and user-created filters that are saved.	Select the Firewall policy filter to be added either by searching the filter name or selecting the policy name from the All Devices Policy list.
<b>Schedule</b>		
Add Schedule	Specifies the option to add a schedule.  <b>NOTE:</b> Report is not generated if the report is not scheduled.	Click <b>Add schedule</b> .
Recurrence	<p>The available options are:</p> <ul style="list-style-type: none"> <li>Repeats—Specifies the option to generate recurring reports. Repeats provides the following options: <ul style="list-style-type: none"> <li>Daily—Specifies the option to generate reports daily.</li> <li>Weekly—Specifies the options to generate reports weekly. You are provided with the option to select the day of the week the recurring report will be generated.</li> <li>Monthly—Specifies the options to generate reports monthly. You are provided with the option to select the day of the month the recurring report will be generated.</li> <li>Every—Specifies the number of days, weeks, or months for which the recurring report will be generated.</li> </ul> </li> </ul>	—
Start Date	<p>The available options are:</p> <ul style="list-style-type: none"> <li>Date—Specifies the start date of report generation.</li> <li>Time—Specifies the start time of the report generation.</li> </ul>	—
End Date	<p>The available options are:</p> <ul style="list-style-type: none"> <li>Date—Specifies the end date of report generation.</li> <li>Time—Specifies the end time of the report generation.</li> </ul>	After entering the end date options, Click <b>Schedule report</b> .

Table 18: Report Options (*continued*)

Options	Description	Action
<b>Add Email Recipients</b>		
Email address(es)	Specifies the recipients of the report.  By default, you can search by first name and select registered Junos Space Network Platform users. You can also type in external e-mail addresses.	Enter the e-mail address.
Subject	Specifies the subject of the e-mail.	Enter the subject line.
Comment	Specifies the section to add comments.	1. Enter comments. 2. Click <b>Add Email Recipients</b> .

3. Click one of the following options:

- Save Report Definition—Saves the report definition.
- Send Report Now—Sends the report through e-mail to the recipient immediately.



**NOTE:**

- If you add e-mail recipients while using Send Report Now, then the recipients receive the actual report for the selected time period. If it is a scheduled report, then the recipients receive the report according to the scheduled date.
- You must configure the SMTP server before using Send Report Now option.

- Preview as PDF—Provides the PDF preview of the report.
- Cancel—Cancels the user operation.

**Related Documentation**

- [Reports Overview on page 87](#)
- [Using Reports on page 92](#)
- [Creating a Log Report Definition on page 88](#)
- [Managing Reports on page 96](#)

## Managing Reports

- [Editing a Report on page 97](#)
- [Deleting a Report on page 97](#)

- [Duplicating a Report on page 98](#)
- [Adding Information to All Reports on page 98](#)
- [Performing Different Actions on Reports on page 99](#)

## Editing a Report

To edit a report:

1. Click **Security Director > Reports**.
2. Select a report by clicking the appropriate check box.
3. On the upper left side of the Reports page, click the Edit button.

The reports options are displayed. The options available on the Create Reports page are available for editing.

4. Click one of the following options:

- Save Report Definition—Saves the report definition.
- Send Report Now—Sends the report through e-mail to the recipient immediately.



**NOTE:** If you add e-mail recipients while using Send Report Now, then the recipients receive the actual report for the selected time period. If it is a scheduled report, then the recipients receive the report according to the scheduled date.

- Preview as PDF—Provides the PDF preview of the report.
- Cancel—Cancels the user operation.

## Deleting a Report

To delete a report:

1. Click **Security Director > Reports**.
2. Select a report.

You can also select multiple reports for deletion.

3. On the upper left side of the Reports page, click the delete button (-).

The delete report notification is displayed.

4. Click **OK**.

The report is deleted.

## Duplicating a Report

To duplicate a report:

1. Click **Security Director > Reports**.
2. Select the report.
3. Click the Action field in the rule and select **Duplicate Report** from the drop-down list of actions.

The reports options are displayed. The options available on the Edit Reports page are available for cloning.

4. Click one of the following options:
  - Save Report Definition—Saves the report definition.
  - Preview as PDF—Provides the PDF preview of the report.

You can see a preview of the PDF with in a new browser window or as a separate PDF file, if you do not have a browser configured.

- Send Report Now—Sends the report through e-mail to the recipient immediately. The user will receive a notification once the report is sent. The user can also use the job id to see more details on the job.



**NOTE:** If you add e-mail recipients while using Send Report Now, then the recipients receive the actual report for the selected time period. If it is a scheduled report, then the recipients receive the report according to the scheduled date.

## Adding Information to All Reports

To add company information to a report:

1. Click **Security Director > Reports**.
2. Right-click and then select the **Upload Logo** option.

The upload logo options are displayed.

3. Click **Change logo image**.

The upload option is displayed.

4. Click **Browse** to navigate to the logo.
5. Enter the PDF footer text.
6. Click **Save**.

## Performing Different Actions on Reports

To perform an action on a report:

1. Click **Security Director > Reports**.

2. Select a report by clicking the appropriate check box.

You can perform different actions on the selected report using the right-click option or from Action menu.

3. Right-click on the selected report or click the Action field in the rule and select the appropriate action from the drop-down list of actions.
  - Preview as PDF—Provides the PDF preview of the report.
  - Send Report Now—Sends the report through e-mail to the recipient immediately. The user will receive a notification once the report is sent. The user can also use the job id to see more details on the job.



**NOTE:** If you add e-mail recipients while using Send Report Now, then the recipients receive the actual report for the selected time period. If it is a scheduled report, then the recipients receive the report according to the scheduled date.

- Duplicate Report—Allows users to create a copy of a report.
- 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.



## PART 6

# Configuring Security Objects

- [Overview on page 103](#)
- [Creating and Managing Services and Service Groups on page 107](#)
- [Creating and Managing Addresses and Address Groups on page 121](#)
- [Creating and Managing Zone Sets on page 139](#)
- [Creating and Managing Variables on page 143](#)



## CHAPTER 8

# Overview

- [Object Builder Overview on page 103](#)
- [Domain RBAC Overview on page 104](#)

### Object Builder Overview

---

You can use the Object Builder workspace in Security Director to create objects used by firewall policies, VPNs, and NAT policies. These objects are stored in the Junos Space database. You can reuse these objects with multiple security policies, VPNs, and NAT policies. This approach makes the design of services more structured and avoids the need to create the objects during the service design.

You can use the Object Builder workspace to create, modify, clone, and delete the following objects:

- Addresses and address groups
- Services and service groups
- Variables

You will not be able to delete any of the objects you have created in Object Builder (except Template definition and Templates) if they are already used in one of the firewall policies, NAT policies, or VPNs.

Object Builder supports concurrent editing of its objects, with a *save as* option to save your changes with a different name.

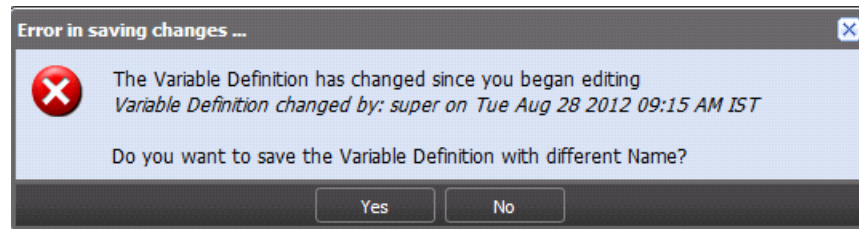
Concurrent editing is supported for the following objects:

- Addresses and address groups
- Services and service groups
- Application signatures
- Schedulers
- Extranet devices
- NAT pools
- Policy profiles

- VPN profiles
- Variables

If a previous user edits any objects and saved the changes, when you attempt to save your changes, the error message appears, as shown in [Figure 9 on page 104](#). This is an example error message received for the Variables object.

**Figure 9: Variable Objects: Concurrent Edit Save Warning Message**



**Related  
Documentation**

- [Address and Address Groups Overview on page 121](#)
- [Service and Service Group Overview on page 107](#)
- [Security Policy Profiles Overview on page 243](#)
- [VPN Profiles Overview on page 291](#)

---

## Domain RBAC Overview

A domain is a sphere or a boundary around which you can interact with a system. A Junos Space domain encompasses all Junos Space objects; it enforces access, visibility, and management of objects. By creating a domain, you create a container for interacting with the system. Devices are the key elements in a domain. You use domains and the devices within those domains to configure a device-management partitioning scheme.

Domains allow you to control and partition a network from the management point of view. You can create a network based on certain criteria while providing users with management access to their devices. At the same time, domains also allow sharing of objects and certain configuration enforcements. Objects of the Global domain can only be accessed in read-only mode by the child domains, if view parent is enabled. Access across peer domains is not allowed. This kind of network partitioning is required for both MSPP and enterprise customers. The Network Application Platform enables users to manage objects from all the allowed domains in the aggregated view. However, Security Director does not support this functionality.

The following sections explain the impact of domain role-based access control (RBAC) on all Security Director objects and services.

### Creation or Addition of an Object or a Service

Prior to domain RBAC, you only needed write permission for an object to create the object. Now with the domain RBAC, you also need an access for a domain to create an object in that domain. For example, consider having domains such as D1, D2, and Global. To create an object in D1, switch to the D1 domain before you can create an object in that

domain. Note that you cannot create an object in one domain while you are in a different domain.

In Security Director Release 13.2, you cannot create an object in a particular domain to which you have the write access through the REST API. This is not supported by the Network Application Platform Release 13.2 either. All the objects created through the REST API are created in the Global domain.

All the objects that are created internally as part of an operation are part of the domain in which the operation is triggered. For example, all audit logs for an operation are created in the domain in which the operation is triggered.

### Reading or Viewing an Object or a Service

You can view all the objects in a domain to which you are having the access. In the Security Director GUI, you must switch the view to the D1 domain to view objects in that domain. If you have read access to both the D1 and D2 domains, you cannot see D2 domain objects in the D1 domain view, and vice versa. You can see objects in the Global domain from the D1 domain, provided the D1 domain has view parent permission. You cannot see D1 or D2 objects from the Global domain.

Viewing of Security Director domain concept is similar to NSM domain concept. Security Director domain additionally supports viewing of objects in the parent domain in read-only mode from the child domain. For example, if you are currently in the D1 domain, you can view objects in the Global domain irrespective of whether you are assigned to the Global domain, provided the D1 domain has view parent enabled on it.

### Updating or Modifying an Object or a Service

To modify a domain object through the Security Director GUI, you must switch to that domain. You cannot switch to a domain for which you do not have a permission. You cannot modify an object in one domain if you are in a different domain.

Modifying objects through REST is ID based. To modify an object in a domain, you must have write access to that domain. Objects in the System domain are in read-only mode and you cannot modify them.

### Deleting an Object or a Service

To delete a domain object through the Security Director GUI, you must switch to that domain. You cannot delete an object in one domain if you are in a different domain.

Deleting objects through REST is ID based. To delete an object in a domain, you must have write access to that domain. Objects in the System domain are in read-only mode and you cannot delete them.

### Referencing Objects

An object can always reference another object in the same domain, with no restrictions. Referring an object from the same domain is safe. An object in the D1 domain can reference other objects in the D1 domain. The rules are more complex for referencing objects in a different domain. For example, a D1 domain object can reference objects in the D1 domain or in its parent domain, the Global domain. However, D1 objects cannot reference D2

objects. Objects in the Global domain cannot reference objects in its child domains, D1 and D2.

There is an exception to referencing the devices. Objects in the D1 domain can reference devices in the same domain or they can refer devices in the D1 or D2 domain. But this is not true the other way, that is objects in D1 domain cannot reference devices in the Global domain.

## Moving Objects Across Domains

You can move objects from one domain to another, in general. For example, you can move an object the D1 domain to the Global domain and from the Global domain back to the D1 domain. A validation is performed to check if the move is valid and invalid moves are disallowed. Moving an object becomes complex if this object is referenced by another object. An object in the D1 domain can be moved up to the Global domain if it is referenced by another object that is either in the D1 domain or in the Global domain. However, moving an object from the Global domain to the D1 domain is disallowed if the object is referenced by another object in the Global domain.

The rules are different for moving device objects between domains. You can move a device from the Global domain to the D1 domain if the device is used by an object in either the Global or the D1 domain. However, moving a device from the D1 domain to the Global domain is not allowed if an object in the D1 domain is using that device.

To move a device that is part of a cluster, you must move both members of the cluster. You cannot move only the primary or only the secondary device. You can move an object from the D1 domain to the Global domain only if you have write access to the Global domain and view parent access enabled in the D1 domain.

## Naming the Objects in a Domain

The name of an object must be unique within a domain hierarchy. Objects with the same name cannot be created in both the D1 and Global domains. The domain hierarchy includes the current domain, its parent, and its child domains.

All the name validations consider domains as one of the constraints.

The object name must be a string beginning with a number or letter and consisting of letters, numbers, colons, periods, slashes, dashes, and underscores. The object name must not contain special characters such as &, <, >, and \n.

## Predefined Objects

All the Security Director predefined objects are in the System domain. The predefined objects are visible from all the domains in read-only mode. The predefined services, addresses, signatures, and so on are all in the System domain.

All the device-specific predefined objects are also in the System domain. When a new predefined object is discovered during the device discover, that object is also placed in the System domain. The All Device policy is in a global domain and you can modify them.

**Related Documentation**

- [Object Builder Overview on page 103](#)

## CHAPTER 9

# Creating and Managing Services and Service Groups

- [Service and Service Group Overview on page 107](#)
- [Creating Services on page 108](#)
- [Managing Services on page 112](#)
- [Creating Service Groups on page 118](#)
- [Managing Service Groups on page 119](#)

## Service and Service Group Overview

---

You can use the Service Creation Wizard to create a service object based on the protocols the service uses. The protocols that are used to create an service object include:

- TCP
- UDP
- MS-RPC
- SUN-RPC
- ICMP
- ICMPv6

You can group service objects to form a service group using the Service Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an service or an service group.

There are Juniper Networks defined service objects for commonly used services.



NOTE:

- You cannot modify or delete Juniper Networks defined service objects.
- The number of allowable objects in one group depends on the model of the SRX Series device.

During the device update, you can delete all the unused services and service groups by selecting an option available under Administration > Applications > Modify Application Settings > Update-Device. Select the **Delete unused Services and Service groups** option to delete all the unused services and service groups. By default, this option is enabled whenever you perform a fresh install of Security Director or upgrade from the previous release.

If the option is enabled, Security Director will manage the services in the same way it manages addresses. Security Director will always delete the unused services (those services that are not referenced by any policy on the device) from the device during publish or update. If the option is disabled, Security Director will never try to delete services from the device, even if the service is unused on a device.



**NOTE:** A *service* in Security Director refers to an application on a device.

---

**Related  
Documentation**

- [Creating Services on page 108](#)
- [Creating Service Groups on page 118](#)
- [Managing Services on page 112](#)
- [Managing Service Groups on page 119](#)

---

## Creating Services

---

To create a service:

1. Select **Security Director > Object Builder > Services**.

The Manage Services page appears, listing all available services.

2. Click the plus sign (+) to create a new service.

The Create Service page appears, as shown in [Figure 10 on page 109](#).

Figure 10: Create Service: Basic View Page

Create Service

Object Type: ☒ Service ☐ Service Group

Name:

Description:

Protocols:

Name	Description	Type	Detail
------	-------------	------	--------

Create Cancel

3. By default, the Object Type is selected as Service.
4. In the Name field, enter the name of the service.
5. In the Description field, enter a description for the service.
6. In the Protocols pane, click the plus sign (+) to configure a new protocol.

The New Protocol page appears, as shown in [Figure 11 on page 110](#).

Figure 11: Create Service: Advanced Settings Page

The screenshot shows the 'New Protocol' dialog box. The 'Name' field contains 'nw-prt'. The 'Description' field is empty. The 'Type' dropdown menu is set to 'TCP'. The 'Destination Port' field is empty. The 'Advanced Settings' section includes a 'Disable Inactivity Timeout' checkbox (unchecked), an 'Inactivity Timeout' field with a spinner, an 'ALG' dropdown menu, and a 'Source Port(s) / Port Range(s)' field with an example '25, 30-50, 80, 90'. At the bottom are 'Add' and 'Cancel' buttons.

- In the Name field, enter a name for the new protocol.
- In the Description field, enter a description for the new protocol.
- Select a protocol type from the Type menu.

You can select the following protocol types from the Type menu:

- TCP
  - a. Select the appropriate option from the ALG menu.
  - b. Enter a range of TCP source ports in the Source Port field.
  - c. By default, the Disable Inactivity Timeout check box is not selected. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
  - d. Enter a value, in seconds, in the Inactivity Timeout field.
- UDP
  - a. Select the appropriate option from the ALG menu.
  - b. Enter a range of UDP source ports in the Source Port field.
  - c. By default, the Disable Inactivity Timeout check box is not selected. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
  - d. Enter a value, in seconds, in the Inactivity Timeout field.
- ICMP
  - a. Enter a value for the ICMP message you want to display in the ICMP Type field.
  - b. Enter a value for the ICMP type you have specified in the ICMP Code field.

- SUN - RPC
  - a. Enter a value for the RPC service you want to use in the RPC Program Number field.
  - b. Select the TCP or UDP option button to specify an appropriate protocol type in the Protocol Type field.
- MS - RPC
  - a. Enter the universally unique ID corresponding to the RPC service you want to use in the UUID field.
  - b. Select the TCP or UDP option button to specify an appropriate protocol type in the Protocol Type field.
- ICMPv6
  - a. Enter a value for the ICMPv6 message you want to display in the ICMP Type field.
  - b. Enter a value for the ICMPv6 type you have specified in the ICMP Code field.
- Other
  - a. Select the appropriate option from the ALG menu.
  - b. Enter a range of TCP source ports in the Source Port field.
  - c. Enter the number of the protocol in the Protocol Number field.  
This number is specified in the Protocol field for IPv4 packets and the Next Header field for IPv6 packets.
  - d. By default, the Disable Inactivity Timeout check box is unchecked. Click the **Disable Inactivity Timeout** check box if you want to disable this option.
  - e. Enter a value, in seconds, in the Inactivity Timeout field.



**NOTE:** All new ALGs supported by Junos OS Release 12.1X45 appear in the ALG drop-down box. These new ALGs are supported only if the Type selected is TCP, UDP, or Other.

- In the Destination Port field, enter destination ports for the selected types.
  - The Advanced Settings fields are not mandatory fields.
  - Click **Add** in the New Protocol dialog box.
7. To create the service, click **Create**.

#### Related Documentation

- [Service and Service Group Overview on page 107](#)
- [Creating Service Groups on page 118](#)
- [Managing Services on page 112](#)

- [Managing Service Groups on page 119](#)

## Managing Services

---

You can modify, delete, or clone services.

- Select **Security Director > Object Builder > Services**.

The Services page appears.

You can right-click to manage a service.

You can perform the following tasks on the Services page:

1. [Modifying a Service on page 112](#)
2. [Deleting a Service on page 113](#)
3. [Cloning a Service on page 113](#)
4. [Find Duplicate Service Objects on page 113](#)
5. [Find Service Usage on page 114](#)
6. [Replace Services on page 115](#)
7. [Show Unused Services on page 117](#)
8. [Delete All Unused Services on page 117](#)

## Modifying a Service

To modify a service:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service you want to modify, right-click and select **Modify Service**.

This action redirects you to the window that you used to create a new service. You can modify all the fields on this window, except the Name field.

3. In the Category field, enter a new category.
4. In the Description field, enter a new description.
5. Make necessary changes in the Protocols pane.
  - To edit a protocol, select the protocol you want to edit and click the Edit icon. Make the necessary changes and click **OK**.
  - To delete a protocol, select the protocol you want to delete and click the **Delete** icon.
6. Click **Modify** to save the changes made to this service.

## Deleting a Service

To delete a service:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service you want to delete, right-click, and select **Delete Services**.

The Delete dialog box appears

3. Select the service you want to delete and click **Delete**.

## Cloning a Service

To clone a service:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service you want to clone, right-click and select **Clone Service**.

You are redirected to the Clone Service page.

3. Make necessary changes and click **Clone**.

## Find Duplicate Service Objects

To find duplicate service objects:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service within which you want to find the duplicate objects. Right-click the service, and then click Show Duplicates.

A window appears, showing all the groups with that include duplicate objects, as shown in [Figure 12 on page 114](#). Predefined services are also listed under duplicate objects.

Figure 12: Window Showing Duplicate Services

Return To Service View			
Service	Name	Type	Description
	dhcp-server (3 members)		
			Merge
	ntp (2 members)		
			Merge
	netbios-session (2 members)		
			Merge
	smtp (2 members)		
			Merge
	dhcp-client (2 members)		
			Merge
	ldap (2 members)		
			Merge
	printer (2 members)		
			Merge
	ike (2 members)		
			Merge
	isp-global (2 members)		
			Merge
	ping (2 members)		
			Merge
	ping6 (2 members)		
			Merge
	icmp6-all	Service	predefined service
	ping6	Service	predefined service
	sctp-any (2 members)		
			Merge
	sunrpc (2 members)		
			Merge

- If you want to merge duplicate objects in a group, select the objects in a group and click **Merge**.

A merge window appears. In the Name field, provide a new object name or select an existing object name from the list. The merge operation deletes or replaces the reference for only the custom services, and predefined services are not affected.



**NOTE:** You can merge all the objects in a group by clicking **Merge** after selecting all the objects by clicking the group name.



**NOTE:** If the selected duplicate objects are referenced in any other services (firewall policy) and security objects (service groups), a warning message is provided before the objects are merged.

- If you want to delete objects in a group, select an object or objects, right-click, and then select **Delete**. A confirmation window appears before the selected objects are deleted.

Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

- If you want to find the usage of the duplicate objects in other groups, select an object, right-click, and then select **Find Usage**.

The usage window appears, showing the usage of the selected object in any service (firewall policy) or security objects (service groups).

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Find Service Usage

To find service usage:

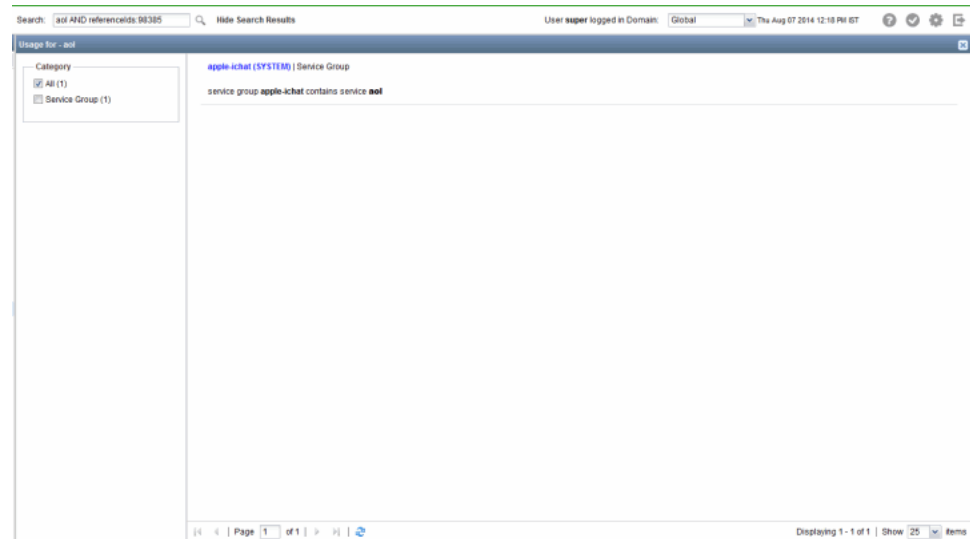
- Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service for which you want to find the usage. Right-click the service, and then click **Find Usage**.

A window appears, showing all the locations where this object is used and also the search syntax is shown in the global search tool, as shown in [Figure 13 on page 115](#).

**Figure 13: Window Showing Service Usage**



Procedure to manually rebuild the Index, see "[Indexing Overview](#)" on page 7

## Replace Services

You can select one or more services to replace with another service, service group, or nested service group. To replace one or more services:

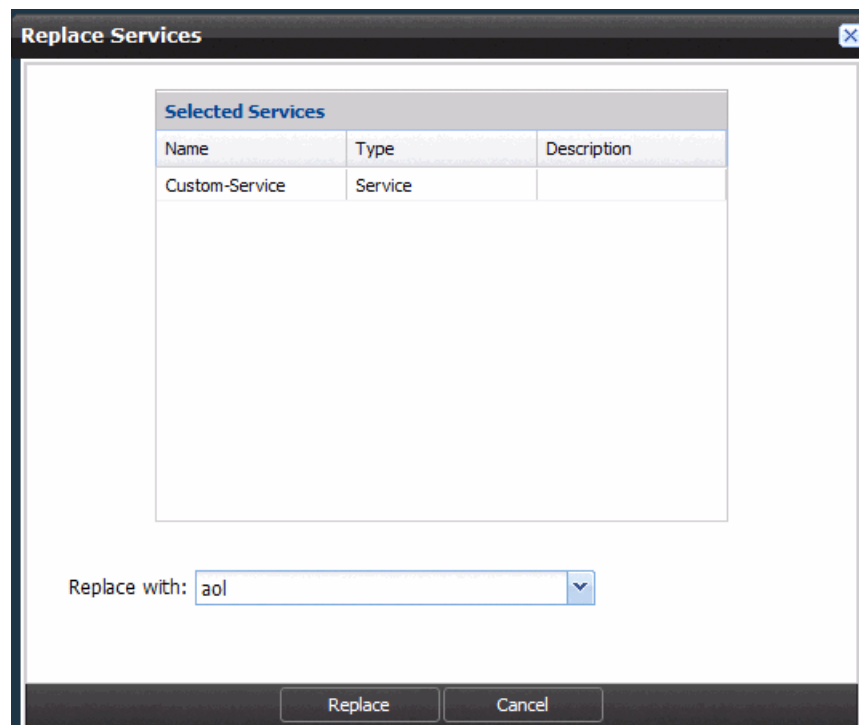
1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service or services that you want to replace. Right-click the service or services, and then click **Replace Services**. You can replace a single service or multiple services.

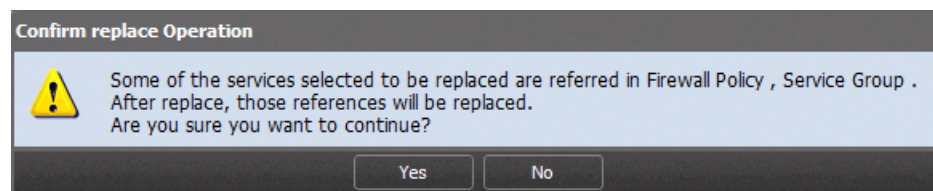
A window appears, showing the service or services you have selected to be replaced, along with a drop-down list of the services that are available to replace the service or services you have selected. See [Figure 14 on page 116](#).

Figure 14: Replace Services Window



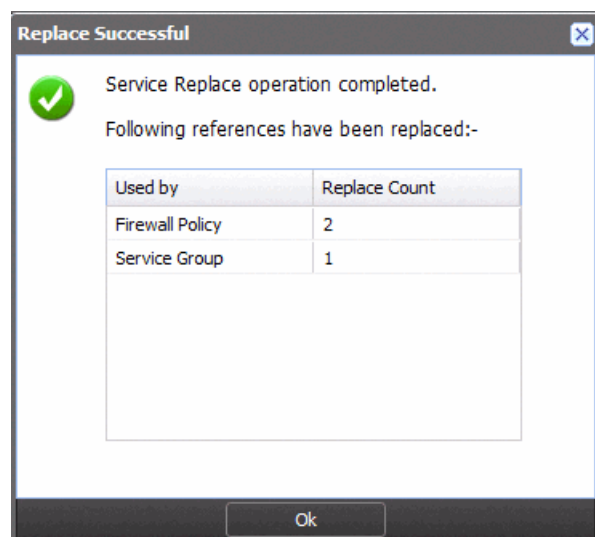
3. In the Replace Services window, select the service, service group, or nested service group that will replace the selected service or services, and click **Replace**. If the selected services are used in any other references, you will receive the following warning message before replacing, as shown in [Figure 15 on page 116](#). Click **Yes** to replace.

Figure 15: Service: Confirm Replace Warning Message



If the operation is successful, you will receive a summary showing the services that were replaced, as shown in [Figure 16 on page 117](#).

Figure 16: Service Replace Successful Message



## Show Unused Services

1. Select **Security Director > Object Builder > Services**.

The Service page appears.

2. You can either right-click any service or use the Actions drawer, and select **Show Unused**.

A list of all unused service objects which are not referenced in any policy or service group, appear on the page.

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Delete All Unused Services

You can find the unused service objects and delete all unused service objects. You can clear all the unwanted objects which are not used anywhere.

To deleted the unused services:

1. Select the unused service object that you want to delete, right-click or from the Action drawer, select **Delete All Unused Services** option.

A warning message is displayed to confirm the delete operation.

2. Click **Yes** to delete all unused service objects, or **No** to cancel the delete operation.

### Related Documentation

- [Service and Service Group Overview on page 107](#)
- [Creating Services on page 108](#)
- [Creating Service Groups on page 118](#)
- [Managing Service Groups on page 119](#)

## Creating Service Groups

To create a service group:

1. Select **Security Director > Object Builder > Services**.

The Services page appears with all the services and service groups.

2. Click the plus sign (+) to create a service group.

The Create Service appears.

3. Select the Object Type as Service Group, as shown in [Figure 17 on page 118](#).

**Figure 17: Create Service Group Page**

**Create Service**

Object Type: ☐ Service ☒ Service Group

Name:

Description:

Services:

Available	Selected
Filter <input type="text"/> Select: All None	Select: All None
aol (tcp/5190-5193) SYSTEM	
apple-ichat (group) SYSTEM	
apple-ichat-snatmap (udp/5678) SYSTEM	
bgp (tcp/179) SYSTEM	
blf (udp/512) SYSTEM	
bootpc (udp/68) SYSTEM	
bootps (udp/67) SYSTEM	
chargen (udp/19) SYSTEM	
cifs (group) SYSTEM	
cvspserver (tcp/2401) SYSTEM	
dhcn-client (udp/68) SYSTEM	
Total: 226	

Create Cancel

4. In the Name field, enter a name for the new service group.

5. In the Description field, enter a description for the new service group.

6. In the Services field, from the Available dialog box, select the service that you want to group, and click the right arrow to add to the Selected column.

Click **All** to move all the services to the Selected column. The service you have selected appears in the Selected section of the dialog box.

7. Click **Create**.

The service group appears on the Services page.

- Related Documentation**
- [Service and Service Group Overview on page 107](#)
  - [Managing Service Groups on page 119](#)

- [Creating Services on page 108](#)
- [Managing Services on page 112](#)

## Managing Service Groups

---

You can modify, delete, or clone service groups listed on the Manage Services page.

To open the Services page:

- Select **Security Director > Object Builder > Services**.

The Services page appears.

You can right-click the service group to manage it.

You can perform the following tasks on the Services page:

1. [Modifying a Service Group on page 119](#)
2. [Deleting a Service Group on page 119](#)
3. [Cloning a Service Group on page 120](#)

### Modifying a Service Group

To modify a service group:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service group you want to modify, right-click and select **Modify Service**.

This action redirects you to the window that you used to create a new service group. You can modify all the fields on this window, except the Name field.

3. In the Description field, enter a new description.
4. In the Category field, enter a new category.
5. In the Members section, make appropriate changes to the services used in this group.
6. Click **Modify** to save the changes made to this service group.

### Deleting a Service Group

To delete a service group:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service group you want to delete, right-click, and select **Delete Services**.

The Delete dialog box appears.

3. Select the service group you want to delete and click **Delete**.

## Cloning a Service Group

To clone a service group:

1. Select **Security Director > Object Builder > Services**.

The Services page appears.

2. Select the service group you want to clone, right-click, and select **Clone Service**.

You are redirected to the Clone Service page.

3. Make the necessary modifications and click **Clone**.

### Related Documentation

- [Service and Service Group Overview on page 107](#)
- [Creating Service Groups on page 118](#)
- [Creating Services on page 108](#)
- [Managing Services on page 112](#)

## CHAPTER 10

# Creating and Managing Addresses and Address Groups

- [Address and Address Groups Overview on page 121](#)
- [Global Address Book Overview on page 121](#)
- [Creating Addresses on page 124](#)
- [Managing Addresses on page 126](#)
- [Creating Address Groups on page 136](#)
- [Managing Address Groups on page 137](#)

## Address and Address Groups Overview

---

You can use the Address Creation Wizard to create an address object that specifies an IP address or a hostname. You can specify a hostname and use the address resolution option to resolve it to an IP address. You can also resolve an IP address to the corresponding hostname.

You can group address objects to form an address group using the Address Group Creation Wizard. Junos Space creates an object in the Junos Space database to represent an address or an address group.

### Related Documentation

- [Creating Addresses on page 124](#)
- [Managing Addresses on page 126](#)
- [Creating Address Groups on page 136](#)
- [Managing Address Groups on page 137](#)

## Global Address Book Overview

---

In Junos OS Release 11.2 and later releases, the address book is moved from the zone level to the device global level. This permits objects to be used across many zones and avoids inefficient use of resources. This change also permits nested groups to be configured within the address book, removing redundancy from repeating address objects.

The Security Director application manages its address book at the global level, assigning objects to devices that are required to create policies. If the device is capable of using

global address book, Security Director pushes address objects used in the policies to the device global address book. Nested address group capability is used in the publish and update feature of Security Director depending on the device capability.

## Differences Between Global and Zone-Based Address Books

The global address book is supported in Junos OS Release 11.2 and later releases.

- An address book is not configured within a specific zone; therefore, one address book can be associated with multiple zones.
- If a global address book is defined, you cannot create zone-based address books.
- By default, there is an address book called *global* associated with all zones.
- A zone can be attached to only one address book in addition to the global address book, which contains all zones by default.
- Address name overlaps are possible between the global address book and zone address book. For example, Security Director will attempt to match an address in the zone-based address book first, and, if the address is not found, the global address book is checked. You must ensure that the correct address objects are used in the policy.
- NAT rules can use address objects only from the global address book. They cannot use addresses from user-defined address books.



**NOTE:** Beginning in Junos OS Release 11.2, NAT rules can use address objects from the global address book. However, Security Director will still continue to define address prefix in NAT rule itself, if the zone addresses are configured in device.

## Nested Address Group Support

In Junos OS versions before Release 11.2, nested address groups were not supported on the device. Because of this, address groups were flattened to a single group when pushed to the device. This caused inefficient of object resource usage. Junos OS Release 11.2 and later releases support the nested references within address sets.

## Mixed-Version Support

Because Security Director supports Junos OS Release 10.3 and later releases, support for both zone-based and global address books is required. SRX Series devices running Junos OS Releases earlier than Release 11.2 must support the current behavior, that is, populating required address book entries in the zone address books and flattening nested groups. SRX Series devices running Junos OS Release 11.2 and later must use the global address book.

Junos OS Release 11.2 supports both zone address and global address books. However, both are configured separately.

## Migrating from Zone to Global Addressing

Table 19 on page 123 gives the migration matrix covering all scenarios:

**Table 19: Migration Matrix**

Address Book Used in Last Push from Security Director or NSM	Is Device Global Address Book Capable?	Address Book Type Used by Device	Security Device That Will Use Zone or Global
Zone	–	Zone	Zone
Zone	–	Global	Global
Zone	Any	Empty	Depends on device capability
Empty	Yes	–	Global
Empty	No	–	Zone



**NOTE:** In Junos OS Release 11.2 and later releases, devices might be managed by the Security Director and the device might be using the zone address book. In this case, if you want to use the global address book, you can do offline device migration from the zone address book to global address book. In this case, if the device was managed by the Security Director application, you must publish the device again, so that the changes are discovered by the application.

## Example: Configuring Address Book Entries in Global Address Book

If you require a policy to permit all the traffic from the trust and untrust zones of FTP and DNS servers to UNIX server, you might require to create addresses of FTP and DNS servers in both the zones. The following procedure shows the creation of address in global address book.

1. Create address in zone-based address book.

```
set security zones security-zone trust address-book address DNS-server
192.168.1.1
set security zones security-zone trust address-book address FTP-server
192.168.2.1
set security zones security-zone trust address-book address unix-server
192.168.3.1
set security zones security-zone untrust address-book address DNS-server
192.168.1.1
set security zones security-zone untrust address-book address FTP-server
192.168.2.1
```

2. Create address in global address book. The same can be achieved with the global address book, and not required to create the same address entries multiple times.

```
set security address-book global address DNS-server 192.168.1.1
set security address-book global address FTP-server 192.168.2.1
set security address-book global address unix-server 192.168.3.1
```

3. Create a policy and permit the traffic. The policy CLI is same for both zone-based address book and global address book.

```
set security policies from-zone trust to-zone trust policy unix-trust match
source-address DNS-server
set security policies from-zone trust to-zone trust policy unix-trust match
source-address FTP-server
set security policies from-zone trust to-zone trust policy unix-trust match
destination-address unix-server
set security policies from-zone trust to-zone trust policy unix-trust match
application any
set security policies from-zone trust to-zone trust policy unix-trust then
permit
```

```
set security policies from-zone untrust to-zone trust policy unix-untrust match
source-address DNS-server
set security policies from-zone untrust to-zone trust policy unix-untrust match
source-address FTP-server
set security policies from-zone untrust to-zone trust policy unix-untrust match
destination-address unix-server
set security policies from-zone untrust to-zone trust policy unix-untrust match
application any
set security policies from-zone untrust to-zone trust policy unix-untrust then
permit
```

- Related Documentation**
- [Firewall Policies Overview on page 151](#)
  - [Creating Firewall Policies on page 159](#)
  - [Managing Firewall Policies on page 201](#)

---

## Creating Addresses

To create an address:

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. To create a new address, click the plus sign (+).

The Create Address page appears, as shown in [Figure 18 on page 125](#).

Figure 18: Create Address Page

3. In the Name field, enter a name for the new address.

**NOTE:**

- The address name must be a string beginning with a number or letter and consisting of letters, numbers, dashes, and underscores.
- The address name must be a string and cannot contain special characters such as &, <, >, and \n.
- The maximum number of characters allowed in the address name is 63.

4. In the Description field, enter a description for the new address. The description must be a string and cannot contain special characters such as &, <, >, and \n.
5. Direct Security Director to resolve an IP address to a hostname or resolve a hostname to an IP address.
  - To specify an IP address as the address type, select **Host** from the drop-down menu and enter the **IP** address in the IP field.
  - To specify a hostname as the address type, select **Host** from the drop-down menu and enter the hostname in the Host Name field.
  - To specify an IP address range, select **Range** from the drop-down menu and enter the IP ranges in the Start IP and End IP fields.
  - To specify a network as an address type, select **Network** from the drop-down menu and enter the network address in the IP and Netmask fields.

- To specify an IP address with a wildcard mask, select **Wildcard** from the drop-down menu and enter the IP address in the IP field and wildcard mask in the Wildcard Mask fields.
- To specify a DNS name as an address type, select **DNS Host** from the drop-down menu and enter the DNS name in the DNS Name field.



**NOTE:** You can resolve an IP address to a hostname and a hostname to an IP address using the green arrows next to the IP and Host Name fields.



**NOTE:** The host and network address types support both IPv4 and IPv6 address types. These address types also supports multicast addresses. However, the range address type supports only IPv4 addresses. NAT and IPsec VPNs do not support IPv6 addressing and wildcard addresses.



**NOTE:** Ensure that the first 8 bits of the address are not 0 and the highest bit of the mask is 1 when you are using the wildcard address type.

6. Click **Create** to create an address.

The new address appears in the Manage Address page.



**NOTE:** You can also add addresses using the Address import functionality. To use this functionality, select the Actions drawer and click Import Addresses from CSV.



**NOTE:** You can export the addresses using the Address export functionality. To use this functionality, select the addresses you want to export and select Export Addresses to CSV from the Actions drawer.

#### Related Documentation

- [Address and Address Groups Overview on page 121](#)
- [Managing Addresses on page 126](#)
- [Creating Address Groups on page 136](#)
- [Managing Address Groups on page 137](#)

---

## Managing Addresses

You can modify, delete, clone, export, and import addresses listed on the Manage Address page. Click the **IP Address** column to sort IP addresses in ascending or descending order.

You can sort IP addresses by host, range, and network types; however, DNS host, wildcard, group, and predefined IP addresses are excluded from any type of sorting.

For address range and network type, IP addresses are sorted by the first two digits. The range value does not affect sorting. Multiple devices that have the same address but different ranges are not sorted.

To open the Address page:

- Select **Security Director > Object Builder > Addresses**.

The Address page appears.

You can right-click an address to manage it.

You can perform the following tasks on the Address page:

1. [Modifying an Address on page 127](#)
2. [Deleting an Address on page 128](#)
3. [Cloning an Address on page 128](#)
4. [Exporting Addresses on page 128](#)
5. [Importing Addresses on page 129](#)
6. [Find Duplicate Address Objects on page 129](#)
7. [Find Address Usage on page 131](#)
8. [Replace Addresses on page 132](#)
9. [Show Unused Addresses on page 134](#)
10. [Delete All Unused Addresses on page 134](#)
11. [Assigning Addresses to Domains on page 135](#)

## Modifying an Address

You can modify an address only from the current domain. The address from the Global domain, which is visible in the child domain, cannot be modified.

To modify an address:

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Select the address you want to modify, right-click and select **Modify Address**.

This action redirects you to the window that you used to create a new address. You can modify all the fields in this window, except the Name field.

3. In the Description field, enter a new description.
4. Enter a new value for the address type you specified earlier in the appropriate field (IP Address field if you choose IP Address as the address type, or hostname if you have chosen Hostname).
5. Click **Modify** to save the changes made to this address.

## Deleting an Address

You can delete an address only from the current domain. The address from the Global domain, which is visible in the child domain, cannot be deleted.

To delete an address:

1. Select **Security Director > Object Builder > Addresses**.  
The Address page appears.
2. Select the address you want to delete, right-click and select **Delete Addresses**.  
The Delete dialog box appears.
3. Select the address you want to delete and click **Delete**.  
Only addresses from the current domain are deleted.

## Cloning an Address

To clone an address:

1. Select **Security Director > Object Builder > Addresses**.  
The Address page appears.
2. Select the address you want to clone, right-click, and select **Clone Address**.  
You are redirected to the Clone Address page.
3. Make the necessary modifications and click **Clone**.

## Exporting Addresses

To export addresses:

1. Select **Security Director > Object Builder > Addresses**.  
The Address page appears.
2. Select the addresses you want to export, right-click, and select **Export Addresses to CSV**.  
The Export Addresses pop-up window appears.
3. Click **Export Selected** to export the addresses you have selected.
4. If you want to export all addresses to CSV, click the **Export Addresses to CSV** link from the Actions, and click **Export All** from the Export Addresses pop-up window.

The addresses from the current and parent domains are exported to CSV. The domain column is shown in the exported CSV.

## Importing Addresses

To import addresses:

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Right-click the address and select **Import Addresses from CSV**.

The Select CSV File window appears.

3. Click **View Sample CSV** to view a sample CSV file. The supported values in the Type field are:

- Host
- Network
- Range
- Wildcard
- DNS Host

4. Click **Browse** and navigate to the location where you saved the CSV file.

5. Click **OK** and then click **Import**.

Importing addresses from CSV creates addresses from the current domain or modifies addresses of the current domain. The new CSVs have an additional Domain Name column in the report. The Older CSVs are also compatible and you can use them for import.

## Find Duplicate Address Objects

To find duplicate address objects:

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Select the address for which you want to find the duplicate objects. Right-click the address, and then click **Show Duplicates**.

A window appears showing all the groups with duplicate objects, as shown in [Figure 19 on page 129](#).

**Figure 19: Page Showing Duplicate Address Objects**

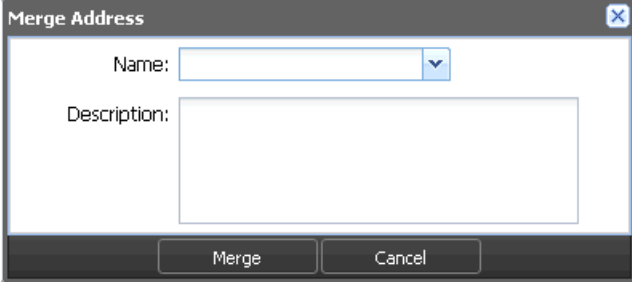
Name	Type	Host Name	IP Address	Description	
1.1.1.1 (2 members)					Merge
Copy_of_host	Host		1.1.1.1		
host	Host		1.1.1.1		
2.2.2.0-2.2.2.20 (2 members)					Merge
3.3.3.0/24 (2 members)					Merge
10.0.0.0/255.0.0.255 (2 members)					Merge
dns (2 members)					Merge
4.4.4.0-4.4.4.255 (2 members)					Merge
2::2 (2 members)					Merge
2::0/20 (2 members)					Merge
emptygrp1 (2 members)					Merge
group1 (2 members)					Merge

The duplicate objects only from the current domain are listed.

3. If you want to merge duplicate objects in a group, select the objects in a group and click **Merge**.

A merge window appears as shown in [Figure 20 on page 130](#). In the Name field, provide a new object name or select existing object names from the list.

**Figure 20: Merge Address Page**



The image shows a 'Merge Address' dialog box. It has a title bar with a close button. Inside, there is a 'Name:' label followed by a text input field and a dropdown arrow. Below that is a 'Description:' label followed by a larger text input area. At the bottom, there are two buttons: 'Merge' and 'Cancel'.

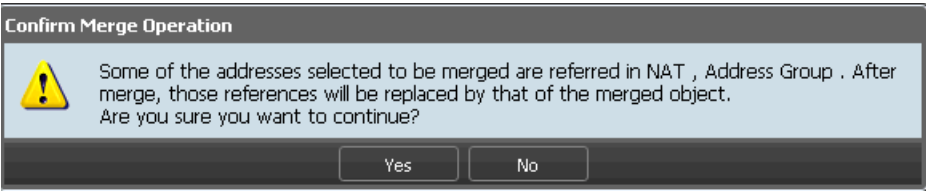


**NOTE:** You can merge all the objects in a group by clicking the Merge button after selecting all the objects by clicking the group name.



**NOTE:** If the selected duplicate objects are referenced in any other services (firewall policy, NAT policy, or VPN), and security objects (NAT pool, address groups), a warning message is provided before the objects are merged, as shown in [Figure 21 on page 130](#).

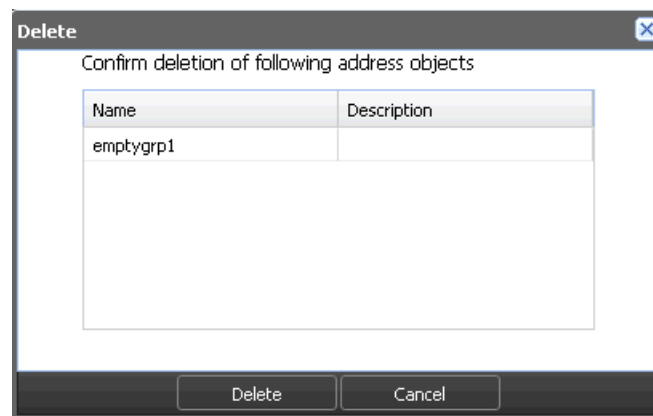
**Figure 21: Merge Operation Confirmation Message**



The image shows a 'Confirm Merge Operation' dialog box. It has a title bar. Below the title bar is a yellow warning triangle icon. To the right of the icon, the text reads: 'Some of the addresses selected to be merged are referred in NAT , Address Group . After merge, those references will be replaced by that of the merged object. Are you sure you want to continue?'. At the bottom, there are two buttons: 'Yes' and 'No'.

4. If you want to delete objects in a group, select an object or objects, right-click and then select **Delete**. A confirmation window appears before the selected objects are deleted, as shown in [Figure 22 on page 131](#).

Figure 22: Duplicate Objects Delete Confirmation Page



Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

5. If you want to find the usage of the duplicate objects in other groups, select an object, right-click, and then select **Find Usage**.

The usage window appears showing the usage of the selected object in any service (firewall policy, NAT policy, or VPN), or security objects (NAT pool, address groups).

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Find Address Usage

To find address usage:

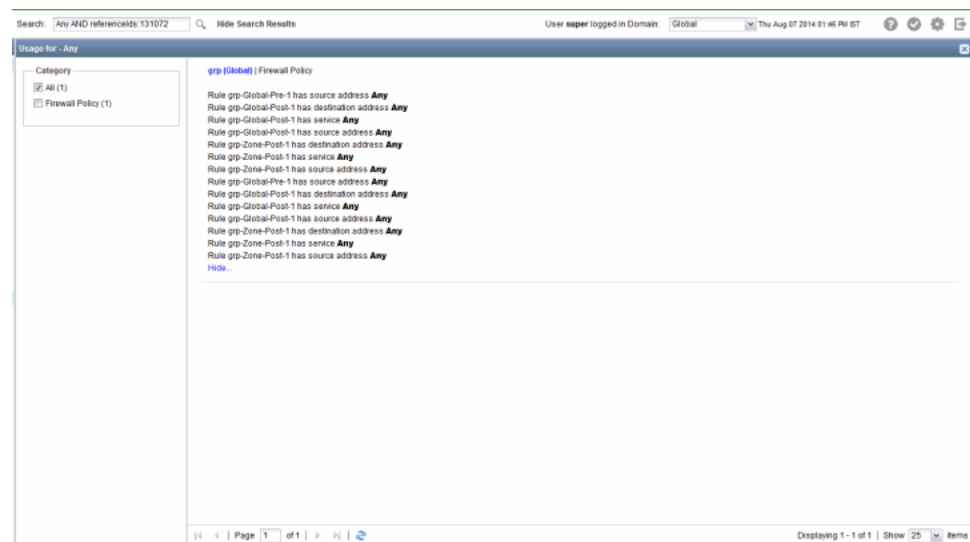
1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Select the address for which you want to find the usage. Right-click the address, and then click **Find Usage**.

A window appears, showing all the locations where this address object is used and also the search syntax is shown in the global search tool, as shown in [Figure 23 on page 132](#).

Figure 23: Window Showing Address Usage



If an address is used across domains, you can only navigate to policies of the current domain. A warning message is shown if you navigate to policies of other domains.

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Replace Addresses

You can select one or more addresses to replace with another address, address group, or nested address group. To replace one or more addresses:

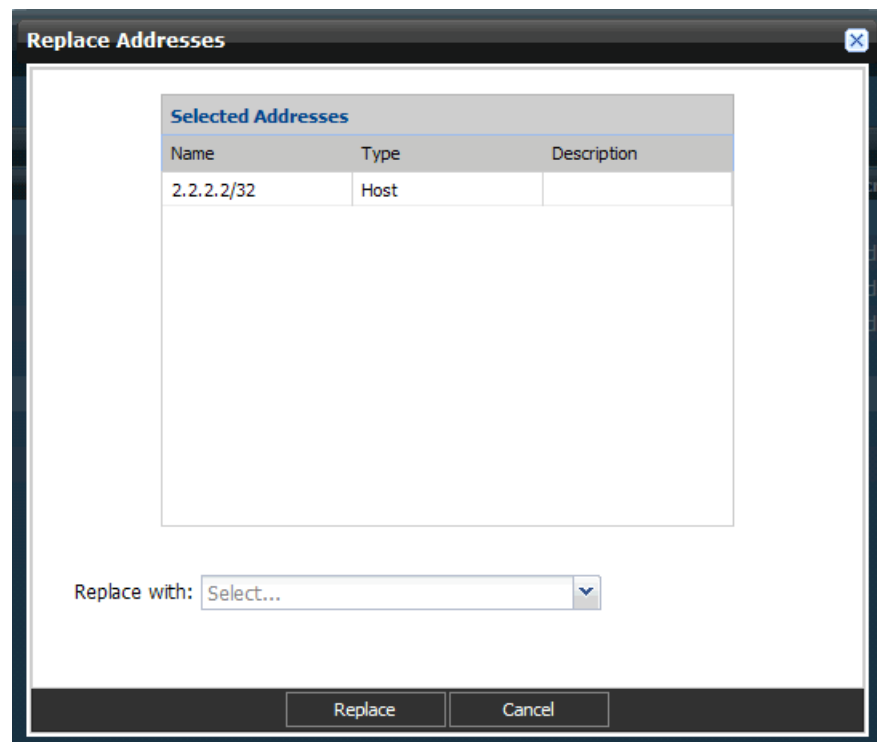
1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Select the address or addresses that you want to replace. Right-click the address or addresses, and then click **Replace Addresses**. You can replace a single address or multiple addresses.

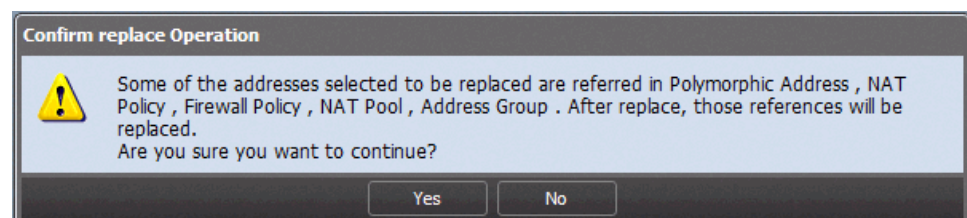
A window appears, showing the address or addresses you have selected to be replaced, along with a drop-down list of the addresses that are available to replace the address or addresses you have selected. See [Figure 24 on page 133](#).

Figure 24: Replace Addresses Window



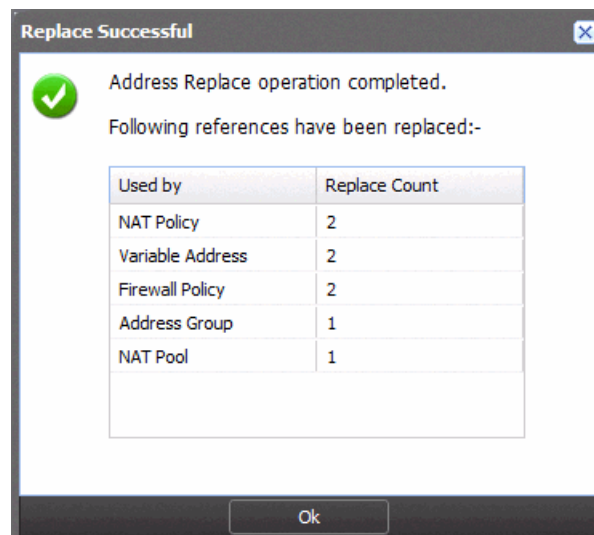
3. In the Replace Addresses window, select the address, address group, or nested address group that will replace the selected address or addresses, and click **Replace**. If the selected addresses are used in any other references, you will receive the following warning message before replacing, as shown in [Figure 25 on page 133](#). Click **Yes** to replace.

Figure 25: Address: Confirm Replace Warning Message



If the operation is successful, you will receive a summary showing the addresses that were replaced, as shown in [Figure 26 on page 134](#).

Figure 26: Address Replace Success Message

**NOTE:**

- You cannot replace VPN with IPv6, DNS, or wildcard addresses.
- You cannot replace addresses with polymorphic addresses or vice versa.
- Only the addresses from the services (firewall, NAT, or VPN policy) or from the address group of the current domain are replaced.

## Show Unused Addresses

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. You can either right-click any address or use the Action, and select **Show Unused**.

A list of all unused address objects which are not referenced in any policy or address group, appear on the page. The unused objects only from the current domain are listed.

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Delete All Unused Addresses

You can find the unused address objects and delete all unused address objects. You can clear all the unwanted objects which are not used anywhere.

To deleted the unused addresses:

1. Select the unused address object that you want to delete, and right-click the object, or use the Actions and select **Delete All Unused Addresses**

A warning message appears, confirming the delete operation.

2. Click **Yes** to delete all unused address objects, or **No** to cancel the delete operation.  
Only unused addresses from the current domain are deleted.

## Assigning Addresses to Domains

You can assign or reassign addresses to different domains. You can assign only one address at a time; multiple selections are not allowed. Before assigning an address to other domain, Security Director checks for the validity of the move. For example, you cannot move an address in the Global domain to a child domain, if it is used by a policy in the Global domain. A warning message is shown for such scenarios.

To assign an address to a domain:

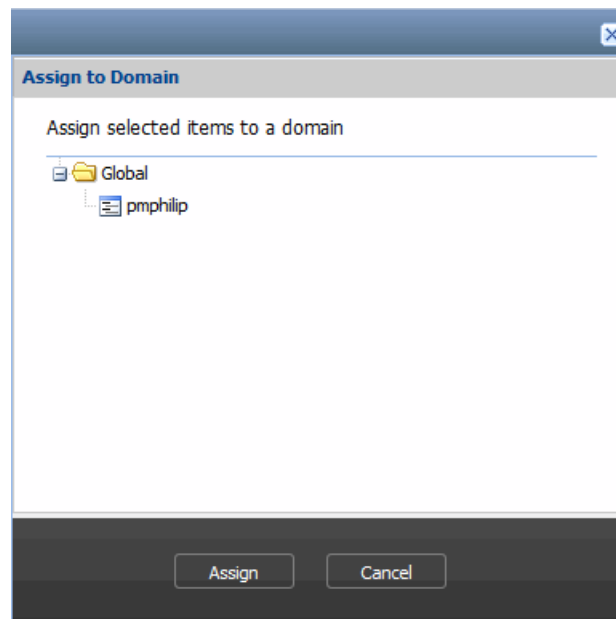
1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. You can either right-click an address or use the Actions, and select **Assign to Domain**.

The Assign to Domain page appears as shown in [Figure 27 on page 135](#).

**Figure 27: Addresses-Assign to Domain**



3. Select the required domain to assign the address, and click **Assign**.

The selected domain is assigned to the address.



**NOTE:** You cannot assign or reassign domains for predefined addresses. These domains are always assigned to the System domain.

- Related Documentation**
- [Address and Address Groups Overview on page 121](#)
  - [Creating Addresses on page 124](#)
  - [Creating Address Groups on page 136](#)
  - [Managing Address Groups on page 137](#)

## Creating Address Groups

To create an address group:

1. Select **Security Director > Object Builder > Address**.  
The Address page appears showing all the addresses and address groups.
2. To create a new address group, click the plus sign (+).
3. Select the Object Type as Address Group, as shown in [Figure 28 on page 136](#).

**Figure 28: Create Address Group Page**

Name	IP Address	Host Name	Type
64.5.195.25	64.5.195.25		Host
64.5.145.253	64.5.145.253		Host
64.4.111.0_27	64.4.111.0/27		Netw
10.159.2.0/25	10.159.2.0/25		Netw
64.34.14.0/24	64.34.14.0/24		Netw
64.74.223.36/	64.74.223.36		Host
64.74.80.0/24	64.74.80.0/24		Netw



**NOTE:** The number of allowable objects in one group depends on the model of the SRX Series device.

4. In the Name field, enter a name for the new address group.
  - The address group name must be a string beginning with a number or letter and consisting of letters, numbers, dashes, and underscores.
  - The address group name must be a string and cannot contain special characters such as &, <, >, and \n.
  - The maximum number of characters allowed in the address group name is 63.

5. In the Description field, enter a description for the new address group. The description must be a string and cannot contain special characters such as &, <, >, and \n.
6. In the Addresses field, from the Available dialog box, select the address that you want to group, and click the right arrow to add to the Selected column.

Click **All** to move all the addresses to the Selected column. The address you have selected appears in the Selected section of the dialog box.

7. Click **Create**.

The address group appears on the Address page.

#### Related Documentation

- [Address and Address Groups Overview on page 121](#)
- [Managing Address Groups on page 137](#)
- [Creating Addresses on page 124](#)
- [Managing Addresses on page 126](#)

---

## Managing Address Groups

You can modify, delete, or clone address groups listed on the Manage Address page.

To open the Address page:

- Select **Security Director > Object Builder > Address**.

The Address page appears.

You can right-click the address group to manage it.

You can perform the following tasks on the Address page:

1. [Modifying an Address Group on page 137](#)
2. [Deleting an Address Group on page 138](#)
3. [Cloning an Address Group on page 138](#)

## Modifying an Address Group

To modify an address group:

1. Select **Security Director > Object Builder > Addresses**.

The Address page appears.

2. Select the address group you want to modify, right-click, and select **Modify Address**.

This action redirects you to the window that you used to create a new address group. You can modify all the fields in this window, except the Name field.

3. In the Description field, enter the new description. The description must be a string and cannot contain special characters such as &, <, >, and \n.

4. In the Members pane, make the appropriate changes to the addresses used in this group.
5. Click **Modify** to save the changes made to this address group.

## Deleting an Address Group

To delete an address group:

1. Select **Security Director > Object Builder > Addresses**.  
The Address page appears.
2. Select the address you want to delete, right-click, and select **Delete Addresses**.  
The Delete dialog box appears.
3. Select the address group you want to delete and click **Delete**.

## Cloning an Address Group

To clone an address group:

1. Select **Security Director > Object Builder > Addresses**.  
The Address page appears.
2. Select the address you want to clone, right-click, and select **Clone Addresses**.  
You are redirected to the Clone Address page.
3. Make necessary modifications and click **Clone**.

### Related Documentation

- [Address and Address Groups Overview on page 121](#)
- [Creating Address Groups on page 136](#)
- [Creating Addresses on page 124](#)
- [Managing Addresses on page 126](#)

# Creating and Managing Zone Sets

- [Creating a Zone Set on page 139](#)
- [Managing Zone Sets on page 140](#)

## Creating a Zone Set

You can group one or more zones into a group and reference them in the global firewall rules. To create a new zone set:

1. Select **Security Director > Object Builder > Zone Sets**.

The Zone Sets page appears, listing the existing zone sets.

2. To create a zone set, click the plus sign (+).

The Create Zone Set page appears, as shown in [Figure 29 on page 139](#).

**Figure 29: Create Zone Set**

**Create Zone Set**

Name\*:  ⓘ

Description:

Zones:

Available		Selected	
Zones	Domain	Zones	Domain
A1			
MGMT			
RI_TUNN_ZONE			
UNTRUST			
VPN			
Z1			
Zone			
junos-host			
rbalugu-chng			
rbalugu123			

Total: 117

Create Cancel

3. In the Name field, enter the name of the new zone set.
  - The zone name must be a string beginning with a number or letter and consisting of letters, numbers, dashes, and underscores.

- The zone name must be a string and cannot contain special characters such as &, <, >, and \n.
  - The maximum number of characters allowed in the zone name is 63.
4. In the Description field, enter a description of the zone set. The description must be a string and cannot contain special characters such as &, <, >, and \n.
  5. In the Zones section, all zones from devices managed by Security Director are displayed in the Available column. Zones for the child domain are also listed.  
  
Choose one or more zones from the Available column and move them to the Selected column.
  6. Click **Create**.  
  
A new zone set is created.

**Related Documentation** • [Managing Zone Sets on page 140](#)

---

## Managing Zone Sets

You can modify, delete, clone, show unused, and find usage for zone sets.

To open the Zone Sets page:

- Select **Security Director > Object Builder > Zone Sets**.  
  
The Zone Sets page appears, listing the zone sets.
- Right-click the zone set to manage it, or select the required options from Actions.

You can perform the following management tasks on the Zone Sets page:

- [Modifying a Zone Set on page 140](#)
- [Deleting a Zone Set on page 141](#)
- [Cloning a Zone set on page 141](#)
- [Showing Duplicate Zone Sets on page 141](#)
- [Finding Zone Set Usage on page 141](#)
- [Showing Unused Zone Sets on page 142](#)
- [Deleting All Unused Zone Sets on page 142](#)

## Modifying a Zone Set

To modify a zone set:

1. Select **Object Builder > Zone Sets**.  
  
The Zone Sets page appears.
2. Right-click the zone set and select **Modify ZoneSet**, or click the pencil icon.  
  
The Modify ZoneSet page appears.

3. You can modify the name, description, and zones selected for that zone set.
4. Click **Modify**.

The required values are modified and saved.

## Deleting a Zone Set

To delete a zone set:

1. Select **Object Builder > Zone Sets**.

The Zone Sets page appears.

2. Right-click the zone set that you want to delete, and select **Delete ZoneSets**.

You can also click the minus sign (-) to delete the zone set.

3. A confirmation message appears before deletion. Click **Delete**.

The required zone set is deleted.

## Cloning a Zone set

To clone a zone set:

1. Select **Security Director > Object Builder > Zone Sets**.

The Zone Sets page appears.

2. Select the zone set you want to clone, right-click, and select **Clone ZoneSet**.

You are redirected to the Clone ZoneSet page.

3. Modify the required field values, and click **Clone**.

## Showing Duplicate Zone Sets

To view the duplicate Zone sets:

1. Select **Security Director > Object Builder > Zone Sets**.

The Zone Sets page appears.

2. Select the zone set within which you want to find the duplicate objects. Right-click the zone set and click **Show Duplicates**.

A window appears, showing all the sets that include the duplicate objects.

## Finding Zone Set Usage

To find usage for a zone set:

1. Select **Security Director > Object Builder > Zone Sets**.

The Zone Sets page appears.

2. Select the zone set for which you want to find the usage. Right-click the zone set and then click **Find Usage**.

A window appears, showing all the locations where this object is used and also the search syntax is shown in the global search tool.

## Showing Unused Zone Sets

To view all the unused zone sets:

1. Select **Security Director > Object Builder > Zone Sets**.

The Zone Sets page appears.

2. You can either right-click any zone set or use the Actions, and select **Show Unused**.

A list of all unused zone sets that are not referenced in any policy appear on the page.

## Deleting All Unused Zone Sets

You can find the unused zone sets and delete them. You can clear all the unwanted objects that are not used anywhere.

To delete all unused zone sets:

1. Select the unused zone set that you want to delete and right-click, or, from the Action, select **Delete All Unused**.

A confirmation message appears before deletion.

2. Click **Yes** to delete all unused zone sets, or **No** to cancel the delete operation.

**Related Documentation**

- [Creating a Zone Set on page 139](#)

## CHAPTER 12

# Creating and Managing Variables

- [Creating Variable Definitions on page 143](#)
- [Managing Variable Definitions on page 147](#)

### Creating Variable Definitions

---

To create variable definitions:

1. Select **Security Director > Object Builder > Variables**.

The Variables page appears. This page displays all the variables you have created.

2. Click the plus sign (+) to create a polymorphic object..

The Create Variable Definition page appears, as shown in [Figure 30 on page 144](#). You can create a variable definition on this page.

Figure 30: Create Polymorphic Object Page

**Create Variable Definition**

Name:  ❗ This field is required

Description:

Type: ☒ Address ☐ Zone

Default Address:  +

Add   Delete	
<input type="checkbox"/>	
Context Value	Address

Create Cancel

3. Enter the name of the variable definition in the Name field.
4. Enter a description for the variable definition in the Description field.
5. Select the type of variable definition, either Address or Zone, from the Type field.
6. Select the default address value from the Default Address menu.
7. To add variable values:
  - If the Type is Address:
    - a. Click the **Add** icon.
    - A new row appears.
    - b. Double-click the **Context Value** field, and select the device.
    - c. Double-click the **Address** field, and select the address for the device from the menu.
  - If the Type is Zone:
    - a. Click the **Add** icon.
    - A new row appears.
    - b. Double-click the **Context Value** field, and select the device.

- c. Double-click the **Zone** field, and select the zone, either trust or untrust, from the menu.

8. Click **Create**.

During the creation of variables, devices from only the current and child domain are listed. Devices in a domain whose view parent is disabled are not listed.

You can create and address or address groups for the polymorphic objects. To create an address or address group:

1. Click the plus sign (+).

The Create Address Object page appears, as shown in [Figure 31 on page 145](#).

**Figure 31: Inline Address Group Creation for a Polymorphic Object**

**Create Address Object**

Object Type: ☒ Address ☐ Address Group

Name:

Description:

Type: Host

IP  Get IP Get Hostname

2. To create an address object, select the **Address** radio button, and configure the following parameters:
  - In the Name field, enter the name of the address object
  - In the Description field, enter a description.
  - From the Type drop-down list, select the type as Host, Range, or Network.
  - In the IP field, enter IPv4 or IPv6 address.
  - In the Host Name field, enter the host name.
  - To create a new address object, click **Create**.

- To create an address group, select the **Address Group** radio button.

A page appears to create an address group, as shown in [Figure 32 on page 146](#). Configure the following parameters:

**Figure 32: Create Address Object-Inline Address Group Creation Page**

**Create Address Object**

Object Type: ☐ Address ☒ Address Group

Name:

Description:

Addresses:

Available		Selected	
Filter	Select: <a href="#">All</a> <a href="#">None</a>		Select: <a href="#">All</a> <a href="#">None</a>
10.159.2.0/25 (10.159.2.0/25)	Global		
10.159.3.0/24 (10.159.3.0/24)	Global		
10.159.4.0/24 (10.159.4.0/24)	Global		
144.201.76.32 (144.201.76....)	Global		
Addr-66.0.192.112/28 (66.0....)	Global		
Addr-66.184.206.216 (66.18....)	Global		
Total: 211			
<input type="checkbox"/> Host	<input type="checkbox"/> Network	<input type="checkbox"/> Wildcard	<input type="checkbox"/> Range
		<input type="checkbox"/> Other	

- Enter the name of an address group in the Name field.
- In the Addresses filed, you can select all addresses available in the Available column or select few addresses to create a new address group.
- Click **Create** to create the address group. This adds the newly created address objects to the selected addresses and returns to the address selector. Click **Cancel** to discard your changes and return to the Create NAT Pool window.

You can also add variables using the Variables import functionality. To use this functionality, select the Actions drawer and click **Import Variables from CSV**. You can export the variables using the Variables export functionality. To use this functionality, select the variables you want to export and click **Export Variables to CSV** from the Actions drawer.

In the CSV file, device-to-address or device-to-zone mapping is provided. After the import, polymorphic address or polymorphic zone is created based on the information available in the CSV file.



**NOTE:** You can search variables by name, description, or default value in the search box available at the top right corner of the Manage Variables page. If you want to tag the variables, right-click the variable and select a tag option. After tagging, you can search for variables by the respective tag names.

#### Related Documentation

- [Managing Variable Definitions on page 147](#)

## Managing Variable Definitions

You can delete, modify, or clone the variable definitions listed on the Variables page.

To open the Variable page:

- Select **Security Director > Object Builder > Variables**.

The Variables page appears.

You can right-click the variable definition to manage it.

You can perform the following tasks on the Variables page:

- [Deleting Variable Definitions on page 147](#)
- [Modifying Variable Definitions on page 147](#)
- [Cloning Variable Definitions on page 148](#)

## Deleting Variable Definitions

To delete a variable definition:

1. Select **Security Director > Object Builder > Variables**.

The Variables page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to delete, and right-click **Delete Variable Definitions**.



**NOTE:** You can also delete the variable definition by right-clicking the variable definition and selecting Delete Variable Definitions. You can select more than one variable to delete.

## Modifying Variable Definitions

To modify a variable definition:

1. Select **Security Director > Object Builder > Variables**.

The Variables page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to modify, right-click and select **Modify Variable Definition**.

The Modify Variable Definitions page appears. You can make the modifications on this page.



**NOTE:** You can also modify the variable definition by right-clicking the variable definition and selecting **Modify Variable Definition**.

3. Click **Modify**.

## Cloning Variable Definitions

To clone a variable definition:

1. Select **Security Director > Object Builder > Variables**.

The Variables page appears. This page displays all the variable definitions you have created.

2. Select the variable definition you want to clone, right-click and select **Clone Variable Definition**.

The Clone Variable Definitions page appears. You can make the modifications on this page.



**NOTE:** You can also clone the variable definition by right-clicking the variable definition and selecting **Clone Variable Definition**.

3. Click **Clone**.

## PART 7

# Configuring Firewall Policies

- [Creating and Managing Firewall Policies on page 151](#)
- [Creating and Managing Application Signatures on page 229](#)
- [Creating and Managing Schedulers on page 237](#)
- [Creating and Managing Policy Profiles on page 243](#)



## CHAPTER 13

# Creating and Managing Firewall Policies

- [Firewall Policies Overview on page 151](#)
- [Multiple Group Policy Membership Overview on page 155](#)
- [Creating Firewall Policies on page 159](#)
- [Unlocking Locked Policies on page 174](#)
- [Inline Creation of Objects in Policy on page 176](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)
- [Policy Priority Precedence Setting on page 188](#)
- [Tracking the Utility Rate of Security Firewall Policies on page 190](#)
- [Publishing Firewall Policies on page 194](#)
- [Managing Firewall Policies on page 201](#)

## Firewall Policies Overview

---

Security Director provides you with four types of firewall policies:

- **All Devices**—Predefined firewall policy that is available with Security Director. You can add prerules and postrules. When the all devices policy configuration information is updated on the devices, the rules are updated in the following order:
  - All devices prerules
  - Group prerules
  - Device-specific rules
  - Group postrules
  - All devices postrules

All devices policy enables rules to be enforced globally to all the devices managed by Security Director. All devices policy is part of the Global domain and is visible in all the child domains if the view parent is enabled.

- **Group**—Type of firewall policy that is shared with multiple devices. This type of policy is used when you want to update a specific firewall policy configuration to a large set of devices. You can create group prerules, group postrules, and device rules for a group

policy. When a group firewall policy is updated on the devices, the rules are updated in the following order:

- Group prerules
- Device-specific rules
- Group postrules

During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.

- **Device Policy**—Type of firewall policy that is created per device. This type of policy is used when you want to push a unique firewall policy configuration per device. You can create device rules for a device firewall policy.

Security Director views a logical system like it does any other security device, and it takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

During a device assignment for a device policy, only devices from the current domain are listed.



**NOTE:** If Security Director discovers the root logical system, the root lsys discovers all other user lsys inside the device.

---

- **Device-Exception Policy**—Type of firewall policy that is created when a device is removed from a group policy.

If you move a device from one domain to another and the move is valid, the device-exception policy is also moved from the current domain to the target domain. This is possible if the view parent mode is enabled in the target domain. If the view parent is not enabled in the target domain, the move is not valid.

- **Global Policy**—Global Policy Rules are enforced regardless of ingress or egress zones; they are enforced on any device transit. Any objects defined in the Global Policy Rules must be defined in the global address book.

Security Director permits users to manage the current zone-based firewall policies and the new global policy rules supported in SRX Series devices. To achieve this the current policy model categorizes the rule bases into zone and global policies. Also, all the existing and new firewall policy features extend to the global rule base. The base includes the prerule or postrule predefined groups and the inheritance concept of current firewall policies. Because both the rule bases are managed within a single firewall policy, there is no change in workflow for publish and update. Therefore, both the zone-based rules and global base rule are published and updated together.

The basic settings of a firewall policy are obtained from the policy profile. The basic settings include log options, firewall authentication schemes, and traffic redirection options.

Firewall policies are displayed in the Tabular view. The left pane of the Tabular view displays all firewall policies. The right pane of the Tabular view displays the rules for the firewall policy that is highlighted in the left pane.

## Rule Base Overview

Security Director allows you to configure one type or both types of rule bases for each policy. If devices are assigned to a policy that does not have one of the rule bases under its management, Security Director still interprets that rule base as being under its scope. For example, if you configure firewall policies out of band on a device under an unmanaged rule base, Security Director deletes those policies. If you do not select the previously configured rule base in a policy in the Security Director policy modify workflow, Security Director automatically deletes all rules in the policy in the next publish and update.

### Example: UnManaging a Previously Managed Rule Base

---

You can remove a managed device from the Security Director management scope. To unmanage a previously managed rule base when no other policies are published on the device except the existing policy:

1. Do not select the Manage Global Policy option on modifying a device policy in Security Director.
2. Security Director deletes the global rule base in the design data of the Security Director application.
3. Publish a policy and update the device. The update deletes all global rules from the device.
4. On successful update, the all devices policy for the device is removed from the Security Director management scope.



**NOTE:** Security Director will continue to delete any all devices policy configured on the device through the CLI at subsequent publish updates.

---

## Policy Analysis

---

Over a period of time, the firewall rule bases can become inefficient as rules become disorganized, causing some rules to become ineffective. This is primarily because of the lack of timely notification given to the end users when they create a new rule or change a rule, if the new rule or changed rule adversely affects the other rules in the rule base. This problem can be addressed by analyzing the policy and reporting the anomalies in the rules of a policy to the end user. Policy analysis reports shadowing and redundant anomalies in a rule; these reports are available in PDF format. Also, policy analysis finds the anomaly between the address and service of the rules.

Policy analysis helps you to analyze the firewall rule base for policies managed by Security Director, and identifies the firewall rules that contain the following issues:

- **Shadowing**—This occurs when a rule higher in the order of the rule base matches with all the packets of a rule lower in the order of the rule base. The shadowed rule is never activated. The possible solution is to reorder the rules, or disable or delete one of the rules. The anomaly calculation is not made for the disabled rules.
- **Redundant**—This occurs when there are two or more rules that perform the same action on the same packets along with the same settings or configurations. The solution is to disable or delete the redundant rules.

The policy analysis report is generated in PDF format and can be e-mailed them to multiple recipients. The reports contain a summary and a pie chart showing all anomalies. You can schedule the report generation.

The following list shows the policy analysis behavior for different types of firewall policies:

- **All devices policy**—This analyzes all the rules present on the right pane of the firewall policy landing page, within the all devices policy.
- **Group policy**—This analyzes all the rules present on the right pane of the firewall policy landing page, within the group policy including the all devices policy rules.
- **Device policy**—This analyzes all the rules present on the right pane of the firewall policy landing page, within the device policy including the all devices policy rules. If you want to analyze all the rules present on a device, you must generate the report by clicking the device policy.
- **Device exception policy**—This analyzes all the rules present on the right pane of the firewall policy landing page, within the device exception policy including all device policy rules and the group policy rules in which the device has been assigned.

The policy analysis is not performed under the following scenarios:

- Disabled rules are not considered for the policy analysis calculation.
- Apart from Address (source and destination) and Service columns, no other columns in the firewall landing page are considered for the policy analysis calculation.
- Variable address, wild card address, and exclude address are not considered for the policy analysis calculation.

## Custom Column Overview

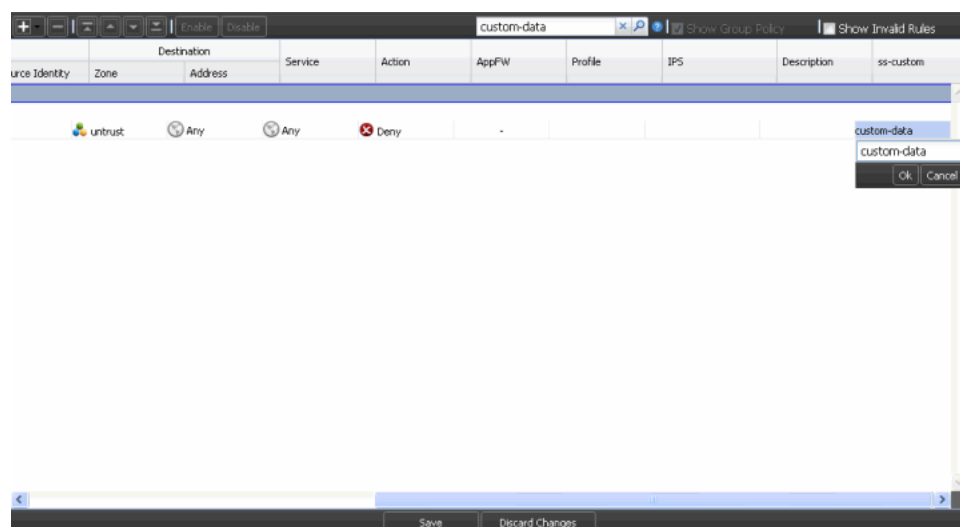
The Custom Column feature is a more structured mechanism used for various purposes such as for tracking changes to firewall policies, owner of the rule, by allowing you to define custom column views. Once the custom columns are defined, they appear on the right pane of the grid, similar to other columns. Data in these columns can be captured and saved in the same way as with other columns. You can also search the custom column data.

You can create a maximum of three custom columns in each domain.

### Custom Column Data Search

Once you entered or modified custom column data, you can perform searches on the data. Security Director searches for the data you specify within the custom column data you have created and filters the results by the rule name that matches the custom column name as well as by the custom column data, as shown in [Figure 33 on page 155](#).

**Figure 33: Custom Column Data Search**



#### Related Documentation

- [Creating Firewall Policies on page 159](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)
- [Managing Firewall Policies on page 201](#)
- [Publishing Firewall Policies on page 194](#)

## Multiple Group Policy Membership Overview

The Multiple Group Policy Membership feature supports the placing of devices in more than one policy group, and assigning priorities to the policy groups. This way, the policies, and the rules within them, are applied in the desired order.

The group priority of firewall group policy has the following two parts:

- Priority
- Precedence

Priority indicates the order in which rules are pushed to the device. Priority can be set to high, medium, or low. Precedence is a value that controls the ordering of group policies within a priority level. If two policies are assigned the same priority, their precedences set the order in which the rules are pushed.

## General Rules About Priority and Precedence

When you create or edit a group policy, if you set the precedence to the same value as an existing policy, the newly created or modified policy gets the assigned precedence. The existing group policy that had the same precedence, and all lower priority (higher precedence value) policies, will have their precedence value increased by 1.

If you make changes to a policy, such as deleting a policy or moving a policy from a different priority level, Security Director reorders the precedence of all policies in that priority level.

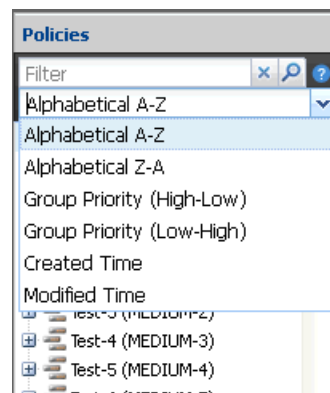
### Example: New Precedence of a Policy Set to the Same Precedence as an Existing Policy

In this example, three medium-priority policies, PolicyA, PolicyB, and PolicyC, are assigned precedences 1, 2, and 3, respectively. If you create a new policy, PolicyNew, and set the priority to medium and the precedence to 2, the order of the policies changes to PolicyA, PolicyNew, PolicyB, and PolicyC, with precedence 1, 2, 3, and 4, respectively.

## Sorting of Firewall Policy Left Pane

The left pane of the firewall policies can be sorted based on priority or precedence values, alphabetically, and by creation or modification time, as shown in [Figure 34 on page 156](#). Global policies always appear at the top of the right pane, and device policies appear at the bottom of the right pane. Only group policies are sorted.

Figure 34: Sorting Order in the Firewall Policy Left Pane



[Table 20 on page 157](#) shows the different sorting orders available for firewall policies.

Table 20: Sorting Order for Firewall Policies

Sorting Order	Description
Alphabetical A-Z	Group policies are sorted alphabetically in ascending order.
Alphabetical A-Z	Group policies are sorted alphabetically in descending order.
Group Priority (High-Low)	Group policies are sorted in the order High, Medium, and Low. For the same priorities, the lower precedence number is placed in the top. For example, High 1 has higher precedence than High 2.
Group Priority (Low-High)	Group policies are sorted in the order Low, Medium, and High. For the same priorities, the higher precedence number is placed in the top. For example, Low 3 has lower precedence than Low 2.
Created Time	Policies are listed based on creation time. The policy created first is placed at the top.
Modified Time	Last modified policies are placed at the bottom (last).

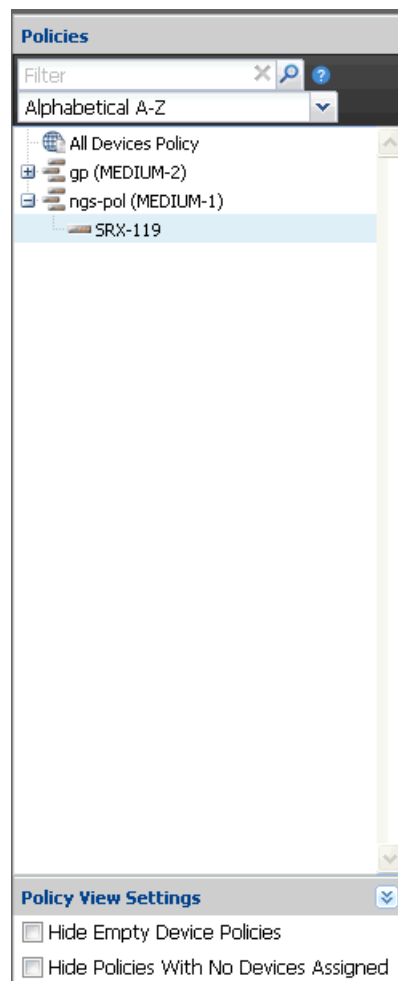


**NOTE:** You cannot set the precedence value greater than the available precedence values that are assigned to the available priority policies. Based on the priority of the policies, the precedence values are applied.

To hide the policies in the left pane that do not have any defined rules:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Empty Device Policies** check box to hide the device exception policies that do not have any rules, as shown in [Figure 35 on page 158](#). Clicking the check box will only hide those device exception policies inside group policies that do not have any rules, not the empty standalone device policies.

Figure 35: Policy View Setting



To hide the policies in the left pane that do not have any devices assigned:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Policies With No Devices Assigned** check box to filter device and group policies that are not assigned to any device, as shown in [Figure 35 on page 158](#).
3. Policies without any assigned devices are hidden in the left pane.

**Related Documentation**

- [Managing Firewall Policies on page 201](#)
- [Policy Priority Precedence Setting on page 188](#)
- [Publishing Firewall Policies on page 194](#)

## Creating Firewall Policies

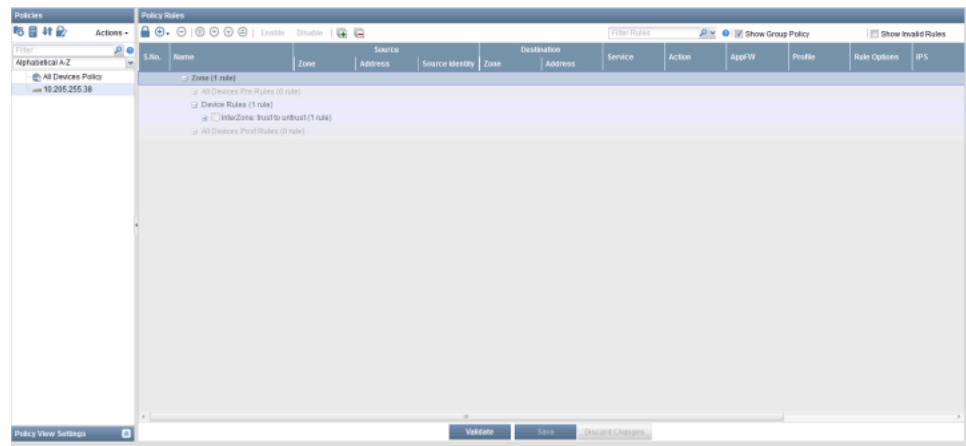
To create a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears. The Policy Tabular view is a table with three panes. The left pane displays all the firewall policies in the system, which includes device, group, and global firewall policies.

If you click a firewall policy in the left pane, the right pane displays the rules and rule groups for the respective policy, as shown in [Figure 36 on page 159](#).

**Figure 36: Firewall Policy Tabular View**



The right pane of the firewall policy divides the set of rules into two rule bases. All zone-based rules are grouped under Zone, and the SRX Series All Devices rules are grouped under Global. You cannot move a rule from one section to the other. The same set of features are available to both the rule bases, however.



**NOTE:** While adding rules, you can select to add them either to the zone rule base or to the global rule base.

2. To create a new firewall policy, click **Create Policy** icon from the middle Policies pane.

The Create Policy page appears, as shown in [Figure 37 on page 160](#). You can create a group policy or a device policy on this page.

Figure 37: Create Firewall Policy

3. Create a group policy:

- a. Enter the name of the group policy in the Name field.
- b. Enter a description for the group policy rules in the Description field. Security Director sends the comments entered in this field to the device.
- c. To manage the firewall rules for SRX Series devices, you can select the following Manage options:
  - Zone Policy—To manage zone-based firewall rules.
  - Global Policy—To manage the global firewall rules.
  - Both Zone and Global Policy—To manage both zone and global firewall rules.

By default, the Manage Zone Policy option is selected and used to manage zone-based firewall rules.

- d. To set the priority for a policy, select **High**, **Medium**, or **Low** from the Priority list.

Enter the order in which group policies are applied to a device when they are assigned multiple policy groups.

For example, if the system has 4 policies Low priority, 5 policies with Medium priority, and 3 policies with High priority, you can set the precedences as follows:

- Low-priority policies—1 through 4
  - Medium-priority policies—1 through 5
  - High-priority policies—1 through 3
- e. Select the profile for the group policy from the Profile menu.
  - f. Click the **Show only devices without policy assigned** check box to see the devices that are not assigned to an all devices policy.
  - g. Select the devices on which the group policy will be published, in the Select Devices pane, select the devices from the Available column and click the right arrow to move these devices to the Selected column.

You can also search for devices by entering the device name, device IP address, or device tags in the Search field in the Select Devices pane. Once the searched devices appear, you can move them to the Selected pane, as shown in [Figure 37 on page 160](#).

By default, all devices appear under Available tab whether or not they have been assigned to an all devices policy.

- h. Click **Create**.



**NOTE:** One device can hold configuration data related to one firewall policy only. Hence you cannot share devices for multiple firewall policies.

#### 4. Create a device policy:

- a. Enter the name of the device policy in the Name field.



**NOTE:**

- The device policy name must be a string beginning with a number or letter and consisting of letters, numbers, dashes, and underscores.
- The policy name must be a string and cannot contain special characters such as &, <, >, and \n.
- The maximum number of characters allowed in the policy name is 63.

- b. Enter a description for the device policy in the Description field. The description must be a string and cannot contain special characters such as &, <, >, and \n.
- c. To manage the firewall rules for SRX Series devices, you can select the following Manage options:
  - Zone Policy—To manage zone-based firewall rules.
  - Global Policy—To manage the global firewall rules.
  - Both Zone and Global Policy—To manage both zone and global firewall rules.

By default, the Manage Zone Policy option is selected and used to manage zone-based firewall rules.

- d. Select the profile for the device policy, from the Profile list.
- e. Select the device on which the device policy will be published from the Device list.
- f. Select the IPS mode from the IPS Configuration Mode list. The following [Table 21 on page 162](#) shows different IPS configuration modes and the purpose:

**Table 21: IPS Configuration Mode**

IPS Mode	Description
Basic	Turns IPS on or off. If you select this mode, you are given the option to select signature sets. Custom and predefined signature sets are listed. The IPS policy is generated by merging the rules from the signature sets you choose. The IPS policy is read-only.
Advanced	Turns IPS on or off. An empty IPS policy is generated. You can either add or delete, disable or enable, or modify IPS rules and exempt rules.
None	If this mode is selected, you cannot configure IPS on or off settings in a firewall rule. You cannot generate any IPS policies.

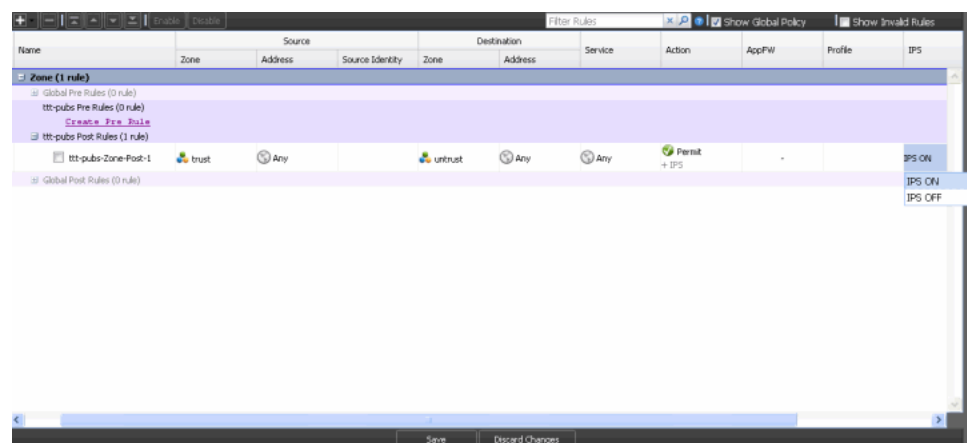
All these IPS modes are available for logical systems also.

- g. Click **Create**.

A tooltip option is available for group policies, device policies, and device exceptions listed in the left pane of the firewall policy ILP. This tooltip also displays the IPS mode.

You can turn the IPS policy on or off on a firewall rule by clicking on the IPS column, as shown in the [Figure 38 on page 162](#). This is available for each rule and you can set on or off only for advanced and basic modes.

**Figure 38: Turning an IPS Policy On or Off**

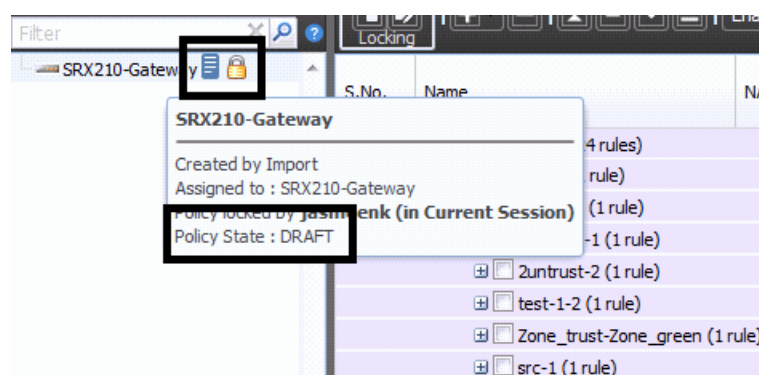


IPS on or off option is available only for permit and tunnel actions. Tooltip is also provided for the IPS column that shows the IPS mode and signature sets.

Validate policies by clicking the **Validate** button, available next to the Save and Discard buttons. If any errors are found during the validation, a red warning icon is shown for the respective policies. For firewall policies, expired schedulers and duplicate rule names are validated.

Security Director permits you to save policies that contain errors. Warnings messages are displayed for policies that contain errors, but you can proceed to save such policies as drafts. You cannot publish policies that are in the draft state. The tooltip for the policy shows the state as draft, as shown in [Figure 39 on page 163](#); because it is a draft, the tooltip does not show the publish option. When you save a policy as a draft, duplicate rule name errors are ignored.

**Figure 39: Policy with Error Saved as Draft**



**NOTE:** If you do not have permission to the device assigned to a device policy, you cannot view the policy in the respective policy ILP.



**NOTE:** When you are viewing a group policy, if you do not want the all devices policy rules to appear in the Policy Tabular view, uncheck the clear the Show Global Policies check box in the right pane. When you are viewing a device policy, if you do not want the global and group policy rules to appear in the Policy Tabular view, clear the Show Global/Group Policies check box in the right pane.



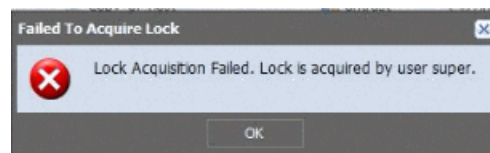
**NOTE:** You can use the search boxes in the left pane and right pane to search for firewall policies and the rules in a specific firewall policy, respectively.



**NOTE:** SRX Series logical systems support complete firewall policy configuration in Security Director. The captive portal is configured in the root logical system and referred from the user logical system. If IPS policy is assigned to a logical system, it enables only the basic IPS mode. When the logical system is published, you'll receive a warning message that the logical system shares only the root device configuration.

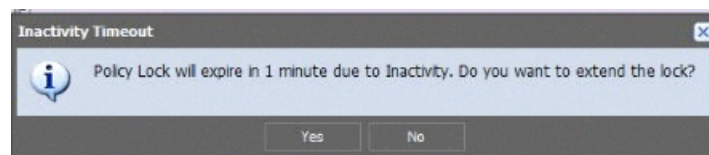
Before you can edit the policy, you must lock it by clicking the lock icon, which is available in the policy view toolbar, as shown in [Figure 36 on page 159](#). You can hold more than one policy lock at a given time. You can unlock the policy by clicking the unlock icon next to the lock icon in the policy tabular view. If you attempt to lock a policy that is already locked by another user, the following message appears, as shown [Figure 40 on page 164](#). The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

**Figure 40: Lock Failure Error Message for the Second User**



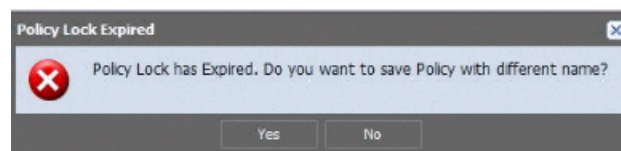
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 41 on page 164](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see ["Unlocking Locked Policies" on page 174](#).

**Figure 41: Inactivity Timeout Error**



Click **Yes** to extend the locking period. If you click **No**, and if there is activity on the policy within the last minute of the lock's life, the timer will be reset and the lock will not be released. If you ignore the message, when the policy lock timeout interval expires 1 minute later, you are prompted to either save the edited policy with a different name or lose the changes, as shown in [Figure 42 on page 164](#).

**Figure 42: Policy Lock Expired Message**



If you click **Yes** to save the edited policy with a different name, the following window appears, as shown in [Figure 43 on page 165](#). If you navigate away from the locked policy, you will get an option to save the edited policy with different name.

**Figure 43: Save the Edited Policy with a Different Name**

The 'Save As' dialog box contains the following fields and options:

- Name:** A text box containing 'copy\_of\_Corp-Gateway'.
- Description:** A text box containing 'Created by Import'.
- Manage Zone Policy:** A checked checkbox.
- Manage Global Policy:** An unchecked checkbox.
- Policy Priority:** A dropdown menu set to 'Low' with a help icon.
- Precedence:** A text box containing '3' followed by 'Of 16'.
- Profile:** A dropdown menu set to 'Select profile...'.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 44 on page 165](#).

**Figure 44: Unsaved Changes Warning Message**

The 'Policy Changed' dialog box contains the following elements:

- Title Bar:** 'Policy Changed' with a close button.
- Message:** 'Policy has changed since it was opened for view. Do you want reload policy?'.
- Buttons:** 'Yes' and 'No' buttons.

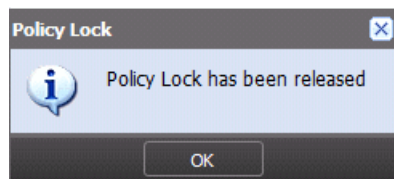
If Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 45 on page 165](#).

**Figure 45: Policy Unlock by Admin Message**

The 'A Policy Lock Has Been Removed' dialog box contains the following elements:

- Title Bar:** 'A Policy Lock Has Been Removed' with a close button.
- Icon:** An information icon (i).
- Message:** 'The lock for Firewall Policy "10.205.61.51" has been released by an administrator.'
- Buttons:** 'OK' button.

If you do not edit the locked policy and the policy lock timeout expires, the following warning message appears, as shown in [Figure 46 on page 166](#).

**Figure 46: Policy Lock Release Message**

The policy is locked and released for the following policy operations. Also, these operations are disabled for a policy, if the policy is locked by some other user.

- Modify
- Assign devices
- Rollback
- Delete

**NOTE:**

- You can unlock the policy by logging out of the application or when the policy lock timeout expires. You can unlock your policies even if they are not edited.
- If the browser crashes when the policy is still locked, the policy is unlocked only after timeout interval expires.
- If there is an object conflict resolution during a migration, import, or rollback, and if you are editing any objects, you will receive a save as option for the edited objects. The behavior is the same when you import addresses from CSV.
- Policy lock is not released under the following scenario:
  - If you save or discard you changes to the locked policy.
  - if you do not make any changes to the locked policy and navigate to another policy.
- It is recommended to configure the session time longer than the lock timeout value.

---

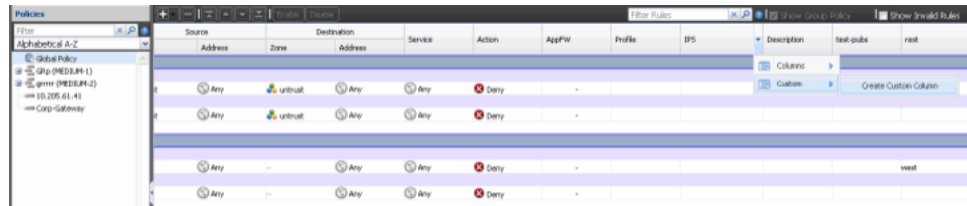
To create a custom column definition for the firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Click on any field in the rule table header, select **Custom**, and then **Create Custom Columns**.

Figure 47: Creating Custom Column



3. A window appears. To create the custom column:

- Enter the name of the custom column in the Name field. This is a mandatory field.
- Enter the regular expression data in the Validation Pattern field to validate the entered data for the given custom column. For example, the typical e-mail regular expression looks like

```
^[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*@[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*(\.[A-Za-z]{2,})$.
```

This is an optional field. However, if you do not provide the regular expression data, the custom column data will not be validated.

Figure 48: Creating Custom Column Page



**NOTE:** The maximum number of custom columns you can define is 3.

4. Before creating the custom column, the system will show the following warning message to confirm the custom column creation. Click **Yes** to create the custom column or **No** to cancel the custom column creation.

Figure 49: Create Custom Column Confirm Page

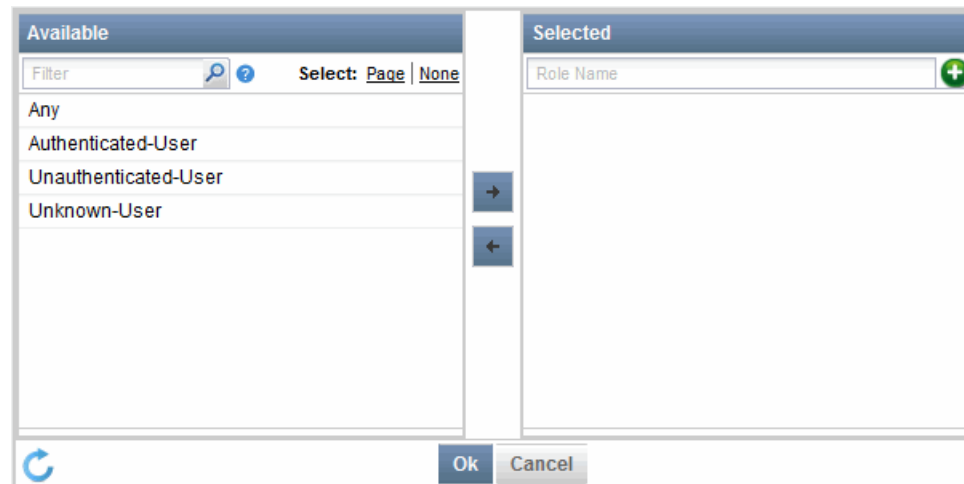
The Infranet Controller (IC) maps users to roles based on the information provided by an authentication server. For example, a user could be mapped to a role based on membership in Active Directory groups.

When a user attempts to access a resource, the SRX Series device passes the username and password to the IC. The IC responds with the role(s) that you are mapped to. The SRX Series device then evaluates the security policies to determine whether the user can access the resource.

To add a role to a user:

1. Click **Source Identity** in the source identity table header. A window appears, as shown in [Figure 50 on page 168](#).

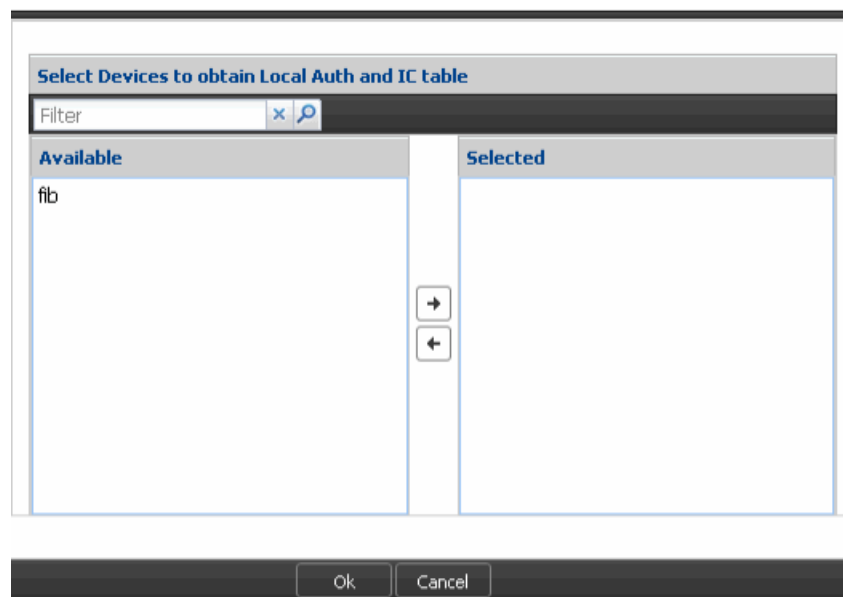
**Figure 50: Source Identity Page**



In addition to the roles provided by IC, the following roles are valid:

- Free text—You can enter a new role name and click Add in the right pane.
  - Any—Default role that matches with any user. The Any role cannot be used in any rule that uses other types of roles. Ensure that the text you enter matches with a role configured in IC.
  - Authenticated-User—User who has an entry in any of the user identification tables (local or ICs). The Authenticated-User role cannot be used in any rule that uses other types of roles. An authenticated user is sometimes referred to as a *known user* in other firewalls.
  - Unauthenticated-User—User with an IP address that does not match the available IP addresses in the user authentication table of the SRX Series device.
  - Unknown-User—Authorization service is unavailable for this user.
2. Click the redo icon to select devices for the selected roles. The following window appears for selecting the devices, as shown in [Figure 51 on page 169](#).

Figure 51: Select Devices Page



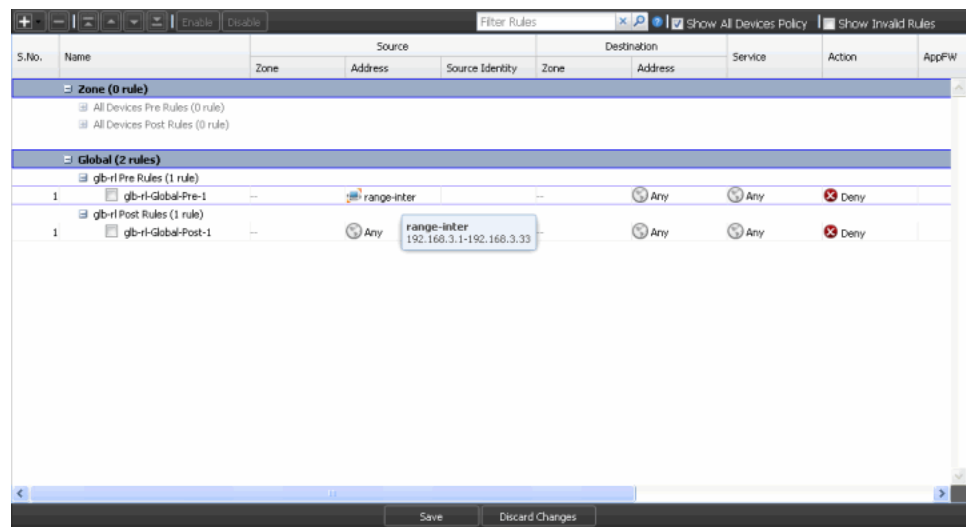
Security Director maintains a list of roles available for a group or for individual devices. You can manually retrieve the available roles from a single SRX Series device or from multiple SRX Series devices.



**NOTE:** Every time you perform a role retrieval, the existing list is overwritten. This prevents deleted roles from persisting.

You can use the available Tooltip view to see information about policy objects. To see the tooltip for an object, you can mouse over the source or destination address object of a rule to see a tooltip containing details about that object. The tooltip displays the address name and other address object details (IP and subnet), as shown in [Figure 52 on page 170](#). For address group, the tooltip shows details regarding its members.

Figure 52: Tooltip Showing Object Information



Tooltips are also available for services. Mouse over a service group to view the group name and other information such as protocol and destination port. For a service group, member details are shown in the tooltip.

You can search for firewall policies in the left pane using the firewall policy names and devices that are used in the firewall policy. You can search rules in the right pane using zones, addresses, description, and services used in the rule.

On the right pane, you can search for rules by using specific search fields, as shown in the [Table 22 on page 170](#)

Table 22: Firewall policy Right Pane Search Options

Rule Column	Search Field	Example Usage	Expected Behavior
Source address name	dcRuleSrcAddressName	dcRuleSrcAddressName:ServerFarm	Searches rules that have serverFarm as the source address
Source address IP	dcRuleSrcIPAddress	dcRuleSrcIPAddress:1.1.1.1	Searches rules that have an address with ip 1.1.1.1 in the source address
Destination address name	dcRuleDstAddressName	dcRuleDstAddressName:ClientMachine	Searches rules that have ClientMachine as the destination address
Destination address IP	dcRuleDstIPAddress	dcRuleDstIPAddress:1.1.1.1	Searches rules that have an address with IP 1.1.1.1 in the destination address
Application name	dcRuleAppName	dcRuleAppName:ftp	Searches rules with application FTP
Application source port	srcPort	srcPort:11243	Searches rules using an application with the source port 11243

Table 22: Firewall policy Right Pane Search Options (*continued*)

Rule Column	Search Field	Example Usage	Expected Behavior
Application destination Port	dstPort	dstPort:22	Searches rules using an application with the destination port 22  To search for destination port range, you must use <i>dstPort: ( 20 AND 65535)</i> . This searches rules using service with destination port range 20-65535.
From Zone	dcRuleFromZone	dcRuleFromZone:trust	Searches rules whose from zone is trust
To Zone	dcRuleToZone	dcRuleToZone:untrust AND dcRuleFromZone:trust	Search rules whose from zone is trust and to zone is untrust



**NOTE:** Any changes you make to both the zone and SRX Series All Devices rule bases are saved or discarded together as a single change list.

Security Director provides advanced search options for the firewall policies. Click the down arrow icon next to the search icon, select **Advanced Search**, and the following dialog appears, as shown in [Figure 53 on page 171](#).

Figure 53: Advanced Search Dialog for Firewall Policies

The Advanced Search dialog box contains the following fields and controls:

- Rule Name:** A text input field.
- Source:** A section containing:
  - Zone:** A text input field.
  - Address:** A text input field.
- Destination:** A section containing:
  - Zone:** A text input field.
  - Address:** A text input field.
- Service:** A text input field.
- Action:** A dropdown menu.
- IPS:** A dropdown menu.
- Description:** A text input field.
- Custom Columns:** A section containing:
  - c1:** A text input field.
- Buttons:** Filter, Reset, and Cancel buttons at the bottom.

You can perform advanced searches for the following fields:

- Rule Name
- Source
  - Zone
  - Address
- Destination
  - Zone
  - Address
- Service
- Action
- IPS
- Description
- Custom column

The following advanced search criteria are available:

- Wildcard search for rule names using an asterisk (\*) is allowed.
- Security Director supports AND and OR operations between search items. The default behavior is OR.
- For rule name search, only the OR operation is allowed, because a policy cannot have multiple rule names.
- For zone search, only the OR operation is allowed. Wildcard search is supported.
- For service and address fields, OR and AND operations are allowed.
- Multiple groups can be grouped using parenthesis. Grouping can be used during filed or keyword searches as well.
- Negate (-) symbol can be used to exclude objects that contain a specific term name.
- The plus (+) operator can be used to specify that the term after the + symbol existing the field value to be filtered along with other searched items.
- Escaping special characters are part of the search syntax. The supported special characters are + - && || ! ( ) { } [ ] ^ " ~ \* ? : \.



**NOTE:** Use the AND operator to find rules that match all values for a given set of fields. Use the OR operator to find rules that match any of the values for a given set of fields.

---

Table 23 on page 173 explains certain specific Security Director search behavior.

Table 23: Specific Security Director Search Behavior

Search Item	Description
IPv4 addresses	If you provide a valid IPv4 address, range, or network in the search field, Security Director finds all addresses that include these IPv4 address, range, or network.
Destination port in service	If you configured a destination port range of a service, Security Director matches ports within this range but this is valid only during field or keyword search.
Keyword or field	If you require to search specific attributes in an object as opposed to global search, you can use keyword or field search.

Table 24 on page 173 shows example search results for different parameters.

Table 24: Examples of Different Advanced Search Parameters

Scenario	Query Parameter	Description
Wildcard search for rule names in both zone and global rules	RuleName:( All* )	Rule names starting with <i>All</i> are filtered.
Wildcard search for a particular rule name pattern	RuleName:(All-Devices-Zone-Pre*)	Returns All Devices Policy Zone Pre rules
	RuleName:(All-Devices-Global-Pre*)	Returns All Devices Policy Global Pre Rules
	RuleName:(All-Devices-Zone-Post*)	Returns All Devices Policy Zone Post Rules
	RuleName:(All-Devices-Global-Post*)	Returns All Devices Policy Global Post Rules
Source zone to destination zone	SrcZone:( polyzone ) AND DstZone:( untrust )	Rules with source zone <i>polyzone</i> and destination zone <i>untrust</i> are filtered.
Source zone and source address to destination zone and destination address	SrcZone:( polyzone ) AND SrcAddress:( any ) AND DstZone:( untrust ) AND DstAddress:( polyaddr )	Rules with source zone <i>polyzone</i> , source address <i>any</i> , destination zone <i>untrust</i> , and destination address <i>polyaddr</i> are filtered.
Source zone and source address to destination zone and destination address along with service	SrcZone:( polyzone ) AND SrcAddress:( polyaddr1 AND polyaddr2 ) AND DstZone:( untrust ) AND DstAddress:( any ) AND Service:( srv1 AND srv2 )	Rules with source zone <i>polyzone</i> , source addresses <i>polyaddr1</i> and <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with Services <i>srv1</i> and <i>srv2</i> , are filtered.
Source zone and source address to destination zone and destination address along with service port range	SrcZone:( polyzone ) AND SrcAddress:( polyaddr1 AND polyaddr2 ) AND DstZone:( untrust ) AND DstAddress:( any ) AND Service:(10 AND 65535)	Rules with source zone <i>polyzone</i> , source addresses <i>polyaddr1</i> and <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with Services having destination port range 10-65535 are filtered.

Table 24: Examples of Different Advanced Search Parameters (*continued*)

Rules with action	SrcZone:( polyzone ) AND SrcAddress:( polyaddr1 polyaddr2 ) AND DstZone:( untrust ) AND DstAddress:( any ) AND Service:( aol apple-ichat ) AND dcRuleAction:( Permit )	Rules with source zone <i>polyzone</i> , source address <i>polyaddr1</i> or <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with service as either <i>aol</i> or <i>apple-ichat</i> , and action <i>Permit</i> , are filtered.
-------------------	--	--



**NOTE:** You can search by giving IPv6 addresses in the source or the destination address field.



**NOTE:** Because you are manually retrieving roles from the SRX Series devices, Security Director might not recognize a valid role on an SRX Series device until you manually retrieve that role.

#### Related Documentation

- [Firewall Policies Overview on page 151](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)
- [Managing Firewall Policies on page 201](#)
- [Publishing Firewall Policies on page 194](#)
- [Unlocking Locked Policies on page 174](#)

## Unlocking Locked Policies

All the locked policies can be viewed in a single page. This page is available for a user having Manage Policy Locks tasks assigned. This page shows all the locks only if the user has Unlock task assigned, other wise user will see only his locks. To view the locked policies:

1. Select **Security Director > Firewall Policy > Manage Policy Locks**.

The Manage Policy Locks page appears showing only those locks that can be managed by the current user. The page contains the following fields:

- Policy name
- User (IP Address)
- Lock acquired time
- Time for lock expiry

Figure 54: Firewall Policy: Manage Policy Locks

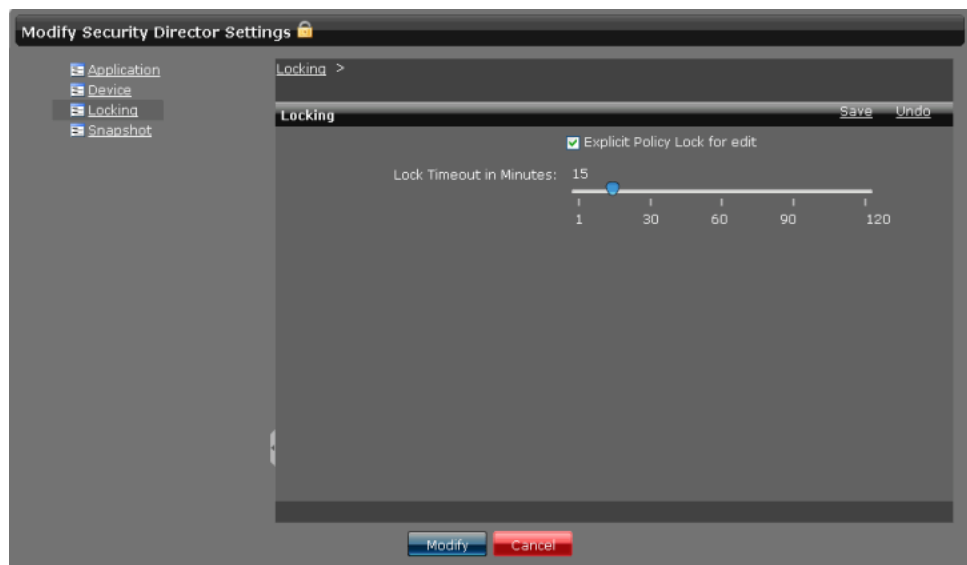
Policy	User	Lock Acquired Time	Lock Expires in
FW_S150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 25 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilp	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	3 Mins 50 Secs

2. Right-click the policy that you want to unlock, and press **Unlock**. You can select policies that are locked by you and unlock them. To unlock your policies, you do not need any administrator privileges. To unlock policies locked by other users, you must have the task **LOCK** assigned to you.

User with administrator privileges can configure the lock settings. To configure the lock settings:

1. Click **Application Switcher**, and go to **Network Application Platform > Administration > Manage Applications**.
2. Right-click the **Security Director** application, and select **Modify Application Settings**. The following page appears, as shown in [Figure 55 on page 175](#).

Figure 55: Modify Security Director Settings



3. Under the Locking option, you can configure the locking timeout value in minutes. The minimum value that you can configure is 2 minutes and the maximum 120 minutes. By default, the timeout value is configured for 5 minutes.
4. By default, the Explicit Policy Lock for edit option is enabled. You can disable this option, if you do not want to lock the policies before editing. When this option is disabled, policies can be edited by any user. The first user gets the preference of saving the changes for a policy. The next save on the same version of a policy results in the user being asked to save policy with new name.



**NOTE:** Acquiring a policy lock or releasing a lock is audit logged. Release locking will show the reason for the release, for example, an explicit release, on save, discard, timeout, or administrator release. Administrator changes of the lock configuration are also audit logged. To see the audit logs, from the Security Director task bar, select Audit Logs.

#### Related Documentation

- [Creating Firewall Policies on page 159](#)
- [Managing Firewall Policies on page 201](#)

## Inline Creation of Objects in Policy

To optimize the creation of policies, Security Director allows you to create new objects for policies you create with the policy editor.

To create objects or address groups for a source address:

1. In the all devices policy page, click on the source address column. [Figure 56 on page 176](#) shows the window that appears showing the available addresses and options for creating the new object. In this address selector window, you can select all addresses listed in the Available column by selecting **Page** and copy them to Selected column. If you want to unselect all, click **None**.

**Figure 56: Inline Address Object Creation in the Source Address Window**

Available		Selected	
Address	Domain	Address	Domain
128.212.104.100/32 (128.212....	Global	Any	SYSTEM
128.212.104.101/32 (128.212....	Global		
128.212.104.102/32 (128.212....	Global		
128.212.104.103/32 (128.212....	Global		
128.212.104.104/32 (128.212....	Global		
128.212.104.105/32 (128.212....	Global		
128.212.104.106/32 (128.212....	Global		
Total: 771		Total: 1	

☐ Host
 ☐ Network
 ☐ Wildcard
 ☐ Variable
 ☐ Range
 ☐ Other

Ok Cancel

You have an option of excluding the source and destination addresses. The selected address list is considered excluded, and the device permits traffic from addresses other than the excluded address.

The following two new radio buttons are available to allow you to include or exclude the source and destination addresses in a firewall rule:

- Include Addresses
- Negate Addresses

The exclude address option is not supported for the address types IPv6, wildcard, unresolved DNS, and any. No more than 10 addresses per rule can be excluded. If more than 10 addresses are excluded, Security Director flags this during the preview or publish.

2. Click the plus sign (+) to create the new address object or address group. By default, the Address radio button is selected

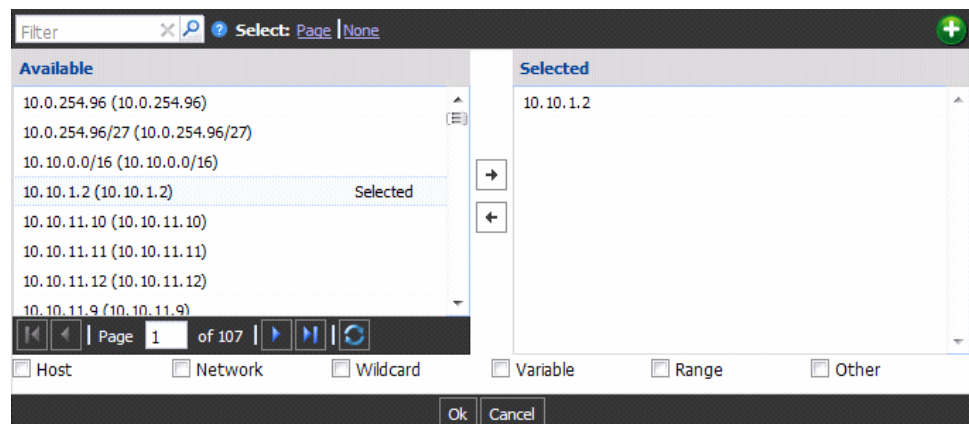
Figure 57 on page 177 shows the page that appears.

**Figure 57: Inline Address Object Create Page**

The Type can be Host, Range, or Network.

3. Click **Create** to finish editing the object. This adds the newly created address object to the selected addresses and returns to the address selector. Click **Cancel** to discard your changes and return to the address selector.

Figure 58: Address Selector Page Showing the New Inline Object

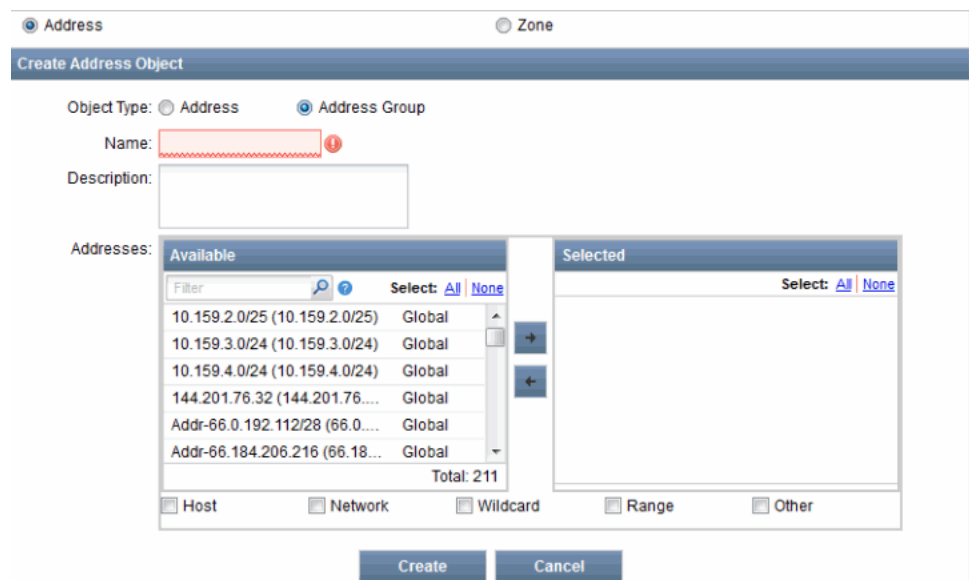


To create address group:

1. Select the Address Group radio button to create the new address group.

Figure 59 on page 178 shows the page that appears.

Figure 59: Inline Address Group Creation



2. Enter the name of an address group in the Name field.
3. In the Addresses field, you can select all addresses available in the Available column or select few addresses to create a new address group.
4. Click **Create** to create the address group. This adds the newly created address objects to the selected addresses and returns to the address selector. Click **Cancel** to discard your changes and return to the address selector.



**NOTE:** Follow the same steps to create objects for the destination address.

To create objects for a service:

1. Click the Service column. Figure 60 on page 179 shows the window that appears, showing the available services. In this service selector window, you can select all services listed in the Available column by selecting **Page** and copy them to Selected column. To unselect all, click **None**.

Figure 60: Inline Service Object Creation in the Service List

Available		Selected	
Service	Domain	Service	Domain
any-tcp-2h (tcp/0-65535)	Global	Any	SYSTEM
any-tcp-6h (tcp/0-65535)	Global		
any-udp-5m (udp/0-65535)	Global		
aol (tcp/5190-5193)	SYSTEM		
apple-ichat (group)	SYSTEM		
apple-ichat-snatmap (udp/0-65535)	SYSTEM		
bgp (tcp/179)	SYSTEM		
BGP-6h (tcp/179-179)	Global		
Total: 254		Total: 1	

2. Click the plus sign (+) to create objects for the service.

Figure 61: Inline Service Object Creation Page

**Create Service**

Name: servicecreate

Description: service create test

Type: TCP

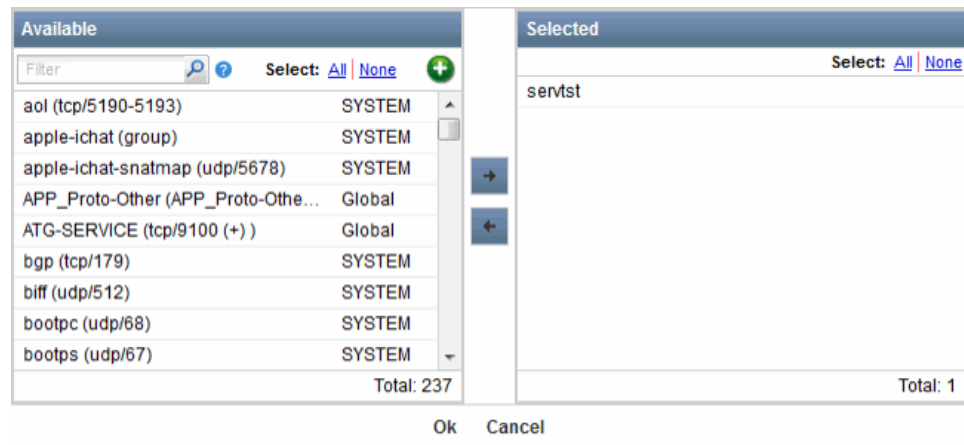
Destination Port:

Create Cancel

Type can be TCP or UDP. Any advanced options must be edited in the Object Builder workspace.

3. Click **Create** to finish editing the object. This adds the newly created object to the selected service and returns to the service selector.

Figure 62: Service Selector Page Showing the New Object



- Click **Cancel** to discard your changes and return to the service selector.



**NOTE:** The policy publish state is changes to Republish required, If an address or service object in the global domain, referred by a policy in another domain changes. This occurs even though the changed address or service objects are in different domain other than the policy domain.

- Related Documentation**
- [Firewall Policies Overview on page 151](#)
  - [Managing Firewall Policies on page 201](#)

## Adding Rules to a Firewall Policy

When a new firewall policy is created, by default the policy displays links to create rules for the policy. If you have created a group firewall policy, you will see the Create Pre Rule and Create Post Rule link in the right pane. If you have any cut or copied rules or rule groups, you will also have Paste Rules to paste the rules or rule groups. The pasting options are available only for the predefined rule groups. If you have created a device firewall policy, you will see the Create Device Rule link.

To add rules to a firewall policy:

- Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
- From the left pane, click the security policy you want to add rules to.  
The existing rules of the security policy are displayed in the right pane.
- Click the **+** icon to add rules, and select the type of the rule you want to add.  
A new rule is added in the bottom-most row of the Pre Rule, Post Rule, or Device Rule section, depending on the type of rule you have added. The newly added rule blinks

a different color for a few seconds. The behavior is same if you add a new rule before or after a rule, clone a rule, or paste a rule.

The rule is assigned a serial number based on the number of rules already added to the policy. By default, the Source zone is set to trust, Destination zone is set to untrust, and the Action is set to Deny. The Source address, Destination address, and Service is set to Any. You can now modify the default settings to the settings that you want for this security policy.

4. Click the **Hit Count** field to view the hit count level of each rule.
5. Click the **Name** field in the rule and change the name of the rule.
6. Click the **Source Zone** field in the rule and select the appropriate zone from the list of zones.

The zones that appear in the list are dependent on the type of security policy you have chosen to add rules to. If you are adding a rule for a group policy, all the zones present on all devices are available for selection. Select the correct zone for the device in the group policy.

For the devices running Junos OS Release 12.1X47, global firewall policy rules are enhanced to specify one or more zones for the fromZone and toZone fields in match criteria. Click the zone column to select zones available from the currently associated devices, and the zone sets.

During the policy creation phase, no validation is performed if you configure multizone global policy rule on a policy associated with a device running releases of Junos OS earlier than Junos OS Release 12.1X47. This is schema driven. During publishing of the policy, the multizone global policy is validated to check if Security Director is applied with Junos OS Release 12.1X47 schema. If the right schema is applied publish is successful; otherwise, publish fails on those devices.

7. Click the **Source Address** field in the rule.

The address selector appears. The dynamic addresses created in the Security Intelligence workspace are listed in the address selector. You can use the dynamic address as the source address.

8. From the Available column, select the addresses you want to associate the rule.
9. Click the right arrow in the address selector.

The selected addresses are now moved to the Selected column.

10. Click **OK**.

11. Click the **Destination Zone** field in the rule and select the appropriate zone from the list of zones.

12. Click the **Destination Address** field in the rule.

The address selector appears.

13. From the Available column, select the addresses you want to associate the rule.
14. Click the right arrow in the address selector.

The selected addresses are now moved to the Selected column.

15. Click **OK**.

16. Click the **Service** field in the rule.

The service selector appears.

17. Select the services you want to associate the rule to, from the Available column. For high-end SRX Series devices, instead of 128 services, 3072 applications per policy are supported.

18. Click the right arrow in the service selector.

The selected services are now moved to the Selected column.

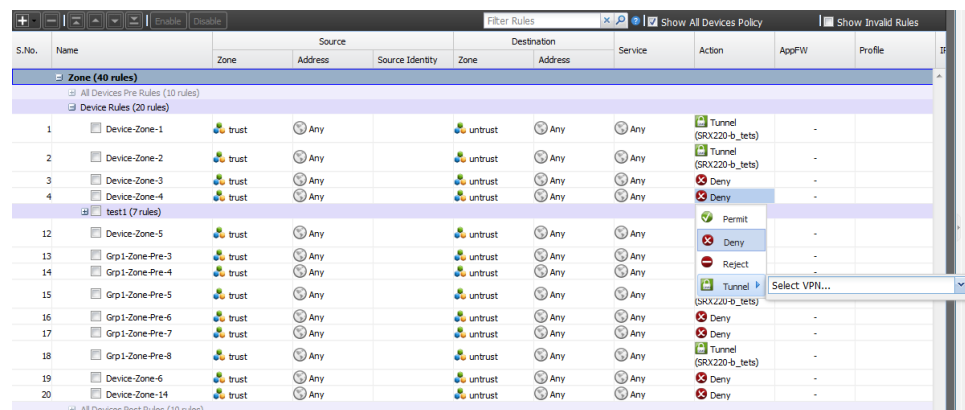
19. Click **OK**.

20. Click the **Action** field in the rule and select the appropriate action from the drop-down list of actions.

You can select Permit, Deny, Reject, or Tunnel as the actions.

If Tunnel action is selected, a list with all the policy-based VPNs that are created is provided, as shown in [Figure 63 on page 182](#).

**Figure 63: Tunnel Option for Device Rule**



From Security Director, you can select the IPsec VPNs that are configured in a device directly in a firewall rule in addition to the ones created and managed from Security Director. Publish will fail if this VPN is deleted from a device.

21. Click the **AppFW** field in the rule and select the appropriate AppFirewall settings from the AppFW Configuration window.



**NOTE:** You can modify the AppFW field only if the Action field in the firewall policy rule action is set to Permit or Tunnel.

22. Click the **Profile** field in the rule and select the appropriate profile.

You can either select a default profile or a custom profile, or you can inherit a policy profile from another policy. Under the Select Another Profile option, you can select the user firewall for the firewall authentication. If you are selecting a custom profile, you can customize the options in the policy profile. For Custom Settings under the

Advanced Settings tab, you can enable TCP session options on a per-policy basis by clicking the **Enable TCP-SYN Check** and **Enable TCP Sequence Check** options, as shown in Figure 64 on page 183.

Figure 64: TCP-Session Options

Profile Type: ☐ None  
☐ Inherit Profile From Policy  
☐ Select Another Profile  
☒ Custom

**Custom Settings**

Template:

**Logging** **Authentication** **Advanced Settings**

Datacenter SRX Acceleration: ☐ Services Offload

Destination Address Translation:

Redirect:

**TCP-Session Options**

☐ TCP-SYN Check

☐ TCP Sequence Check

Ok Cancel

You can click **Show Invalid Rules** check box to view the invalid rules in any policy. You can either first validate the policy and apply the filter to see the invalid rules, or the filter can be directly applied to the policies which are saved as drafts with errors.



**NOTE:**

- Update is committed only if these TCP session options are disabled globally. Otherwise, update fails if enabled globally.
- If the update fails for logical systems, you must disable TCP session options for logical systems and not in the root devices.
- If you are making any changes at the root device level or at the policy level, the same changes are captured in the audit trail.
- When you are importing a device configuration, TCP session options are also imported if they are enabled.
- In case of policy export, you can find these TCP session options under Rule Options column.
- TCP session options are retained in case of version roll back and when you take the firewall policy snapshot.

23. To assign a scheduler and UTM policy for a rule, click **Rule Options**. Select the required scheduler from the Scheduler field, and the UTM policy from the UTM Policy field.

To assign the scheduler and UTM policy, click **OK**.

You can select a UTM policy profile object for a rule only when the configured action is Permit.

For rules with an expired scheduler, a warning message appears during the Publish workflow.

24. Click the **IPS** field in the rule and select options wither IPS ON or IPS OFF depending on the firewall rule action and the IPS mode configured in the firewall policy.
25. Click the **Security Intelligence** column and select the listed profile.
26. Click the **Description** field and enter a description for the security policy.
27. Click **Save**.

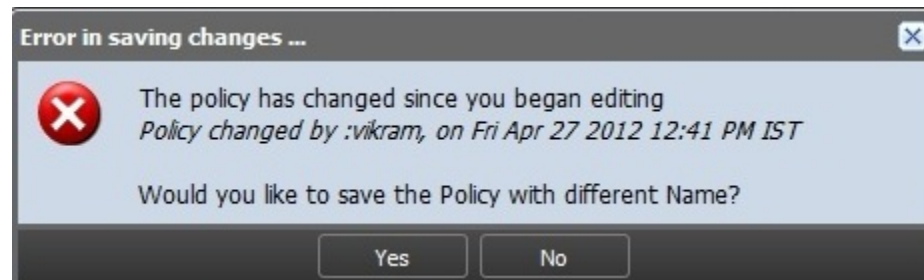


**NOTE:** You should click **Save** to save any changes you have made to the firewall policy. While in the process of making changes to the firewall policy, If you click any of the tasks in the task ribbon before saving the firewall policy changes, all changes you have made will be lost. If you click anywhere inside the Policy Tabular view, a window appears, displaying a message asking if you want to confirm your changes.



**NOTE:** If a previous user has added new rules to the policy and saved the changes, when you attempt to save your changes, the error message shown in [Figure 65 on page 184](#) appears.

Figure 65: Concurrent Policy Edit Error Message



The error message shows the name of the user who made the previous changes and the time they were saved. The changes made by the first user take precedence over any later changes. You will be given an option to save the policy with a different name. Click **Yes** to save the policy with different name. Only saved rules are published to the policy.

#### Related Documentation

- [Firewall Policies Overview on page 151](#)
- [Creating Firewall Policies on page 159](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)
- [Managing Firewall Policies on page 201](#)

- [Publishing Firewall Policies on page 194](#)

## Ordering the Rules in a Firewall Policy

To reorder the rules in a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Select the firewall policy whose rules you want to reorder.

The rules of the firewall policy are displayed in the right pane.

3. Select a rule that you want to reorder and click the appropriate icon on the top of the right pane.

Icon Name	Description
Move Rule Up	Moves the rule one level up in the hierarchy.
Move Rule Down	Moves the rule one level down in the hierarchy.
Move Rule to Top	Moves the rule to the top of the hierarchy.
Move Rule to Bottom	Moves the rule to the bottom of the hierarchy.

The rule is now positioned accordingly. When the policy is provisioned, the rules are provisioned to the devices in the order you have specified.

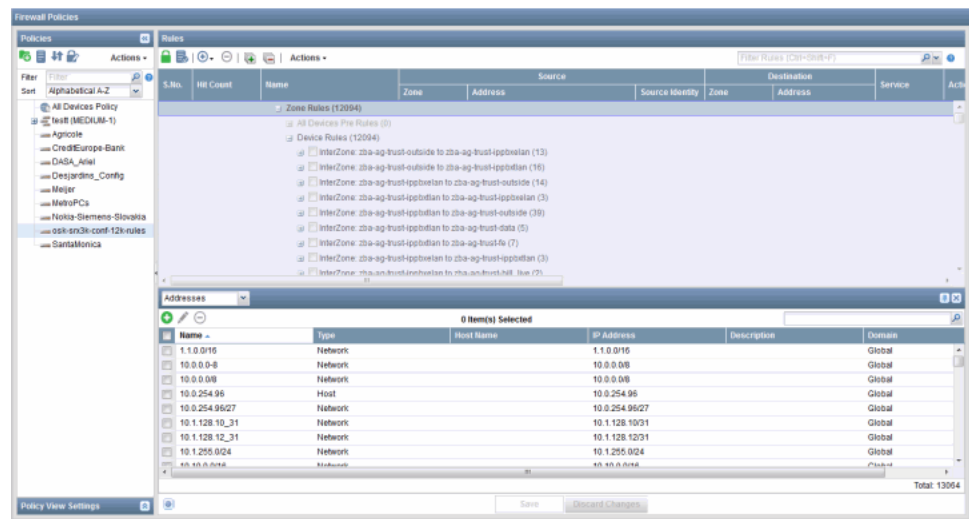
You can reorder the rules across Pre Rule and Post Rule of a group policy. For example, if you move the last rule in the Pre Rule one level down, it is moved to the Post Rule. Similarly, if you move the first rule in the Post Rule one level up, it is moved to the Pre Rule.



**NOTE:** Movement of Pre and Post rules across zone and global is not permitted.

The address and service objects can be created, managed, dragged and dropped to the required rules from the firewall policy landing page. The objects are listed in the policy landing page, as shown in [Figure 66 on page 186](#).

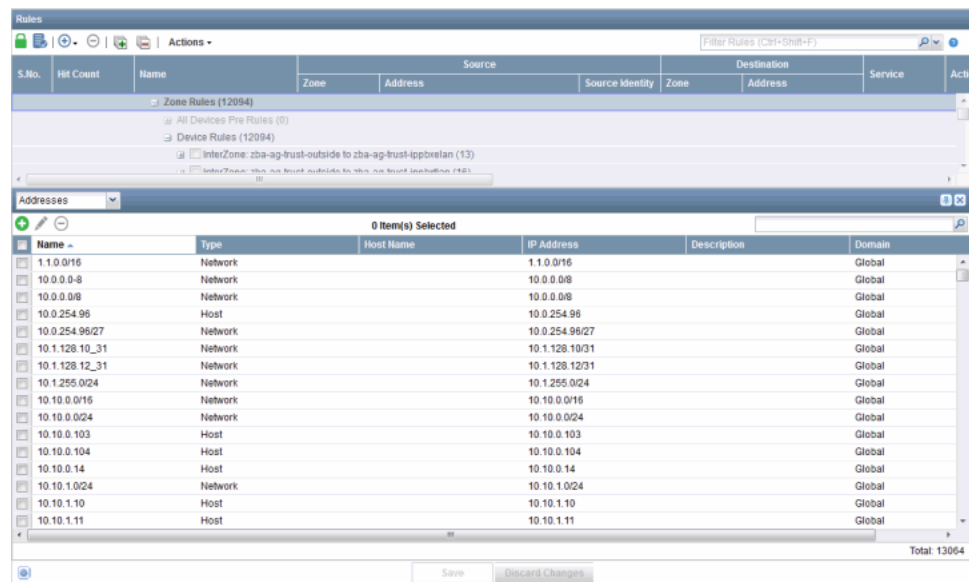
Figure 66: Firewall Policy Landing Page



You can select address or service objects from the drop-down list. To create a new address or service object, click the plus sign (+). To know more about creating address and services objects, see [“Creating Addresses” on page 124](#) and [“Creating Services” on page 108](#).

You can modify an object by clicking the pencil icon and delete objects by clicking the minus sign (-). You can search for any object by its name and IP address in the search field available in the top right corner, as shown in [Figure 67 on page 186](#).

Figure 67: Firewall Policy-Drag and Drop Objects Window



You can drag more than one object and drop on the respective columns in the policy tabular view. Security Director ensure that objects are dropped in the supported columns and it does not permit to drop under any other columns. The drag and drop of objects is

supported on the Source Address, Destination Address, and Service columns. Before dropping any object to the policy rules, you must first lock the respective policy. A single address can be dragged and dropped from source address field to destination address field of same rule or across rules. A single service also dragged and dropped across rules. In the firewall policy landing page, you can reorder the rules by dragging and dropping.

You can drag and drop the objects across the rules. If an object already exists for a rule and you drop a new object, the previous object is overwritten by the new object. The new object is copied to the rule.

**Related  
Documentation**

- [Firewall Policies Overview on page 151](#)
- [Creating Firewall Policies on page 159](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Managing Firewall Policies on page 201](#)
- [Publishing Firewall Policies on page 194](#)

## Policy Priority Precedence Setting

To change the priorities and precedences of different policies simultaneously:

1. Select **Security Director > Firewall Policy**.

In the firewall policies page, select **Prioritize Policies** icon from the Policies pane

The Priority and Precedence page appears with all the group policy names, as shown in [Figure 68 on page 188](#). The page contains the following fields:

- Group Policy Name—Name of the group policies.
- Description—Description of the policy.
- Priority—Priority of the group policy (Low, Medium, or High).

Figure 68: Policy: Priority And Precedence Page

Group Policy Name	Description	Priority
testLSYS		Medium-1

2. Select any group policy and right-click the selected policy. The following options shown in [Table 25 on page 189](#) are provided to move the priority up or down or to change the precedence and priority simultaneously.

Table 25: Priority and Precedence for Firewall Policies

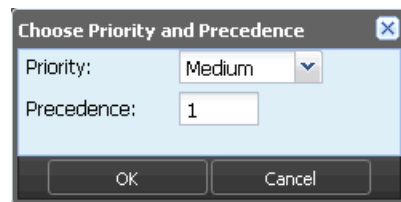
Options	Description
Move Up	<p>You can choose one or more policies and select the Move Up in the right-click menu. This option is also available in the toolbar. All the selected policies are moved up by one level. For example:</p> <ul style="list-style-type: none"> <li>Move up a medium-priority policy with a precedence value 1. If a high-priority policy already exists, the medium-priority policy is moved just below the high-priority policy or moved to a high priority.</li> <li>Move up a medium-priority policy with a precedence value 2. If a medium-priority policy with a precedence value 1 already exists, a medium-priority with precedence value 2 is moved up to precedence value 1 and an already existing medium-priority with a precedence value 1 is changed to precedence value 2.</li> <li>Move up a low-priority policy with precedence value 1. The priority of the policy is changed to Medium with precedence value 1, only if there are no medium-priority policies, otherwise it would have the lowest precedence (highest number) in the medium- priority. If you move the policy up again, the priority of the policy is changed to High with precedence value 1.</li> </ul> <p>In all the Move Up operations, the remaining policies in the same priority are pushed up by one level.</p>
Move Down	<p>You can choose a single policy or more than one policy by selecting the Move Down in the right-click menu. This option is also available in the toolbar. All the selected policies are shifted by one level down individually. For example:</p> <ul style="list-style-type: none"> <li>Move down medium-priority with precedence 1. If a medium-priority policy with precedence 2 exists, the precedence of the moved down policy becomes precedence 2, and the original precedence 2 policy is now precedence 1. If there are no other medium-priority policies, the move down moves the policy to low-priority and precedence 1.</li> </ul>
Assign	<p>You can choose this option to set the priority and precedence at the same time. If you choose the same priorities for the policies, set the precedence value between 1 to the number of policies of the same priority. If the priorities are different, set the precedence value between 1 to number of policies in the priority. If highest precedence medium-priority policy is moved down, it becomes priority low and precedence 1.</p>



**NOTE:** If multiple policies are selected, all the policies are moved one-by-one to the given priority and precedence slot sequentially.

3. Click **Assign** to provide precedence value.

Figure 69: Setting Priority And Precedence Value Page



4. Click **Save** to save all the priority and precedence changes. These changes are saved in the database, and page is shown with all the annotations of the changes. If you do not want to save, click **Cancel** to go back to the firewall policies page.

- Related Documentation**
- [Multiple Group Policy Membership Overview on page 155](#)
  - [Managing Firewall Policies on page 201](#)

## Tracking the Utility Rate of Security Firewall Policies

The utility rate of firewall policies can be tracked by analyzing the number of hits they receive from Security Director. You can also determine the policy rules that are currently used on the device, the hit levels of the policy rules that are hit by the traffic, and the usage frequency of the policy rules. Using hit data, you can identify the important and less important policy rules, and take further action to optimize the policy rules by deleting the unwanted policy rules.

The system job probes all devices managed by Security Director for the hits. This system job starts automatically when Security Director is deployed, both during the upgrade and during a fresh installation. Currently, the system job runs daily at 2 AM and collects the hit levels for all the devices present in Security Director. You can view the approximate date at which the last hit occurred for the rule. Also, you can view the number of hits for each device for a particular rule, and the current or cumulative hits for the rule. The level for each rule is calculated based on the percentage of total hits in a policy. You can filter the rules in a policy based on the hit level. If you want to calculate the hits trend of all the rules over a period of time, you can do so by resetting the hits to zero. You can also export the hits details when you export a firewall policy.

To view the policy rule hits:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears, as shown in [Figure 70 on page 190](#).

**Figure 70: Firewall Policy with Rule Hits**

The screenshot displays the 'Firewall Policies' management interface. On the left, a sidebar shows a tree view with 'All Devices Policy' selected, displaying a hit count of 10,207,982,19. The main area is titled 'Rules' and contains a table with columns: S.No., Hits, Name, Zone, Source (Address, Source Identity), Destination (Zone, Address), and Service. The table is filtered to show 'Zone Rules (10)'. Under this filter, there are sub-sections for 'All Devices Pre Rules (1)', 'Device Rules (14)', 'IntraZone: untrust (1 - 8)', 'InterZone: trust to untrust (9 - 14)', and 'All Devices Post Rules (1)'. A 'Global (1)' section is also visible. The first rule listed is 'p1' with 7,62K hits. The interface includes a 'Filter Rules (ctrl+shift+F)' search bar, a 'Policy View Settings' button, and 'Save' and 'Discard Changes' buttons at the bottom.

S.No.	Hits	Name	Zone	Source	Destination	Service
<b>Zone Rules (10)</b>						
All Devices Pre Rules (1)						
Device Rules (14)						
IntraZone: untrust (1 - 8)						
InterZone: trust to untrust (9 - 14)						
All Devices Post Rules (1)						
<b>Global (1)</b>						
Device Rules (1)						
1	7,62K	p1		Any	Any	ftp, ping, telnet, top-any, More -

- On the right pane, you can view the number of hits in the Hits column.

For the group policy, the hit value is the total number of hits for that rule across all the assigned devices. For the device policy, the hit value is only for that device and the corresponding rule.




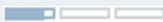
The hit values are shown with the following letters at the end of each value:

- K—1,000 hits
- M—1,000,000 hits
- G—1,000,000,000 hits
- T—1,000,000,000,000 hits

For example, if the hit value is 159K, it means 159 thousand hits. If the hit value is 112, it means only 112 hits.

The hit levels are calculated based on the total hits across all the policy rules, as shown in [Table 26 on page 191](#).

**Table 26: Policy Rule Hit Level**

Hits Level	Display	Description
Zero		Zero hits
High		70% of the total hit range for the policy.
Medium		30-70% of the total hit range for the policy.
Low		30% of the total hit range for the policy.

You can calculate the percentage of hit range using the following formulas:

Range = Maximum hits – Minimum hits(maximum or minimum among the rules in the policy)

Percentage = ((Rule hits – Minimum hits )/range) \* 100

You can click the hit level of each rule to view more details of the hits, as shown in [Figure 71 on page 192](#).

Figure 71: Firewall Policy Hit Levels

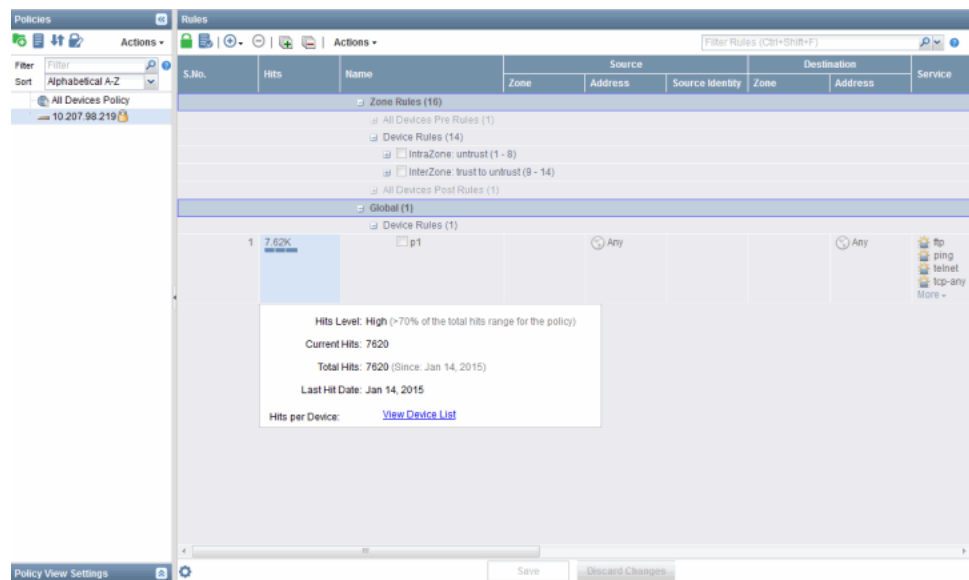


Table 27 on page 192 describes different parameters displayed in the hit view window.

Table 27: Hits Detail View

Hits Parameter	Description
Hit Level	Shows high, medium, or low.  <b>NOTE:</b> For all the rules with a zero hit, the hit level is not calculated. It is shown as Zero.
Current Hits	Number of hits of the rule from the last reset (you can reset the current hit level to zero).  <b>NOTE:</b> <ul style="list-style-type: none"> <li>The reset action resets the current hit to zero; however, the total hits is not changed.</li> <li>The device reboot will not reset the hits in Security Director. Any new hit after a restart is identified and shown in the GUI along with the previous hit.</li> </ul>
Total Hits	Cumulative hits of a rule from the day Security Director started collecting the hits.
Last Hit Date	Approximate date when the traffic last hit the rule on a device.
Hits per Device	The total number of hits shown is the total hits across all devices. Click <b>View Device List</b> to view the hits for each device.

You can view the hits for each device assigned to the current firewall policy. To view the hits, click **View Device List** to display the device level hits, as shown in Figure 72 on page 193.

Figure 72: Hits Per Device

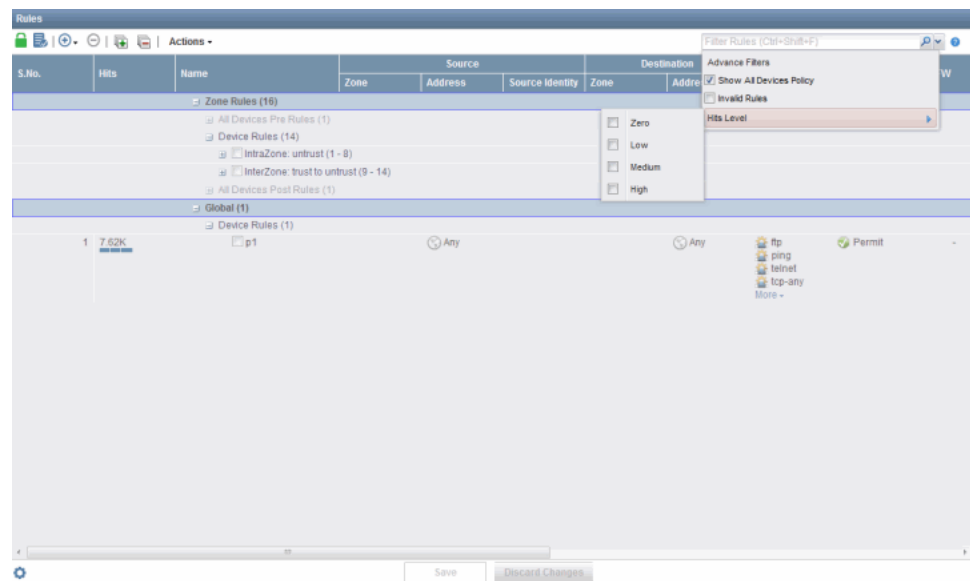
Hits per Device			
Filter by device name <input type="text"/>			
Device	Current Hits	Total Hits	
10.207.98.219	7620	7620	
			Total: 1
OK			

This view shows the number of hits for each device. You can search for any particular device from the search field. If a device is unassigned in the firewall policy, the hit value is not shown for that device.

You can filter the policy rules based on the hit levels. To filter the rules based on the hit levels:

1. On the right pane, click the down arrow icon next to the filter, or click a search box.
2. Move the mouse over the Hit Level option, and select the required hit level check box, as shown in [Figure 73 on page 193](#).

Figure 73: Hit Level Filter



3. Rules with the selected hit level are filtered and shown.

**Related Documentation**

- [Firewall Policies Overview on page 151](#)
- [Creating Firewall Policies on page 159](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Managing Firewall Policies on page 201](#)
- [Publishing Firewall Policies on page 194](#)

---

## Publishing Firewall Policies

When you publish firewall rules, 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, with prerules in the High priority group publishing first, before prerules in the Medium and Low priority groups. Within the same priority group, the prerules of policies with lower precedence values are published before the prerules of policies with higher precedence values. Device rules are published after all group prerules have been published. Finally, the Group postrules are published last in the process. The postrules are published in the reverse order of the prerules.

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 policies do not need to be republished in order for their changes in priority or precedence to take effect for the policies that are implicitly changed by the explicit changes to the republished policy.

To publish a firewall policy:

1. Select the firewall policy that you want to publish and click **Publish Policy** icon from the Policies pane. You can also right-click the policy and select Publish Policy.

The Services page appears with all the firewall policies. It also displays the publish states of the firewall policies.

2. Select the check box next to the firewall policy that you want to publish.



**NOTE:** You can search for a specific device on which the policy is published by entering the search criteria in the search field, in the top-right corner of the Services page. You can search the devices by their name, IP address, and device tags.

---



**NOTE:** If the firewall policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices to view all devices on which the firewall policy is published.

3. You can publish the IPS policies along with the firewall policies by selecting the Include IPS Policy check box. By default, this check box is selected.

If the Include IPS Policy check box is selected, two jobs are created after you click the Publish button. The first job is to publish the selected firewall policies. Once the firewall policy publish is successful, the IPS policy publish job is invoked.

If the Include IPS Policy check box is not selected, only the selected firewall policies are published.



**NOTE:** Firewall policy publish and IPS policy publish are mutually exclusive. The firewall policy publish job focuses only on firewall policy-related configuration, and IPS policy publish job focuses only on the IPS policy-related configuration.

4. Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later, as shown in [Figure 74 on page 195](#).

**Figure 74: Policy Publish Page**

Name	Publish State	Description	Priority	Precedence
All Devices Policy	Not Published	Predefined Policy for all devices	-	-
gdb-t	Not Published		Medium	1
gdb-t-zn	Not Published		Medium	2

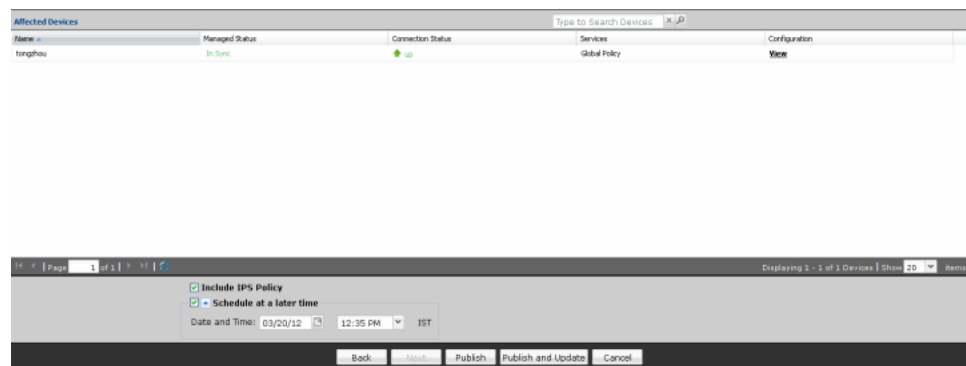
☒ Include IPS Policy  
☒ Schedule at a later time  
 Date and Time: 04/16/12 1:29 PM IST

Back Cancel Publish Publish and Update Cancel

5. Click **Next**.

The Affected Devices page displays the devices on which the policies will be published as shown in [Figure 75 on page 196](#).

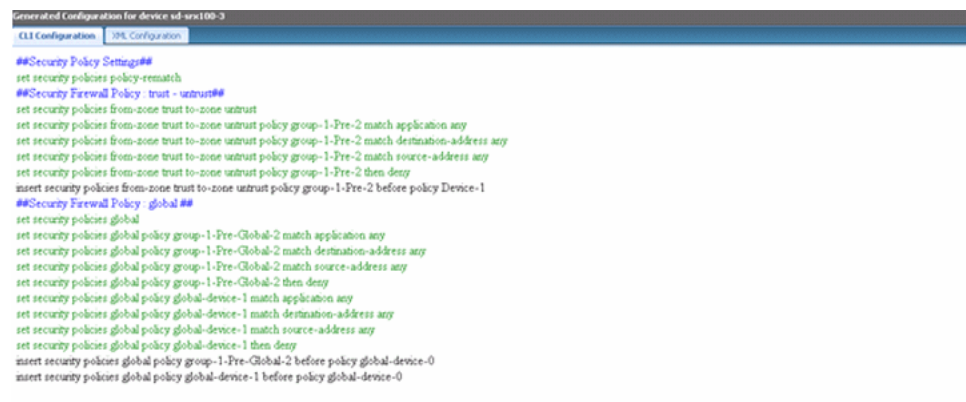
Figure 75: Devices on Which the Policies Will Be Published



- If you want to preview the configuration changes that will be pushed to the device, click **View** in the **Configuration** column corresponding to the device. A Configuration Preview progress bar is shown while the configuration pushed to the device is generated.

The CLI Configuration tab appears by default. You can view the configuration details in the CLI format as shown in [Figure 76 on page 196](#).

Figure 76: Policy Publish-CLI Configuration



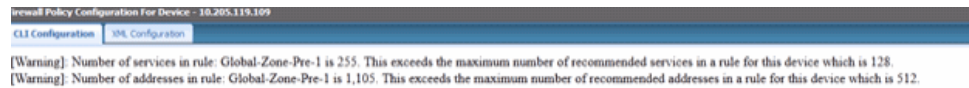
If the device does not support global policies, the rules are truncated with a warning message. A device will not support global policies for the following reasons:

- The device is running a Junos OS version earlier than 11.2.
- Global policy is supported only on the global address book. If the device is configured with a zone-based address book, Security Director will not publish a global policy for that device.

SRX Series devices have scaling capacity limitations for networking services. These capacities vary with the “platform” and Junos OS version. Security Director validates these limitations during the publish or preview of the policies and provides warning messages.

Security Director validates only the published service capacities. These validations are not applicable for the designed services that are still not published. If a particular capacity is exceeded, a warning message appears, as shown in [Figure 77 on page 197](#).

Figure 77: Device Validation Warning Message



For logical systems that have an assigned security profile, including the root logical system, Security Director validates the resource usage against the maximum and reserved quota configured in the respective profile.

When IDP is assigned to a security profile and that profile is assigned to multiple logical systems, Security Director overwrites the IDP policy with the new name and this effects other logical systems as well. This occurs when you import any logical system and update again. You must use separate security profiles, if you do not want to share the same IPS policy across all logical systems instances.

If you do not specify any resource limits in logical systems security profile, Security Director shows the following warning messages:

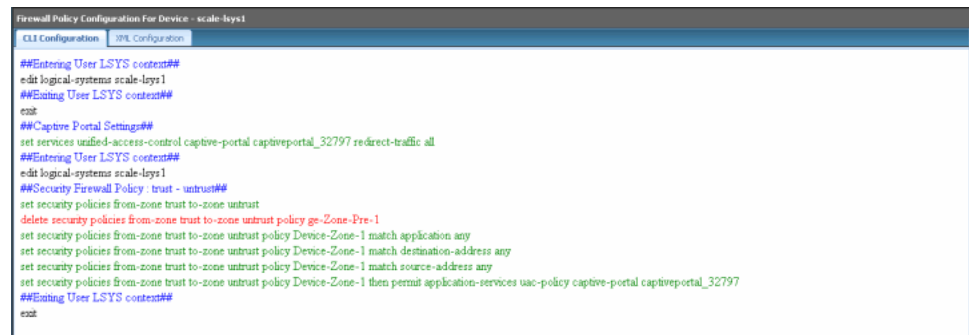
[Warning]: Reserved quota is not specified in the security-profile for nat-destination-pool

[Warning]: Reserved quota is not specified in the security-profile for nat-destination-rule

[Warning]: Reserved quota is not specified in the security-profile for policy

If a logical system is assigned to services, you can publish those services to the logical system. You can view the configuration details in CLI format, as shown in [Figure 78 on page 197](#).

Figure 78: Policy Publish-LSYS Device CLI Configuration



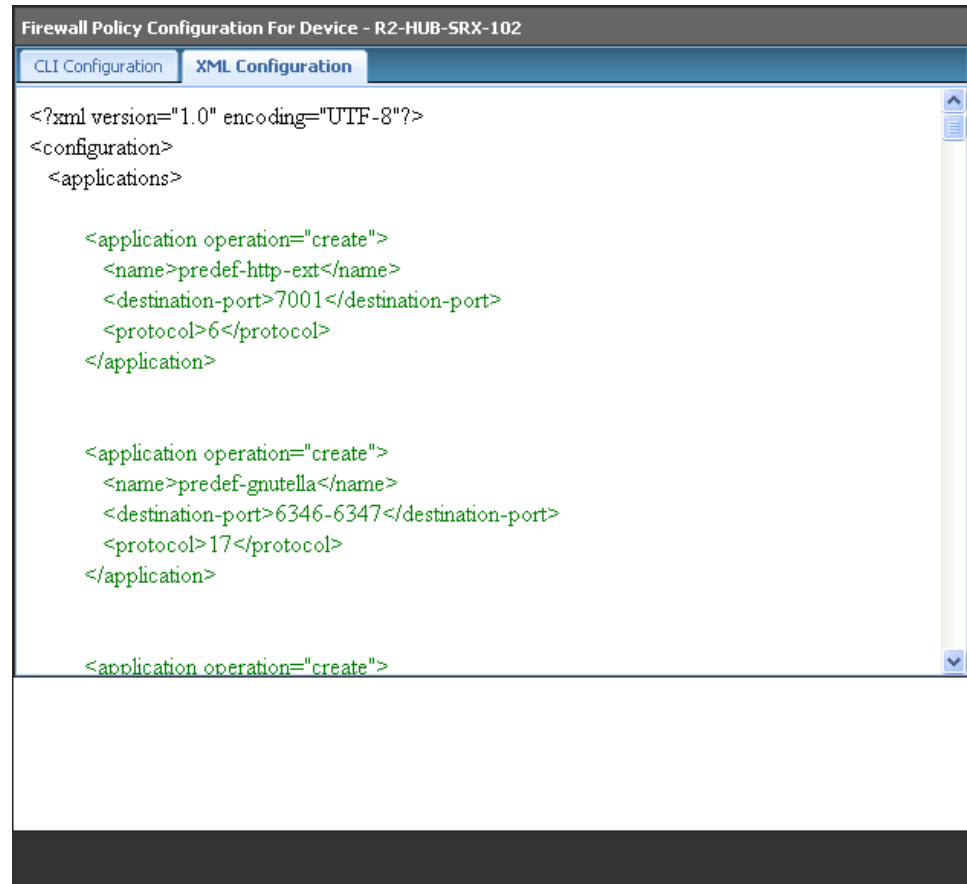
**NOTE:** Captive portal setting can be configured only at the root logical system and referenced only in the user logical system.



**NOTE:** Configuration updates to the root logical systems are automatically done as part of the user logical system update. For such objects, the LSYS name is appended to the object names to differentiate across logical systems.

7. View the XML format of the configuration by clicking the **XML Configuration** tab, as shown in [Figure 79 on page 198](#).

**Figure 79: Policy Publish-XML Configuration**



8. Click **Back**.
9. Click **Publish** if you want only to publish the configuration.  
A new job is created, and the job ID appears in the Job Information dialog box.
10. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The firewall policy is now moved into the Published state if the configuration is published to all devices involved in the policy. If the configuration is not published to all devices involved in the firewall policy, the firewall policy is placed in the Partially Published state. If a firewall policy is created but not published, the firewall policy is placed in the Unpublished state. If any modifications are made to firewall policy configuration after it is published, the firewall policy is placed in the Republish Required state. You can view the states of the firewall policy by hovering over them. When an address object in the Global domain referenced by a policy in the D1 domain changes, the state of the policy is changed to Republish Required. This occurs though the changes are in the address object, which is in the other domain, and is not same as the policy domain. This applies to all the objects referenced by all the services.

A new job is created and the job ID appears in the Job Information dialog box.

11. Click the job ID to view more information about the job created. This action directs you to the Job Management work space.

If you get an error message during the publish or if the firewall policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.

In the Job Details window, use the available filter box to search for any device by filter name, tag name, or IP address. Filtering works only for currently available devices. Search with the first character of the tag name to search by tag name. If you search with any middle characters, the search fails.

During publish and update, the disabled rules and objects are not deleted. Disabled rules are updated as inactive configuration. This is an optional step. You can choose to push the disabled rules to a device by selecting the **Update disabled rules to device** option in the Security Director application setting, under Platform. By default, the Update disabled rules to device option is disabled. For the pushed disabled rules to work after the upgrade, Security Director must import the policy again and the application firewall signature must be downloaded prior to the import.

If you are having a disabled rules on the device, as shown in the following example:

```
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
destination-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
application any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 then
deny
deactivate security policies from-zone untrust to-zone trust policy Device-Zone-5
```

When you import this rules, Security Director sets the state as disabled. If a particular node in the CLI is deactivated, that node is not imported into the Security Director.

If you import a rule, as shown in the following example, Security Director will not set the application service.

```
set security policies from-zone trust to-zone untrust policy Device-Zone-2
description "Rule With Infranet All Traffic Auth"
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
source-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
destination-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
application any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
permit application-services idp
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
permit application-services uac-policy captive-portal captiveportal_65573
deactivate security policies from-zone trust to-zone untrust policy Device-Zone-2
then permit application-services
```

Security Director does not support inactive nodes and the inactive rules. If the objects in the rule are not defined, Security Director provides a warning message, at the time of import, listing the objects that are not defined.



---

**NOTE:**

- You can also publish a firewall policy by right-clicking the firewall policy in the Policy Tabular view and selecting Publish Policy. You are redirected to the Affected Devices page.
  - You cannot publish a global firewall policy if you have not added rules to the all devices policy.
  - During preview, the global rules shown under the comment Security Firewall Policy > Global, if global rules are supported. Otherwise, a warning message is shown.
  - If you have configured AppFW and IPS for a firewall policy and the device you are using has the IPS license installed, when you publish and update the device with the firewall policy configuration, IPS and AppFW and IPS-related configuration will also be pushed to the device.
  - When you publish a firewall policy that has a custom object associated to it, Security Director generates the custom object-related commands to be updated on the device. The commands for custom objects are generated irrespective of whether the firewall policy is already published or updated. If the custom object is associated with the firewall policy at the time of update, these commands are pushed to the device. Security Director pushes these commands to the device even though these commands may have been pushed to the device in an earlier update.
  - You cannot publish a group policy, if you do not have permission for all the assigned devices. Also publish is not permitted if one or more devices are labeled by another Junos Space user.
  - The publish fails if you have two addresses in a rule with a same name, one from the Global domain and the other from the child domain.
  - You can publish or update the group policy of the global domain from another domain. In this case, policy is published or updated to only those devices which are part of the another domain. However, if you publish or update the group policy in the global domain, the policy is published or updated to all the devices including the devices from the another domain.
  - If a global firewall policy rule containing multiple zones is published to a device that is running a Junos OS release earlier than Junos OS Release 12.1X47, publish fails with an error message. This is a schema driven and you must configure the correct schema for the publishing to be successful. Security Director does check the device version during the publish.
- 

**Related Documentation**

- [Firewall Policies Overview on page 151](#)
- [Creating Firewall Policies on page 159](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)

- [Managing Firewall Policies on page 201](#)

## Managing Firewall Policies

---

You can modify, delete, clone, or export the security policies that are listed on the Manage Policies page.

To open the Manage Policies page:

- Select **Security Director > Firewall Policy**.

The Policy Tabular view appears. You must lock the policy before editing.

You can perform the following tasks in the Manage Policies space:

1. [Modifying Firewall Policies on page 202](#)
2. [Comparing Firewall Policies on page 203](#)
3. [Deleting Firewall Policies on page 205](#)
4. [Adding Rules to a Firewall Policy on page 206](#)
5. [Cloning Firewall Policies on page 206](#)
6. [Promoting a Firewall Policy on page 207](#)
7. [Exporting a Firewall Policy on page 207](#)
8. [Policy Versioning on page 208](#)
9. [Managing Policy Versioning on page 210](#)
10. [Deleting Rules in a Firewall Policy on page 215](#)
11. [Cloning a Rule in a Firewall Policy on page 216](#)
12. [Grouping Rules in a Firewall Policy on page 216](#)
13. [Enabling/Disabling Rules in a Firewall Policy on page 216](#)
14. [Expanding/Collapsing All Rules in a Firewall Policy on page 217](#)
15. [Cutting/Copying and Pasting Rules or Rule Groups in a Firewall Policy on page 217](#)
16. [Assigning Devices to a Firewall Policy on page 218](#)
17. [Firewall Policy Rule Hits on page 219](#)
18. [Generating the Policy Analysis Report on page 221](#)
19. [Deleting Devices from a Firewall Policy on page 223](#)
20. [Rule Operations on the Filtered Rules on page 223](#)
21. [Managing Custom Column Data on page 225](#)
22. [Modifying Custom Columns Definitions on page 225](#)
23. [Deleting a Custom Columns Definition on page 226](#)
24. [Exporting a Custom Columns Definition on page 226](#)
25. [Showing Firewall Policy for a Corresponding Log on page 226](#)

## Modifying Firewall Policies

To modify a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the security policy you want to modify from the left pane and select **Modify Policy**.

The Edit Policy window appears. You can modify the name, description, profile, and IPS configuration mode of the firewall policy.

**Figure 80: Modify Policy Page**

3. You can modify the Manage Zone Policy and Manage Global Policy options.
4. You can modify the Priority and Precedence for the policy. If the priority is the same, you can enter precedence value from 1 to the number of policies of the same priority. If the priority is changed, you can enter the precedence value from 1 to the number of priorities.

For example, the system has 4 Low priorities, 5 Medium priorities, and 3 High priority policies. [Table 28 on page 202](#) shows the precedence value that can be set for different priorities.

**Table 28: Setting Precedence Values for Different Priorities**

Existing Priority	Modified Priority	Precedence that can be Set
Low	Low	1 to 4
Low	Medium	1 to 5

Table 28: Setting Precedence Values for Different Priorities (*continued*)

Existing Priority	Modified Priority	Precedence that can be Set
Low	High	1 to 4

5. Click **Modify**.

Whenever you make any changes to the firewall policy, you will have the option of entering a comment before saving the policy. You can enable or disable this option in Platform > Administration > Applications. To enable this option, right-click **Security Director**, and select the **Modify Security Director Settings** option. Under Applications, select the **Enable save comments for policies** check box. By default, this option is disabled.

In firewall ILP, once you enter the comment, you can save this version with a different name. Click **Save as Draft** from Save drop-down list to save the edited firewall policy with a different name. Entering a comment is not required. All comments you enter are logged.

## Comparing Firewall Policies

To compare any two policies:

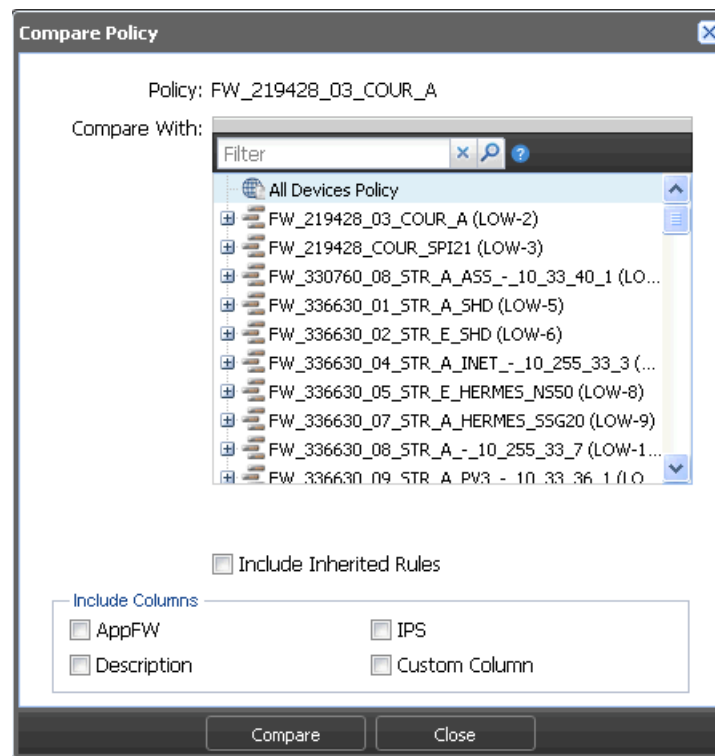
1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to compare with other policies and select **Compare Policy**.

Compare Policy box appears, as shown in [Figure 81 on page 204](#).

Figure 81: Compare Policy



**NOTE:** You can select the Include Inherited Rules check box to include inherited rules while comparing. By default, inherited rules are not part of the comparison.

3. Select the policy to compare with, and click **Compare**.

The following window appears showing the compare result, as shown in [Figure 82 on page 205](#).

Figure 82: Compare Policy Result

Compare Policy -> FW\_219428\_03\_COUR\_A : FW\_219428\_COUR\_SPI21

Previous Diff | Next Diff | Top

Show Unchanged Rules

Added to FW\_219428\_03\_COUR\_A | Modified in FW\_219428\_03\_COUR\_A | Deleted from FW\_219428\_03\_COUR\_A

Policy Property Changes

Property	FW_219428_COUR_SPI21	FW_219428_03_COUR_A
Name	FW_219428_COUR_SPI21	FW_219428_03_COUR_A

Rule Changes

Rule Name	Source			Destination		Service	Action	Profile
	Zone	Address	Sourceidentity	Zone	Address			
Zone								
5	admin	FW_219428_03_COUR_A		dmz	GrpRes.Admin_NOC	GrpSvc_Vers-Admin	PERMIT	Log Session Close
4	admin	Any		dmz	Any	Any	DENY	Log Session Close
6	dmz	GrpRes.Admin_NOC		admin	FW_219428_03_COUR_A	GrpSvc_Vers-Plateforme	PERMIT	Log Session Close
3	dmz	Any		admin	Any	Any	DENY	Log Session Close
7	dmz	GrpRes.Admin_NOC		trust	Res.FW-WANHD-SPI21	GrpSvc_Vers-Plateforme	PERMIT	Log Session Close
2	dmz	Any		trust	Any	Any	DENY	Log Session Close
1	trust	FW_219428_01_COUR FW_219428_02_COUR		dmz	Lp.Srv_NSM1_Mts Srv_Nsmcompress1_Bdx	ping Recu_NSM_1	PERMIT	Log Session Close
8	trust	Res.FW-WANHD-SPI21		dmz	GrpRes.Admin_NOC	GrpSvc_Vers-Admin	PERMIT	Log Session Close
9	trust	Any		dmz	Any	Any	DENY	Log Session Close
1	trust	Any		untrust	Any	Grp_Q0_basse_depriorise	PERMIT	Log Session Close
2	trust	Any		untrust	Any	Any	PERMIT	Log Session Close
3	untrust	Any		trust	Any	Grp_Q0_basse_depriorise	PERMIT	Log Session Close
4	untrust	Any		trust	Any	Any	PERMIT	Log Session Close

Close

## Deleting Firewall Policies

To delete a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to delete and select **Delete Policy**.

A confirmation window appears.

3. Click **Yes**.



**NOTE:** If you delete a firewall policy, the erase configuration is sent to all devices that were a part of the firewall policy during the next Update operation for the device.



**NOTE:** If the published policy is deleted, Security Director application will unpublish the policy on the device.

## Adding Rules to a Firewall Policy

You can add the rules before or after the firewall rule. To add rules:

1. Select **Security Director > Firewall Policy**.

The Policy tabular view appears.

2. Select the firewall rule to which you want to add rules, right-click, and select **Add Rules Before** or **Add Rules After**.

You will get an option to add rules before the firewall rule, or after the firewall rule.

## Cloning Firewall Policies

To clone a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to clone and select **Clone Policy**.

The **Clone Policy** window appears. You can modify the name, description, profile, manage all devices policy, manage zone policy, priority, precedence, and IPS mode of the firewall policy. By default, the original policy values are displayed in the Priority and Precedence fields. If required, you can change them. When you clone a firewall policy, IPS settings are also cloned.

Figure 83: Clone Policy Page

The screenshot shows the 'Clone Policy' dialog box. It contains the following fields and controls:

- Name:** A text box containing 'copy\_of\_Gateway-BNG'.
- Description:** A text box containing 'Created by Import'.
- Manage Zone Policy:** A checked checkbox.
- Manage Global Policy:** An unchecked checkbox.
- Policy Priority:** A dropdown menu set to 'Low' with a help icon.
- Precedence:** A text box containing '4' followed by 'Of 16'.
- Profile:** A dropdown menu set to 'Select profile...'.
- Buttons:** 'Clone' and 'Cancel' buttons at the bottom.



**NOTE:** The priority and precedence value of the cloned policy is same as the priority and precedence of the original policy. For the other policies, the priority and precedence value will be moved to one level down.

3. Click **Clone**.

## Promoting a Firewall Policy

To promote a device policy to the group policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the device policy you want to promote, and select **Promote Policy to Group Policy**.

The Promote Device Policy to Group Policy window appears, as shown in [Figure 84 on page 207](#).

**Figure 84: Promote Policy Page**

3. Enter the name, description, policy priority, and precedence. Click **Promote**.

The device policy is promoted only to the prerule of the group policy.



**NOTE:** By default, the policy profile and IPS mode of a device policy is promoted to the group policy.

## Exporting a Firewall Policy

To export a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to export and select **Export Policy**.

The Export Policy window appears.

3. Click **Export**.

## Policy Versioning

You create a policy version by taking a snapshot of the policy. You can create versions for all types of firewall policies including All devices, Group, Device, and Device exceptions. The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you must delete the unwanted versions before saving a new version. Versioning and rollback are independent operations for each policy. For example, if you take a snapshot of a group firewall policy, it does not version all device policy rules and hence you must separately version each policy rules.

You can delete the older version of snapshots by clicking the **Auto delete oldest version** option, as shown in [Figure 86 on page 210](#). This option is enabled by default. If this option is disabled, every time the oldest version of snapshots are deleted (after the maximum number of versions is reached), a warning message is displayed on the screen. If you enable this option, the oldest snapshots are deleted automatically, without any warning messages.

To create a version of the policy:

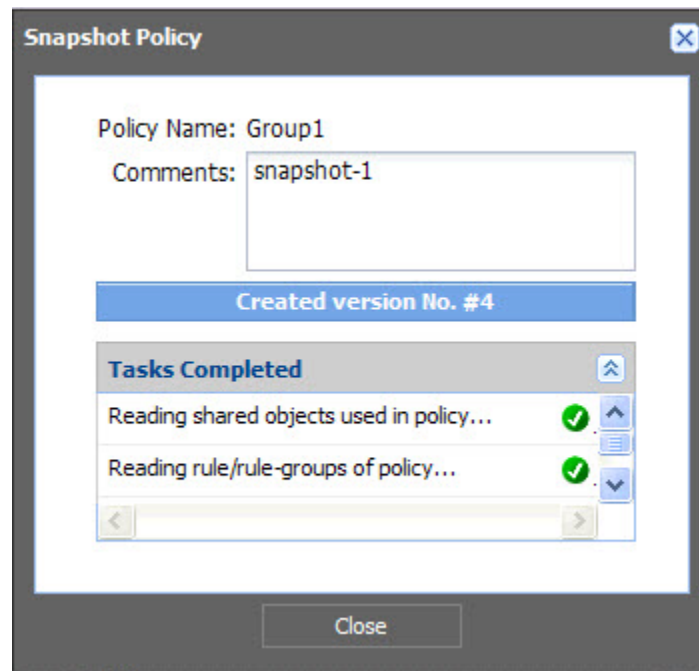
1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to take a snapshot of, and select **Snapshot Policy**.

The Policy Name field shows the name of the firewall policy for which the snapshot is taken. Enter your comments in the Comments field, and press **Create to take the snapshot**. The Snapshot Policy Window appears, showing the status of the version as it is created, [Figure 85 on page 209](#).

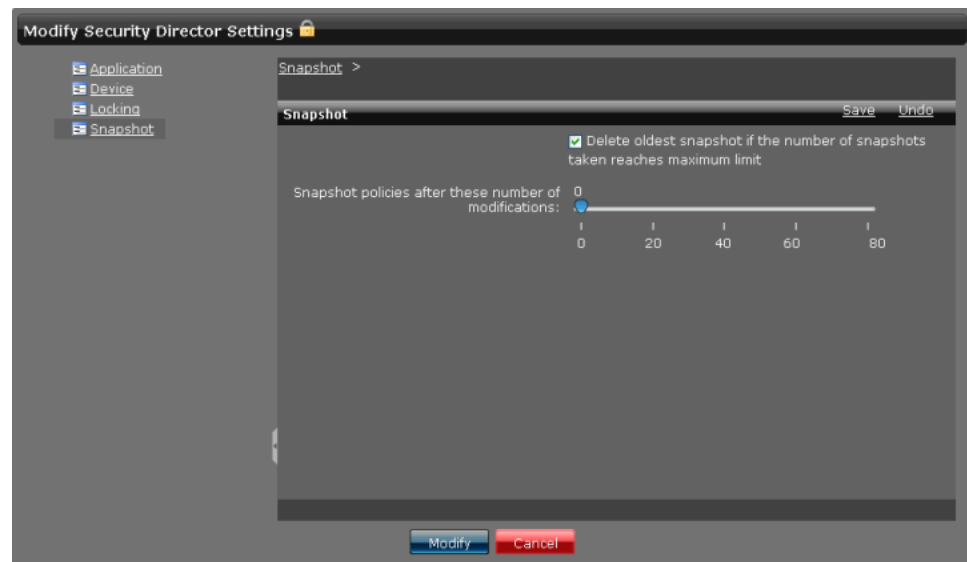
Figure 85: Snapshot Policy Window



The versioned data includes the multiple zones for global rules.

**NOTE:**

- During policy publish, Security Director takes an automatic snapshot of the policy.
- You can set an option to take the snapshot automatically after you have modified and saved a policy after configured number of times, as shown in [Figure 86 on page 210](#). When the snapshot is taken automatically, Security Director does not make any log entry because it is an internal operation.

**Figure 86: Modify Security Director Settings****Managing Policy Versioning**

You can view or manage all available versions of a selected policy. You can perform the following tasks on the snapshots:

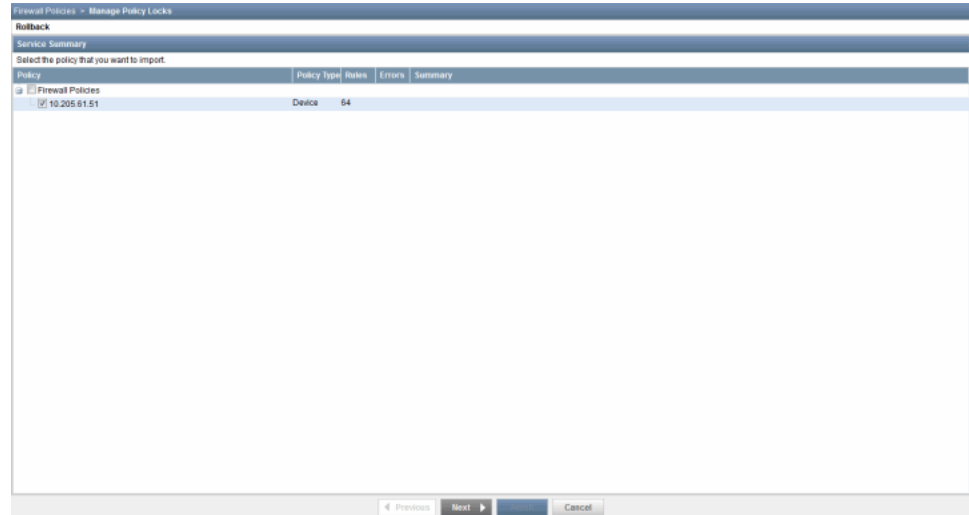
- Roll back to a specific version.
- View the differences between any two versions (including the current version) of the policy.
- Delete one or more versions from the system.

To rollback the selected version as the current version:

1. Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
2. Right-click the firewall policy and select **Manage/Rollback Policy**.  
A window appears showing all the versions of the policy.
3. Select the version that you want to make as current and click **Rollback**.

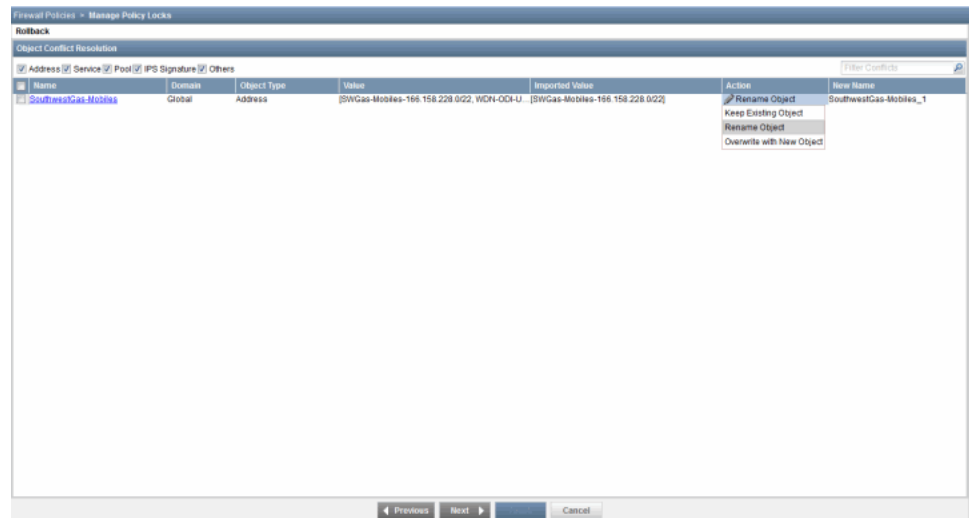
A service summary window appears, as shown in [Figure 87 on page 211](#).

**Figure 87: Rollback Service Summary Page**



The rollback operation replaces all the rules and rule groups of the current version with rules and rule groups from the selected version. For all the shared objects, Object Conflict Resolution (OCR) is done. If there are any conflicts between the versioned data and the current objects in the system, the OCR window is displayed, as shown [Figure 88 on page 211](#).

**Figure 88: Object Conflict Resolution Window**



From the OCR window, you can choose to retain the existing object, rename the object, or overwrite it with the new object.

4. After finishing all the conflict resolution, click **Next** to view the OCR summary report, as shown [Figure 89 on page 212](#).

Figure 89: Rollback OCR Summary Report

Firewall Policies > Manage Policy Locks

Rollback

Print Report

Selected Services

Type	Name	Policy Type	Total Rules	Imported Rules	Errors	Warning	Summary
Preval	10.205.61.51	Device	64	64	0	0	

Object Error Summary

Type	Object	Affected Objects	Errors
No Errors			

Object Conflict Resolution

Object Type	Original Name	Domain	Resolution	Resolved Name	Old Value	New Value
Address	SouthwestGas-Mobiles	Global	Create with New Name	SouthwestGas-Mobiles_1	[SWGas-Mobiles-166.158.228.0/22, VIOFI-CDI-Unraid-MP-Pool]	[SWGas-Mobiles-166.158.228.0/22]

Object Creation List :


Address

Name	Type	IP Address	Host Name	Members	Description
SouthwestGas-Mobiles_1	Group			SWGas-Mobiles-166.158.228.0/22	

PreviousNextFinishCancel

- Click **Finish** to replace the current policy with the versioned data. Summary of the snapshot policy is provided, as shown in Figure 90 on page 212.

Figure 90: Rollback Snapshot Policy Report

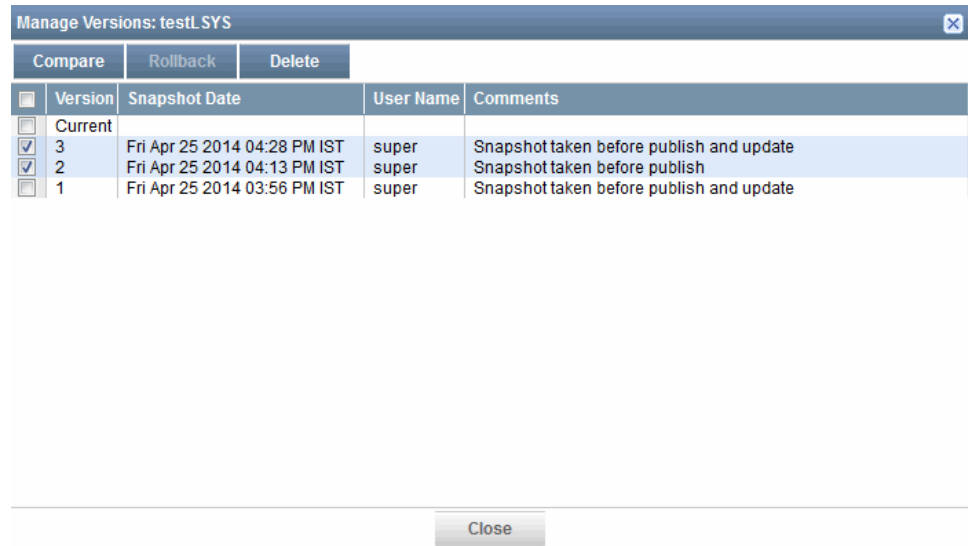
Snapshot Policy		
<div>  <b>Status: SUCCESS</b>  <b>Start Time: Aug 14, 2012 3:16:15 PM UTC+05:30</b>  <b>End Time: Aug 14, 2012 3:16:17 PM UTC+05:30</b> </div>		
Rollback Policy-361353		
Task	Status	Details
Reading import Files	In Progress	Started at Tue Aug 14 09:46:15 UTC 2012
Reading import Files	Success	Finished at Tue Aug 14 09:46:15 UTC 2012
Rollback Addresses	In Progress	Started at Tue Aug 14 09:46:15 UTC 2012
Rollback Addresses	Success	Finished at Tue Aug 14 09:46:16 UTC 2012
Rollback Services	In Progress	Started at Tue Aug 14 09:46:16 UTC 2012
Rollback Services	Success	Finished at Tue Aug 14 09:46:16 UTC 2012
Acquiring Policy Lock	Success	
Rollback Firewall Policy	In Progress	Started at Tue Aug 14 09:46:16 UTC 2012
Rollback Firewall Policy	Success	Started at Tue Aug 14 09:46:16 UTC 2012
Releasing Policy Lock	Success	
Summary		<a href="#">Summary Report</a>
<div> <div>Page 1 of 1</div> <div>Displaying 1 - 11 of 11</div> </div>		
Close		

To compare two different versions of a policy:

- Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
- Right-click the firewall policy, and select **Manage/Rollback Policy**.

The Manage Versions window appears, showing all policy versions, as shown in [Figure 91 on page 213](#).

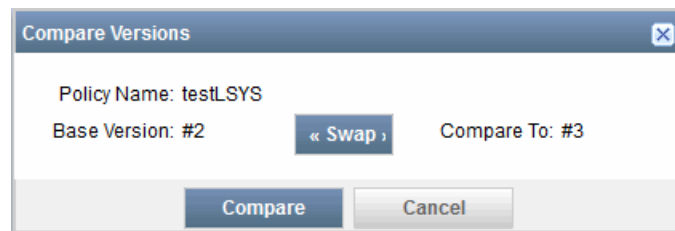
**Figure 91: Manage Versions Window**



3. Select the versions to be compared, and click **Compare**. You can select only two versions at a time to compare.

You can clear the columns you do not want included in the comparison. By default, all columns are selected in the Compare Versions window, as shown in [Figure 92 on page 213](#).

**Figure 92: Compare Versions Window**



4. Click **Compare** to view the results.

A Compare Versions results window appears, showing the differences between the selected versions, as shown in [Figure 93 on page 214](#).

Figure 93: Compare Versions-Results Window

Compare Versions : 10.205.61.41 -> #3: Current

Previous Diff

Next Diff

Top

Show Unchanged Rules

10.205.61.41(Exception)#Current Modified

Added to 10.205.61.41(Exception)#Current

Deleted from 10.205.61.41(Exception)#Current

Policy Property Changes

Name	10.205.61.41_2#3	10.205.61.41(Exception)#Current
Name	10.205.61.41_2	10.205.61.41(Exception)

Rule Changes

Rule Name	Source			Destination		Service	Action	Profile	AppFW	IPS	Description
	Zone	Address	SourceIdentity	Zone	Address						
Zone											
Device Rules											
Device-Zone-2	trust	Any		untrust	Any	Any	DENY		None		
Global											
Device Rules											
Device-Global-11111		Any		Any	Any	Any	PERMIT	Custom	None	IPS ON	
Device-Global-2		Any		Any	Any	Any	DENY		None		
Device-Global-3		Any		Any	Any	Any	DENY		None		
Device-Global-4		Any		Any	Any	Any	DENY		None		
Device-Global-6		Any		Any	Any	Any	DENY		None		
Device-Global-7		Any		Any	Any	Any	DENY		None		
Device-Global-8		Any		Any	Any	Any	DENY		None		
Device-Global-9		Any		Any	Any	Any	DENY		None		
Device-Global-11		Any		Any	Any	Any	DENY		None		
Device-Global-111		Any		Any	Any	Any	DENY		None		
Device-Global-1		Any		Any	Any	Any	PERMIT	Custom	None	IPS ON	

Column Changes

Rule	Column	10.205.61.41_2#3	10.205.61.41(Exception)#Current

Close

Shahida

The general policy Compare Versions results window has the following sections:

- Policy Property Changes—Shows policy changes for the modified rules.
- Rule Changes—Displays rules that are added, modified, or deleted.
- Column Changes—Shows the differences between the column contents for modified rules.

Global policy zone columns are compared according to their content. For example, in version 1 of the policy, the fromZone and toZone columns are configured with the inline values trust, dmz, and vpn. In version 2 of the policy, the Zone column is modified to use a zone set with the same values: trust, dmz, and vpn. Therefore, the policy diff does not show that the Zone column is changed. Although the string representations of the column values are different, the effective fromZone and toZone values are the same and are therefore considered not to have changed.

To delete versions:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

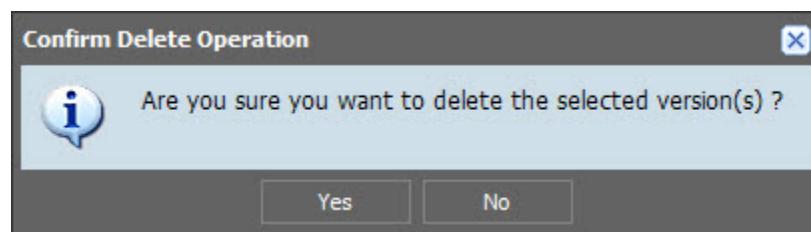
2. Right-click the firewall policy, and select **Manage Snapshots**.

A window appears, showing all policy versions.

3. You can delete multiple versions at a time. During a rollback operation, you are given an option to delete older versions. Select the version that you want to delete, and click **Delete**.

You will receive a Confirm Delete Operation message before you can delete the version, as shown in [Figure 94 on page 215](#).

Figure 94: Confirm Delete Operation Message



4. Click **Yes** to delete the version, or click **No** to abort the operation.



**NOTE:** If you delete a policy, all versioned data for that policy is deleted. Promoting the device to a group policy operation deletes the associated versions.



**NOTE:**

- Priority and precedence of a policy are not rolled back. Only values from the current policy are retained.
- Priority, precedence, IPS mode, IPS signature set (if the mode is basic), and IPS policy rules (if the mode is advanced) are neither versioned, nor rolled back.
- Rollback operation sets the policy publishing state to republishing if the current policy is in the published state.
- For the custom column, only column values are stored in versioned data and rolled back. Column definitions are not part of versioned data.
- If the objects are not present, the following shared objects are not rolled back:
  - Custom template
  - Policy-based VPNs
  - Application signature

## Deleting Rules in a Firewall Policy

To delete rules in a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Select the firewall policy whose rules you want to delete.

The rules of the firewall policy appears in the right pane.

3. Select the check boxes next to the rules that you want to delete.
4. Click the **Delete Rule** icon on the top of the right pane.

## Cloning a Rule in a Firewall Policy

To clone a rule in a firewall policy:

1. Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
2. Select the firewall policy whose rule you want to clone.  
The rules of the firewall policy appears in the right pane.
3. Select the check box next to the rule that you want to clone.
4. Right-click and select **Clone**.

## Grouping Rules in a Firewall Policy

To group rules in a firewall policy:

1. Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
2. Select the firewall policy whose rules you want to group.  
The rules of the firewall policy are displayed in the right pane.
3. Select the check boxes next to the rules you want to group.
4. Right-click the rules and select **Rule Group > Create Rule Group**.  
The Create Rule Group pop-up window appears.
5. Enter a name for the rule group in the Name field.
6. Enter a description for the rule group in the Description field.
7. Click **Create**.



**NOTE:** When the rule group is created, you can add rules in the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

## Enabling/Disabling Rules in a Firewall Policy

To enable or disable rules in a firewall policy:

1. Select **Security Director > Firewall Policy**.  
The Policy Tabular view appears.
2. Select the firewall policy whose rules you want to enable or disable.

The rules of the firewall policy are displayed in the right pane.

3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.



**NOTE:** You can enable or disable a rule group. When a rule group is disabled, all rules in the rule group are also disabled. The rule group row in the Tabular view appears dimmed, but the rules do not appear dimmed. However, if the rules in the rule group appear dimmed, they are not published to the device during the publish operation, if they are disabled.

## Expanding/Collapsing All Rules in a Firewall Policy

To expand or collapse all rules in a firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

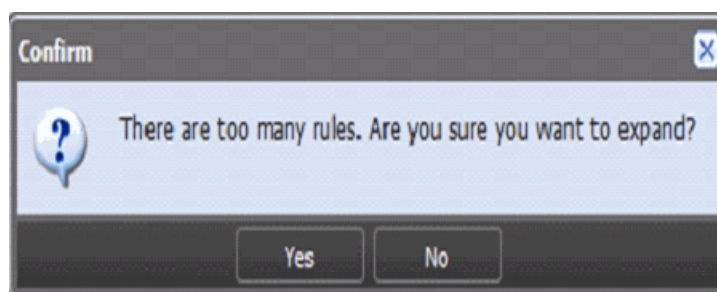
2. Select the firewall policy whose rules you want to expand.

By default, firewall policy rules in collapsed state are displayed in the right pane.

3. Click the **Expand All RuleGroups** icon, and all rules corresponding to that particular policy are expanded.

If a policy contains more than 1000 rules, a warning message is displayed before expanding, as shown in [Figure 95 on page 217](#).

**Figure 95: Expand All Warning Message for More Than 1,000 Rules**



4. Click the **Collapse All RuleGroups** icon to collapse all rules.

## Cutting/Copying and Pasting Rules or Rule Groups in a Firewall Policy

To cut or copy and paste rules or rule groups in a firewall policy:

1. On the right pane, select the device rule or rule group that you want to cut or copy. Right-click the selected device rule or rule group, and select **Cut** or **Copy**. If Cut is selected, related rule or rule group is removed from the right pane view.

You can copy the rules without locking a policy. However, you must lock the policy for the cut operation. You can select the combination of rules or rule groups for cutting

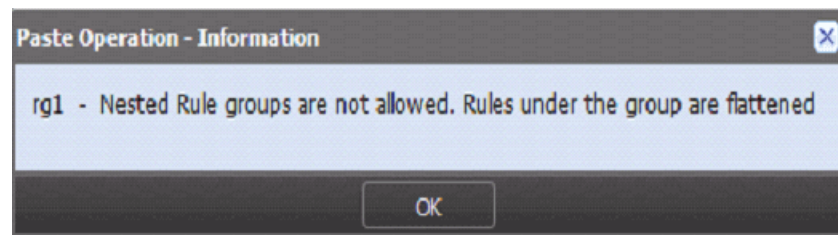
or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

2. On the left pane, select the firewall policy in which you want to paste the rule or rule group. On the right pane, right-click the rule or rule group that you want to paste. You can paste the rule or rule group before or after the selected rule or rule group by choosing the **Paste Before** or **Paste After** option, respectively.

If you are cutting and pasting rules across different policies, you must first save the cut operation in the current policy before moving to another policy for pasting. Otherwise, an error message is displayed, giving you the option either save or discard the changes.

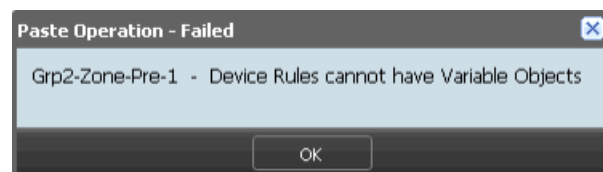
Security Director does not support nested rule grouping. If you paste a rule group in another custom rule group, an error message is displayed, giving you the option to proceed by flattening the copied rule group, as shown in [Figure 96 on page 218](#).

**Figure 96: Nested Rule Group Paste Operation Warning Message**



**NOTE:** If you copy a rule that contains variable objects from the all devices policy and attempt to paste the rule into other policy rules, the following error message is displayed:

**Figure 97: Variable Objects Rule Paste Error**



## Assigning Devices to a Firewall Policy

To assign devices to a group firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy to which you want to assign devices and select **Assign Devices**.

The Assign Devices to Service window appears.

3. Select the devices that need to be added to the firewall policy in the Select Devices pane, select the devices from the Available column and click the right arrow to move these devices to the Selected column. There is option to search for any devices in the Selected column of the Assign Devices window. By default, all the selected devices are sorted in a list and you can search for any devices again, if required.
4. Click **Modify**.

**NOTE:**

- If you do not have permission to certain devices, they will not be visible while assigning devices to a new or existing firewall policy.
- You cannot view the device or exception policies at the left pane, for the assigned devices, that are labeled by the other Junos Space users.

## Firewall Policy Rule Hits

You can perform a probe and reset actions for the rule hits. These probe and reset actions are on a per device basis.

To reset the hits for all policy rules:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the policy rule for which you want to reset the hits, and select **Policy Hits > Reset Hits for All Policy Rules**.

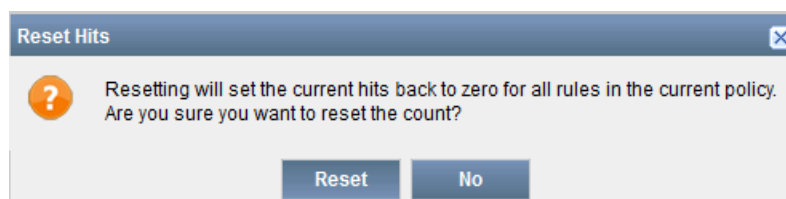
This resets the current hits to zero. This is useful for monitoring the utility rate for each rule. The current hits for all the devices assigned to the current firewall policy are reset to zero.

**NOTE:**

- The reset action resets the current hits to zero; however, the total hits is not changed. Also the date of the current hit is shown.
- The device reboot will not reset the hits in Security Director. Any new hit after a restart is also identified and shown in the GUI along with the previous hit.

Before resetting the hits, a pop-up window appears, requiring you to confirm the reset, as shown in [Figure 98 on page 220](#).

Figure 98: Reset Hit Confirm



3. Click **Reset**.

The current hit is reset to zero.

To probe for the latest hits:

1. Right-click the policy rule that you want to probe for the latest hits, and select **Policy Hits > Probe Latest Hits**.

This probes for the latest hits information for all the Security Director devices. The probe request starts a new job. You can monitor the progress and status of each device probe, as shown in [Figure 99 on page 221](#).

**Figure 99: Probe Latest Hits Job Details**

The screenshot shows a window titled "Job Details: 3342902". It contains the following information:

- User: super
- Job ID: 3342902
- Job type: Policy Hits Collection
- Job status: SUCCESS
- Actual start time: Jan 9, 2015 11:20:08 AM IST
- Scheduled start time: Jan 9, 2015 11:20:07 AM IST
- Percentage completion: 100
- End time: Jan 9, 2015 11:20:09 AM IST

Below this is a section titled "Policy Hits Details" with a search bar "Search Device By Name". It contains a table with the following data:

Device Name	Status	Summary
10.207.98.219	SUCCESS	Policy Rule Count: 15

At the bottom, there is a pagination bar showing "Page 1 of 1", "Auto Refresh" checked, and "Displaying 1 - 1 of 1" items. A "Close" button is at the bottom right.

The hit job fails if the status of the device is DOWN in Security Director. Also, you cannot probe for the current hit if the device is running Junos OS Release 12.1 or prior releases.



**NOTE:** If you probe for the current hit or reset the hits of a group policy, Security Director polls all the devices in the group policy and updates the hits. Even if one of the devices is assigned to the other group policy or device exception policy, those rules are also updated with the latest hits.

## Generating the Policy Analysis Report

To generate the policy analysis report:

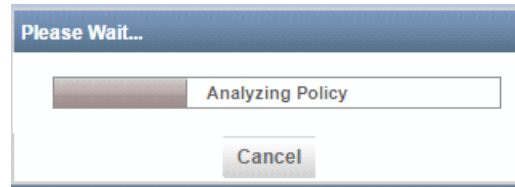
1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy for which you want to generate the policy analysis report, or, from Actions, select **Generate Policy Analysis Report**.

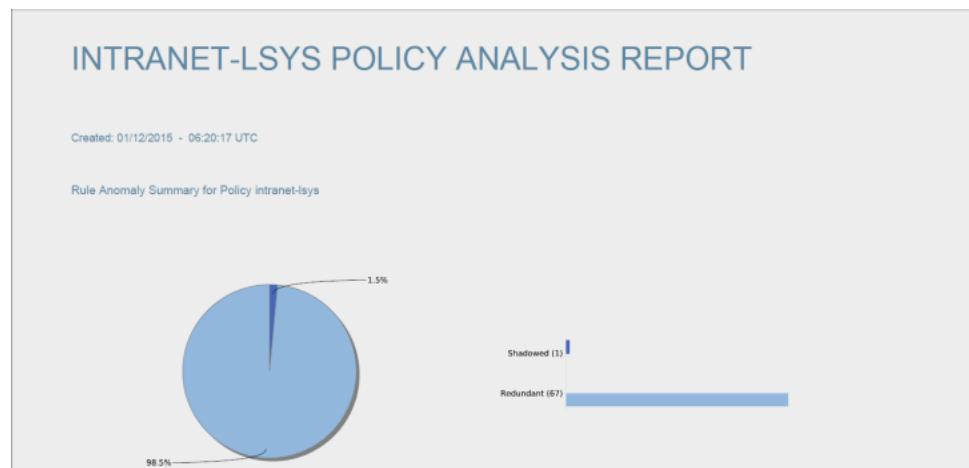
A progress bar is shown displaying the status of the report generation. You can click **Cancel** on the progress bar at any time to cancel the report generation, as shown in [Figure 100 on page 222](#).

**Figure 100: Policy Analysis Progress Bar**



The report is generated in PDF format. Once the report is generated, you get an option to either open the PDF file or save it to the local system. [Figure 101 on page 222](#), [Figure 102 on page 222](#), and [Figure 103 on page 223](#) show the policy analysis report.

**Figure 101: Policy Analysis Report**



**Figure 102: Policy Analysis Report-Shadowed**

**Shadowed**

A rule is shadowed when a previous rule matches all the packets of the current rule, and the Actions for each rule are different. As a result, the shadowed rule will never get hit.

No	Rule Name	SOURCE		DESTINATION		Service	Action
		Source Zone	Source Address	Destination Zone	Destination Address		
<b>Problem:</b> Rule 2343 (Oracle-Server-to-Client-Deny_All) is shadowed by Rule 2342 (Oracle-Server-to-Client-01)							
<b>Recommendation:</b> Move Rule 2343 (Oracle-Server-to-Client-Deny_All) before Rule 2342 (Oracle-Server-to-Client-01) or delete Rule 2343 (Oracle-Server-to-Client-Deny_All)							
2342	Oracle-Server-to-Client-01	Oracle-Server-Test	Any	Oracle-Client-Test	Any	Any	Permit
2343	Oracle-Server-to-Client-Deny_All	Oracle-Server-Test	Any	Oracle-Client-Test	Any	Any	Deny

Figure 103: Policy Analysis-Redundant

Redundant							
A rule is redundant if there exists some preceding rule within the policy which performs the same action on the same packets as performed by the current rule. Removing redundant rules can increase performance by reducing rule comparisons.							
No	Rule Name	SOURCE		DESTINATION		Service	Action
		Source Zone	Source Address	Destination Zone	Destination Address		
Problem: Rule 2 (PERMIT_ALL), Rule 3 (ID-484) is redundant with Rule 1 (ID-TEST-POLICY) Recommendation: Delete Rule 2 (PERMIT_ALL), Rule 3 (ID-484)							
1	ID-TEST-POLICY	A.O.T.P.VPRN22	Any	A.O.T.P.VPRN22	Any	Any	Permit
2	PERMIT_ALL	A.O.T.P.VPRN22	Any	A.O.T.P.VPRN22	Any	Any	Permit
3	ID-484	A.O.T.P.VPRN22	22.ALL	A.O.T.P.VPRN22	22.ALL	Any	Permit
Problem: Rule 3 (ID-484) is redundant with Rule 2 (PERMIT_ALL) Recommendation: Delete Rule 3 (ID-484)							
2	PERMIT_ALL	A.O.T.P.VPRN22	Any	A.O.T.P.VPRN22	Any	Any	Permit
3	ID-484	A.O.T.P.VPRN22	22.ALL	A.O.T.P.VPRN22	22.ALL	Any	Permit
Problem: Rule 27 (ID-1061), Rule 28 (ID-677), Rule 29 (ID-607), Rule 30 (ID-610), Rule 31 (ID-614), Rule 32 (ID-618), Rule 33 (ID-617), Rule 34 (ID-620), Rule 35 (ID-623), Rule 36 (ID-600), Rule 37 (ID-625), Rule 38 (ID-1003), Rule 39 (ID-1482), Rule 40 (ID-1483), Rule 41 (ID-1751), Rule 42 (ID-1913), Rule 43 (ID-2240), Rule 44 (ID-2322), Rule 45 (ID-2343), Rule 46 (ID-2616), Rule 47 (ID-2617), Rule 48 (ID-2667), Rule 49 (ID-2706), Rule 50 (ID-2934), Rule 51 (ID-2937), Rule 52 (ID-2952), Rule 53 (ID-2953), Rule 54 (ID-3072) is redundant with Rule 26 (ID-3183) Recommendation: Delete Rule 27 (ID-1061), Rule 28 (ID-677), Rule 29 (ID-607), Rule 30 (ID-610), Rule 31 (ID-614), Rule 32 (ID-618), Rule 33 (ID-617), Rule 34 (ID-620), Rule 35 (ID-623), Rule 36 (ID-600), Rule 37 (ID-625), Rule 38 (ID-1003), Rule 39 (ID-1482), Rule 40 (ID-1483), Rule 41 (ID-1751), Rule 42 (ID-1913), Rule 43 (ID-2240), Rule 44 (ID-2322), Rule 45 (ID-2343), Rule 46 (ID-2616), Rule 47 (ID-2617), Rule 48 (ID-2667), Rule 49 (ID-2706), Rule 50 (ID-2934), Rule 51 (ID-2937), Rule 52 (ID-2952), Rule 53 (ID-2953), Rule 54 (ID-3072)							
26	ID-3183	A.T.O.T.P.01	ALL	A.P.O.T.P.IFTEL	ALL	Any	Permit
27	ID-1061	A.T.O.T.P.01	DC2WR06566	A.P.O.T.P.IFTEL	ALL-PCX-PMDC-CS1-VP	DNS ICMP_ANY	Permit

You can schedule the report generation task from the Reports workspace. Along with scheduling the task, you can also configure e-mail recipients to send the reports to them automatically. You require only the view policy permission to generate the policy analysis report. To know more about scheduling the report generation, see [“Creating a Policy Analysis Report Definition” on page 94](#).

## Deleting Devices from a Firewall Policy

To delete devices from a group firewall policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy from which you want to delete devices and select **Assign Devices**.

The Assign Devices to Service window appears.

3. Select the devices that need to be deleted from the firewall policy in the Select Devices pane, select the devices from the Selected column and click the left arrow to move these devices to the Available column.

4. Click **Modify**.



**NOTE:** Deleting a device from a group firewall policy creates a device firewall policy. This policy carries all the device rules of the device from the group firewall policy.

## Rule Operations on the Filtered Rules

You can perform various rule operations on the filtered list of rules. For example, consider a policy having seven rules such as *a*, *b*, *c*, *d*, *e*, *f*, and *g* in an order inside a rule group. After filtering, if only second and sixth rules are filtered, that is only rules *b* and *f*,

[Table 29 on page 224](#) explains the various rule operations on the filtered rules.

Table 29: Various Rule Operation on the Filtered Rules

Rule Operation	Action
Add rule before	<p>To add a new rule before an existing rule, select the existing rule in the filtered list and add the new rule above it.</p> <p>For example, if you perform this operation by selecting the sixth rule that is <i>f</i>, the seventh rule must be added before the sixth rule, in the filtered list. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Add rule after	<p>To add a new rule after an existing rule, select the existing rule in the filtered list and add the new rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the seventh rule must be added after the second rule. This rule is added at the third place in the full list.</p>
Paste before	<p>To paste a copied rule before an existing rule, select the existing rule in the filtered list and paste the copied rule above it.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the copied rule must be added after the sixth rule. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Paste after	<p>To paste a copied rule after an existing rule, select the existing rule in the filtered list and paste the copied rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the copied rule must be added after the second rule. The new rule is added at the third place in the full list.</p>
Clone	<p>To clone a selected rule, select the existing rule you want to clone in the filtered list. The cloned rule will be added above the selected rule.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the cloned rule must be added after the sixth rule, at the seventh place. The rule <i>g</i> must be moved down to the eighth place in the full list. This can be checked by clearing the filter from the search box.</p>
Move rule to top	<p>To move a rule to the top of a list, select the rule you want to move in the filtered list and move rule to the top. If you move a rule from a filtered list to the top of that list, the selected rule is also moved to the top of the full list.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved to the top in the rule group, at first place in the original list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule to bottom	<p>To move a rule to the bottom of the list, select the rule you want to move in the filtered list and move rule to the bottom. If you move a rule from a filtered list to the bottom of that list, the selected rule is also moved to the bottom of the full list.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved to the bottom in the rule group, at the seventh place in the full list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the last rule in the full list.</p>

Table 29: Various Rule Operation on the Filtered Rules (*continued*)

Rule Operation	Action
Move rule up	<p>To move a rule up one position in the list, select the rule you want to move in the filtered list and move rule up one position.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved before the second rule <i>b</i> in the filtered list. This rule is moved to the second place in the rule group in the full list.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule down	<p>To move a rule down one position in the list, select the rule you want to move in the filtered list and move rule down one position.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved after the sixth rule <i>f</i> in the filtered list. This rule is moved to the sixth rule in the rule group in the full list.</p> <p>This option is disabled for the last rule in the full list.</p>

## Managing Custom Column Data

You can insert, edit, or delete custom columns and their corresponding policy rules through an inline edit.

Security Director uses the following parameters to validate custom column data:

- Explicit regular expression—Validation is based on the optional regular expression property, if defined for the current custom column.
- Implicit length check—The maximum length of the data must be 256 characters. It is applicable to all custom columns.



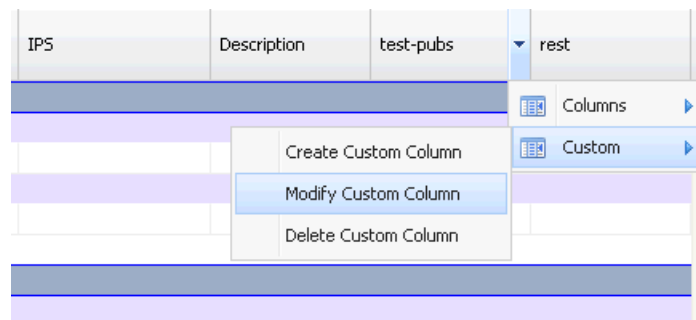
**NOTE:** The Save and Discard buttons, which are used to save or discard all the edits—including inline edits of custom column fields—are not used for registering custom columns. These actions are committed as soon as they are completed in their respective UI and are independent of the Save or Discard button.

## Modifying Custom Columns Definitions

To modify a custom column:

1. Click the custom column name in the column header, go to **Custom**. Click and select **Modify Custom Column**.

Figure 104: Modifying a Custom Column



2. Once the edit is complete, the column header is refreshed to reflect the changes.



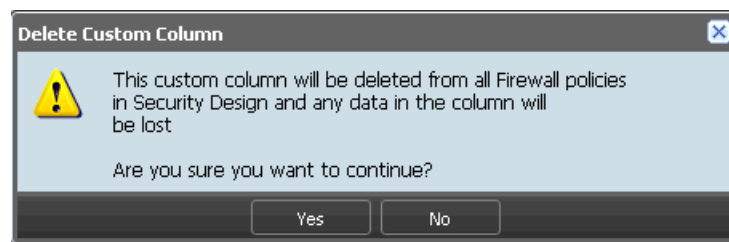
**NOTE:** You must have edit permissions to modify the custom column registration settings.

## Deleting a Custom Columns Definition

To delete the custom column definition:

1. Click the custom column name in the column header, go to **Custom**, then select and click **Delete Custom Column**.
2. A delete confirmation message appears, as shown in [Figure 105 on page 226](#). After you confirm the deletion and the delete process finishes, Security Director updates the header and removes the column.

Figure 105: Deleting a Custom Column



## Exporting a Custom Columns Definition

Custom column definition is exported when a firewall rule is exported.

## Showing Firewall Policy for a Corresponding Log

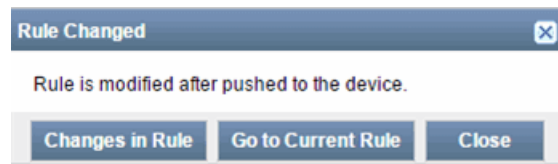
When a log is generated for a policy rule in the Event Viewer workspace, you can view the corresponding firewall policy.

To view the source NAT policy for a corresponding log:

1. Under the Event Viewer workspace, if a log is generated by a policy rule, the corresponding rule name is populated in the Policy Name column. Right-click the required log, and select **Show Policy**.

If there are no changes in the rules, you are directly redirected to the corresponding rule with filters applied on both left and right pane of the Firewall Policies landing page. If there is a change in the current rule and the rule that generated the log, a pop-up window is displayed, as shown in [Figure 106 on page 227](#).

**Figure 106: Jumping to the Current Policy Rule**



2. Click **Changes in Rule** to view the diff between the current rule and the version of the rule that generated the log. The current version of the rule is compared with the version that existed at the time of log generation.

In the Show Rules window, click Go to Policy Comparison to compare the rules within the policy.

OR

Click **Go to Current Rule** to view the current policy rule. In the left-pane search window, the policy name search string is shown; In the right-pane search window, the current rule name filter string is shown.

#### Related Documentation

- [Firewall Policies Overview on page 151](#)
- [Creating Firewall Policies on page 159](#)
- [Adding Rules to a Firewall Policy on page 180](#)
- [Ordering the Rules in a Firewall Policy on page 185](#)
- [Publishing Firewall Policies on page 194](#)
- [Tracking the Utility Rate of Security Firewall Policies on page 190](#)



## CHAPTER 14

# Creating and Managing Application Signatures

- [Creating Application Signatures on page 230](#)
- [Managing Application Signatures on page 233](#)

## Creating Application Signatures

To create an application signature:

1. Select **Security Director > Firewall Policies > Application Signatures**.

All application signatures that are downloaded appears on the Application Signatures page, as shown in [Figure 107 on page 230](#). This page displays the version of the signature database. On the left side of the page are the different categories of signature, and on the right side of the page are the signatures.

Figure 107: Application Signatures Page

Name	Object type	Category	Sub-Category	Risk	Characteristic	Device Comp.	Pre-defined/C.	ID	Domain
ICMP-ASSIGN	Application	Infrastructure	Networking	Low		All Devices	Predefined	1006	SYSTEM
ICMP-TYPE-114	Application	Infrastructure	Networking	Low		All Devices	Predefined	11451	SYSTEM
ICMP-TYPE-173	Application	Infrastructure	Networking	Low		All Devices	Predefined	11510	SYSTEM
ICMP-TYPE-208	Application	Infrastructure	Networking	Low		All Devices	Predefined	11545	SYSTEM
GRABOID	Application	Web	Multimedia	Moderate	Bandwidth Consumer	All Devices	Predefined	10956	SYSTEM
ICMP-PORT-UNREACH	Application	Infrastructure	Networking	Low		All Devices	Predefined	11311	SYSTEM
CAFEMOM	Application	Web	Social-Networking	Low	Loss of Productivity	All Devices	Predefined	374	SYSTEM
ICMP-ASSIGN	Application	Infrastructure	Networking	Low		All Devices	Predefined	1590	SYSTEM
CAMPPIRENOW	Application	Web	Applications	Moderate	Prone to Misuse	All Devices	Predefined	770	SYSTEM
SKYPE	Application	Infrastructure	VOIP	High	Bandwidth Consumer	All Devices	Predefined	183	SYSTEM
ICMP-ECHO-REPLY	Application	Infrastructure	Networking	Low		All Devices	Predefined	11304	SYSTEM
ENDNOTE	Application	Web	Applications	Unsafe	Can Leak Information	All Devices	Predefined	11250	SYSTEM
XNDEGS	Application	Web	Multimedia	Moderate	Bandwidth Consumer	All Devices	Predefined	1077	SYSTEM
NATEDN-LOGIN	Application	Messaging	Instant-Messaging	Low	Loss of Productivity	All Devices	Predefined	11190	SYSTEM
LINKEDIN	Application	Web	Social-Networking	Low	Loss of Productivity	All Devices	Predefined	305	SYSTEM

From Junos OS Release 12.1X47 onwards, the Nested applications are termed as Applications with the same details converted as members of Application signature. These Application signatures are called ngAppIDs. The Application Signatures page shows only the ngAppID2.0 applications and application group.

2. Click **Create Application Signature**.

The Create Application Signature page appears, as shown in [Figure 108 on page 231](#).

Figure 108: Create Application Signature

**Create Application Signature**

**GENERAL INFORMATION**

Name:

Description:

**TAGS** ?

Category:  ▼

Sub-Category:  ▼

Risk:  ▼

**SIGNATURE TYPE** ?

☒ Basic ☐ Advanced

**SIGNATURE DETAILS**

Min Data\*:

Port Range\*:

**Patterns**

Client to Server:

**Create** **Cancel**

3. Enter the name of the application signature in the Name field.
4. Enter the description for the application signature in the Description field.
5. Select the category of the application signature from the Application Signature drop-down menu.
6. Select the subcategory of the application signature from the Sub-Category drop-down menu.
7. Select the category of risk from the Risk drop-down menu.
8. Select the signature type as either Basic or Advanced.

For the devices running Junos OS Release 12.1X46 and previous versions, Basic is same as Application, and Advanced is same as the Nested Application.

9. If you select Basic as the signature type, enter the following information under the Signature Details tab:
  - a. Enter the data range in the Min Data field.
  - b. Enter the range of ports in the Port Range field.

- c. Under the Patterns, enter the following information:
    - Enter the appropriate information in the Client to Server field.
    - Enter appropriate information in the Server to Client field.
  - d. Click **Create**.
10. If you selected Advanced as the signature type, enter the following information:
- a. Enter the range of ports in the Max Transactions field.
  - b. To create the signature details, click the plus sign (+).  
The Signature Details page appears.
  - c. From the Protocol drop-down select the protocol. The available protocols are HTTP and SSL.  
You can create signature details for a single protocol, and each protocol can have members up to 16.
  - d. Select the Chain Order check box which is used to match the pattern.
  - e. Click the plus sign (+) to create the signature.  
The Signature page appears.
  - f. From the Context drop-down list, select required context to match.
  - g. From the Direction drop-down list, select the direction as Client to Server, Server to Client, or Any.
  - h. In the Pattern field, enter the appropriate information.
  - i. Click **OK**.
11. Click **Create**.  
A new Application Signature is created.

Publish fails under the following conditions:

- If you push custom signatures to a device running Junos OS Release 12.1X47.
- Security Director trims the signature if the predefined signatures are not supported.



**NOTE:** In the left pane of the Application Signatures landing page, you can see the device compatibility information under the Device Compatibility column.

---

**Related  
Documentation**

- [Managing Application Signatures on page 233](#)

## Managing Application Signatures

---

You can filter, modify, delete, or clone, application signatures listed on the Application Signatures page. You can also create application signature groups in this page.

To open the Application Signatures page:

- From the **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page appears.

You can right-click the application signatures to manage them.

You can perform the following tasks on the Application Signatures page:

- [Filtering Application Signatures on page 233](#)
- [Modifying Application Signatures on page 234](#)
- [Modifying Application Signature Groups on page 234](#)
- [Deleting Application Signatures on page 234](#)
- [Cloning Application Signatures on page 235](#)
- [Cloning Application Signature Groups on page 235](#)
- [Viewing Application Signature Details on page 235](#)

## Filtering Application Signatures

To filter application signatures:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded. The right pane displays the signatures and the left pane displays the different filters that can be used to filter the signatures. The different parameters that can be used to filter the signatures include Category, Sub-Category, Risk, Predefined/Custom, Object Type, Activation Date, Device Compatibility, and Modify Date. Every parameter has different subparameters.

2. Click the check box next to the subparameters within a parameter.

To filter the signatures based on the device compatibility parameter:

1. In the left pane, under the Advanced Filter, expand the Device Compatibility column.

The available device compatibility version are:

- All Devices
- X46 and older devices
- X47 and newer devices

2. Select the required compatibility version check box.
3. The filtered data is available in the right pane.

## Modifying Application Signatures

To modify application signatures:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Select the check box next to the application signature you want to modify.



**NOTE:** You cannot modify the predefined application signatures. You can only modify the custom application signatures you have added.

3. Right-click the application signature and select **Modify Application Signature**.

You will be redirected to the Modify Application Signature page. You can make necessary changes to the application signature here. However, you cannot modify the signatures in the System domain.

4. Click **Modify**.

## Modifying Application Signature Groups

To modify application signature groups:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Select the check box next to the application signature group you want to modify.

3. Right-click the application signature group, and select **Modify Application Signature Group**.

You will be redirected to the Modify Application Signature Group page. You can make necessary changes to the application signature group here.

4. Click **Modify**.

## Deleting Application Signatures

To delete application signatures:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Select the check box next to the application signatures you want to delete.



**NOTE:** You cannot delete the predefined application signatures, and the signatures in the System domain. You can only delete the custom application signatures you have added.

3. Right-click the application signature and select **Delete Selected**.

A confirmation window appears.

4. Click **Yes**.

## Cloning Application Signatures

To clone application signatures:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Select the check box next to the application signature you want to clone.
3. Right-click the application signature and select **Clone Application Signature**.

You are redirected to the Clone Application Signature page. You can clone the application signature here.

## Cloning Application Signature Groups

To clone application signature groups:

1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Select the check box next to the application signature group you want to clone.
3. Right-click the application signature group, and select **Clone Application Signature Group**.

You are redirected to the Clone Application Signature Group page. You can clone the application signature group here.

## Viewing Application Signature Details

You can view the details of any application signature. To view the details:

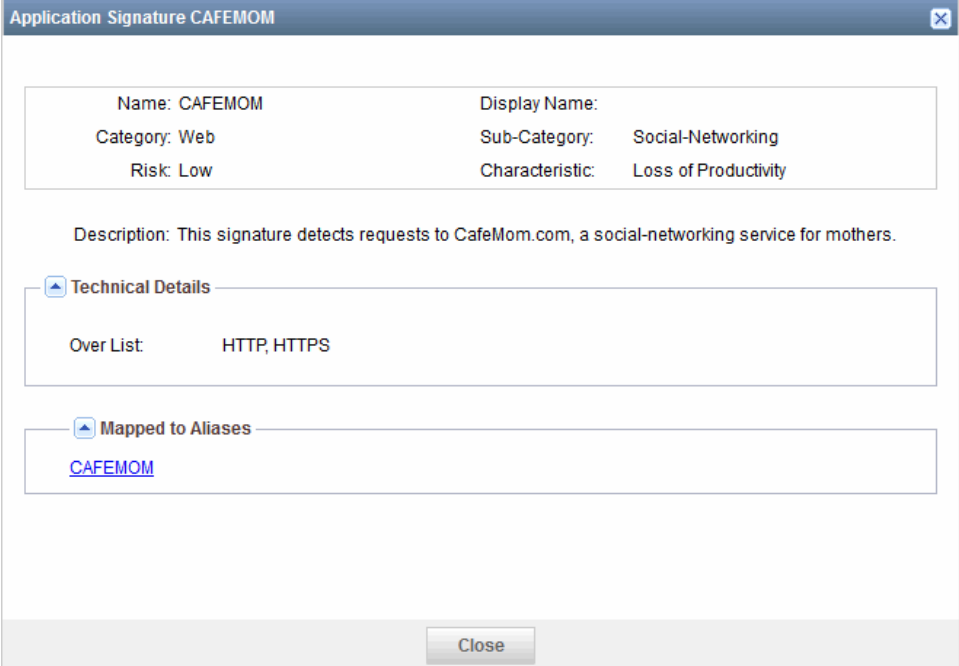
1. Select **Security Director > Firewall Policies > Application Signatures**.

The Application Signatures page displays all signatures that are downloaded.

2. Double click on any application.

A pop-up Application Signature window appears, with details of that particular application, as shown in [Figure 109 on page 236](#).

Figure 109: Application Signature Details



The image shows a dialog box titled "Application Signature CAFEMOM". It contains a table with application details, a description, and two expandable sections for technical details and mapped aliases.

Name: CAFEMOM	Display Name:
Category: Web	Sub-Category: Social-Networking
Risk: Low	Characteristic: Loss of Productivity

Description: This signature detects requests to CafeMom.com, a social-networking service for mothers.

**Technical Details**

Over List: HTTP, HTTPS

**Mapped to Aliases**

[CAFEMOM](#)

Close

## CHAPTER 15

# Creating and Managing Schedulers

- [Scheduler Overview on page 237](#)
- [Creating a Scheduler on page 238](#)
- [Managing Scheduler on page 240](#)

### Scheduler Overview

---

A scheduler allows a policy to be active for a specified duration. You can create a scheduler without linking it to a policy; such schedulers are applicable at the rule level. However, if you want a policy to be active during a scheduled time, you must first create a scheduler for that policy or link the policy to an existing scheduler. When a scheduler 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 scheduler, that schedule determines when the policy is active. When a policy is active, it can be used as a possible match for traffic. A scheduler lets you to restrict access to a resource, or remove a restriction to a resource, for a period of time.

A schedule uses the following guidelines:

- A scheduler can have multiple policies associated with it; however, a policy cannot be associated with multiple schedulers.
- A policy remains active as long as the scheduler it refers to is also active.
- You can configure a scheduler using one of the following scenarios:
  - A scheduler can be active during a single time slot, as specified by a start date and time, and a stop date and time.
  - A scheduler 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

- [Creating a Scheduler on page 238](#)

- [Managing Scheduler on page 240](#)

## Creating a Scheduler

A scheduler allows a policy to be activated for a specified duration. You can define a scheduler for a single or recurrent time slot during which a policy is active.

To create a scheduler:

1. From the left pane, select **Security Director > Firewall Policies > Scheduler**.

The main Scheduler page appears, as shown in [Figure 110 on page 238](#).

**Figure 110: Scheduler Main Page**

Name	Description	StartDate1	StopDate1	StartDate2	StopDate2	Schedules
TwoStartEnd_1		2012-12-02 00:00	2012-12-03 00:00			
SingleStartEnd_1		2012-12-02 00:00	2012-12-03 00:00			
TwoStartEnd-allday		2012-02-12 00:00	2012-03-12 00:00	2012-04-12 00:00	2012-08-12 00:00	MONDAY, Exclude=false, AllDay=true
TwoStartEnd-daily-FRIAllDay		2012-02-12 00:00	2012-03-12 00:00	2012-04-12 00:00	2012-08-12 00:00	DAILY, Exclude=false, AllDay=false, AllDay=true, startTime1=00:00, stopTime1=12:00, FRIDAY, Exclude=false, AllDay=true
TwoStartEnd-daily-exclude		2012-02-12 00:00	2012-03-12 00:00	2012-04-12 00:00	2012-08-12 00:00	DAILY, Exclude=false, AllDay=false, AllDay=true, startTime1=00:00, stopTime1=12:00, MONDAY, Exclude=true, AllDay=false
TwoStartEnd-daily-day-startstop		2012-02-12 00:00	2012-03-12 00:00	2012-04-12 00:00	2012-08-12 00:00	DAILY, Exclude=false, AllDay=false, AllDay=true, startTime1=00:00, stopTime1=12:00, TUESDAY, Exclude=false, AllDay=false, AllDay=true, startTime1=00:00, stopTime1=10:00
TwoStartEnd-daily-day-multiplestart		2012-02-12 00:00	2012-03-12 00:00	2012-04-12 00:00	2012-08-12 00:00	DAILY, Exclude=false, AllDay=false, AllDay=true, startTime1=00:00, stopTime1=00:00, startTime2=00:00, stopTime2=00:00

2. Click the plus sign (+) to create a new scheduler. The Create Scheduler window appears, as shown in [Figure 111 on page 239](#).

Figure 111: Create Scheduler

**Create Scheduler**

Name:  !

Description:

Start Date1:

Stop Date1:

Start Date2:

Stop Date2:

**Daily** Monday Tuesday Wednesday Thursday Friday Saturday Sunday

Day Option:

Start Time1:

Stop Time1:

Start Time2:

Stop Time2:

Create Cancel

3. Enter the name of the scheduler in the Name field. The maximum allowed characters are 63. The name must be a string beginning with a number or a letter. The name can have numbers, letters, hyphens, and underscores.
4. Enter the description in the Description field. The maximum allowed characters are 900. The description must be a string and must not contain special characters such as &amp;, &lt;, &gt;, and \n.
5. You can configure two sets of start and end dates and times for a single scheduler. For the first set of the schedule, enter the start date and time in the Start Date1 field, and enter the end date and time in the Stop Date1 field. You must enter the times in HH:MM format.  
  
For the second set of the schedule, enter the start date and time in the Start Date2 field, and enter the end date and time in the Stop Date2 field.
6. You can create a scheduler to be active daily or for any particular day(s) of the week. Select the **Daily** or **any day** option, and enter the start time in the Start Time field and the stop time in the Stop Time field. You must enter times in HH:MM:SS format.
7. Click **Create** to create a new scheduler.

**Related Documentation**

- [Scheduler Overview on page 237](#)
- [Managing Scheduler on page 240](#)

## Managing Scheduler

---

You can modify, delete, and clone a scheduler listed on the Scheduler main page.

To open the Scheduler page:

- Select **Security Director > Firewall Policies > Scheduler**.

The Scheduler page appears.

Right-click the scheduler to manage it, or select the required options from the Actions drawer.

You can perform the following tasks on the Scheduler page:

- [Modifying a Scheduler on page 240](#)
- [Deleting a Scheduler on page 240](#)
- [Find Scheduler Usage on page 241](#)
- [Show Unused Schedulers on page 241](#)

### Modifying a Scheduler

To modify a scheduler:

1. Select **Security Director > Firewall Policies > Scheduler**.

The Scheduler page appears.

2. Select the scheduler that you want to modify and click the pencil icon or right-click and select **Modify Scheduler**.

The Modify Scheduler page appears.

3. On the Modify Scheduler page, you can modify name, description, start and stop date, and time.
4. Click **Modify** to modify the scheduler.

### Deleting a Scheduler

To delete a scheduler:

1. Select **Security Director > Firewall Policies > Scheduler**.

The Scheduler page appears.

2. Select the scheduler that you want to delete, and click the X icon or right-click and select the **Delete Schedulers** option. A confirmation window appears before you can delete the scheduler.

3. Click **Delete** to delete the scheduler.

You can delete a single scheduler or multiple schedulers.

## Find Scheduler Usage

To find scheduler usage:

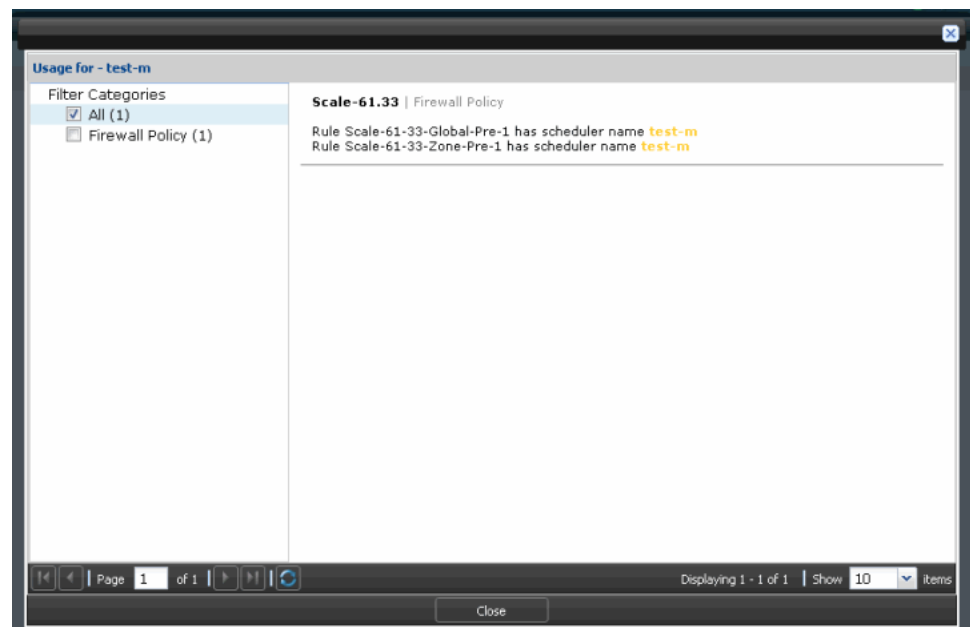
1. Select **Security Director > Firewall Policies > Scheduler**.

The Scheduler page appears.

2. Select the scheduler that you want to find the usage, right-click and select **Find Usage**.

The usage window appears, as shown in [Figure 112 on page 241](#).

**Figure 112: Scheduler Find Usage Window**



## Show Unused Schedulers

To show unused schedulers:

1. Select **Security Director > Firewall Policies > Scheduler**.

The Scheduler page appears.

2. From Actions, select **Show Unused**.

The unused schedulers which are not used for any policy are listed.

- Related Documentation**
- [Scheduler Overview on page 237](#)
  - [Creating a Scheduler on page 238](#)



# Creating and Managing Policy Profiles

- [Security Policy Profiles Overview on page 243](#)
- [Creating Policy Profiles on page 244](#)
- [Managing Policy Profiles on page 248](#)
- [Creating Template Definitions on page 249](#)
- [Managing Template Definitions on page 250](#)
- [Creating Templates on page 252](#)
- [Managing Templates on page 253](#)

## Security Policy Profiles Overview

---

You can use the Policy Profile Wizard to create an object that specifies the basic settings of a security policy. You can configure these basic settings using the Policy Profile Wizard:

- Log options
  - Log at session initiation
  - Log at the close of a session
  - Enable counting for the number of packets, bytes, and sessions that enter the firewall for a given policy
- Firewall authentication schemes
  - Pass-through authentication
  - Web authentication
  - Infranet authentication
- Traffic redirection options
  - No traffic redirection
  - Redirect Wx—Wx redirection for packets that arrive from the LAN
  - Reverse Redirect Wx—Wx redirection for the reverse flow of packets that arrive from the WAN
  - TCP-SYN Check and TCP Sequence Check—TCP session options for policy profile

When a policy profile is created, Junos Space creates an object in the Junos Space database to represent the policy profile. You can use this object to create security policies.

There are two Juniper Networks defined policy profiles:

- All logging enabled — All logging options are enabled. Logging is enabled at session initiation and the close of the session. Counters are also enabled to collect the number of packets, bytes, and sessions that enter the firewall for a given policy. The alarm thresholds are set to 100 bytes/second and 100 kilobytes/minute.
- All logging disabled — All logging options are disabled.



**NOTE:** You cannot modify or delete Juniper Networks defined policy profiles. You can only copy them and create new policy profiles.

---

**Related  
Documentation**

- [Creating Policy Profiles on page 244](#)
- [Managing Policy Profiles on page 248](#)

---

## Creating Policy Profiles

To create a security policy profile:

1. Select **Security Director > Firewall Policies > Policy Profiles**.

The Policy Profiles page appears with all the policy profiles. The first two policy profiles listed here are Juniper Networks defined policy profiles.

2. Click the plus sign (+) to create a new policy profile.

The New Policy Profile page appears, as shown in [Figure 113 on page 245](#).

Figure 113: New Policy Profile Page

3. Enter the name of the policy profile in the Name field.
4. Enter the description of the policy profile in the Description field.
5. In the Logging pane of the New Policy Profile page, configure the log options for this policy profile. You can configure the following log options:
  - a. If you want to log the events when the session is created, select the **Log at Session Init** check box.
  - b. If you want to log the events when the session is closed, select the **Log at Session Close** check box.
  - c. Enter the number of bytes to be logged per second in the Bytes/Second field.
  - d. If you want to enable counting, select the **Enable Count** check box.
 

If counting is enabled, counters are collected for the number of packets, bytes, and sessions that enter the firewall for a given policy
  - e. Enter the value of the count in the Kilobytes/Minute field.
6. Use the Authentication pane on the New Policy Profile page to provide authentication to clients. You can configure the following authentication options:
  - a. If you want to use Web Authentication, select **Web** in the Authentication Type drop-down menu and enter the hostname or IP address of the client used to perform Web authentication in the Client Name field.
  - b. If you want to use Pass Through Authentication, select **Pass Through** in the Authentication Type drop-down menu and enter the hostname or IP address of the client used to perform Pass Through authentication in the Client Name field.

- c. If you do not want to use any authentication, select **None** in the Authentication Type drop-down menu.
- d. If you want to use Infranet Authentication, select **Infranet** in the Authentication Type drop-down menu and enter the redirect URL in the Redirect URL field. You can also select the appropriate redirect options from the respective check boxes.
- e. If you want to create a user firewall authentication, select **User Firewall** in the Authentication Type drop-down menu.

Enter domain name in the Domain Name field, and access profile information in the Access Profile Name field.

- 7. Use the Advanced Settings section of the New Policy Profile page to configure the traffic redirection options for this policy profile, as shown in [Figure 114 on page 247](#).
  - a. If you want to use the Services Offload option in the Datacenter SRX Acceleration list, select this option.
  - b. If you do not want to take any action for destination address, select **None** from the Destination Address Translation list.
  - c. If you do not want to translate the destination address, select **Drop Untranslated** from the Destination Address Translation list.
  - d. If you do want to translate the destination address, select **Drop Translated** from the Destination Address Translation list.
  - e. If you want traffic to be redirected, select the **None** check box.
  - f. If you want to enable Wx redirection for packets that arrive from the LAN, select the **Redirect Wx** check box.
  - g. If you want to enable Wx redirection for the reverse flow of packets that arrive from the WAN, select the **Reverse Redirect Wx** check box.
  - h. You can enable TCP session options for a policy profile by clicking the **TCP-SYN Check** and **TCP Sequence Check** options.

Figure 114: Create Policy Profile-Advanced Settings

**Create Policy Profile**

Name:

Description:

Template:

**Logging** **Authentication** **Advanced Settings**

Datacenter SRX Acceleration: ☐ Services Offload

Destination Address Translation:

Redirect:

**TCP-Session Options**

☐ TCP-SYN Check

☐ TCP Sequence Check

**NOTE:**

- The update is committed only if these TCP session options are disabled globally. Otherwise, the update fails.
- If the update fails for logical systems, you must disable TCP session options for logical systems but not in the root devices.
- Any changes you make at the root device level or at the policy level are captured in the audit trail.
- When you import a device configuration, TCP session options are also imported, if they are enabled.
- When you export a policy, you can find the associated TCP session options under the Rule Options column.
- When you take a firewall policy snapshot, TCP session options are retained for possible future rollback.

8. Click **Create**.

The new security policy profile appears on the Policy Profiles page.

**Related  
Documentation**

- [Security Policy Profiles Overview on page 243](#)
- [Managing Policy Profiles on page 248](#)

## Managing Policy Profiles

---

You can delete, modify, or clone policy profile listed in the Policy Profiles page.

To open the Policy Profiles page:

- Select **Security Director > Firewall Policies > Policy Profiles**.

The Policy Profiles page appears.

You can right-click the policy profile to manage it.

You can perform the following tasks on the Policy Profiles page:

- [Deleting Policy Profiles on page 248](#)
- [Modifying Policy Profiles on page 248](#)
- [Cloning Policy Profiles on page 249](#)

### Deleting Policy Profiles

To delete a policy profile:

1. Select **Security Director > Firewall Policies > Policy Profiles**.

The Policy Profiles page appears.

2. Select the policy profile that you want to delete and select **Delete Policy Profiles** from the Actions drawer.

The Delete pop-up window appears.

3. Select the security policy profiles you want to delete and click **Delete**.



**NOTE:** You can also delete the policy profile by right-clicking the policy profile and selecting **Delete Policy Profiles**.

### Modifying Policy Profiles

To modify a policy profile:

1. Select **Security Director > Firewall Policies > Policy Profiles**.

The Policy Profiles page appears.

2. Select the policy profile that you want to modify, right-click, and select **Modify Policy Profile**.

The Modify Policy Profile page appears. You can modify all the fields on this window, except the Name field.

3. Make the appropriate changes to the security policy and click **Modify**.



**NOTE:** You can also modify the policy profile by right-clicking the policy profile and selecting **Modify Policy Profile**.

## Cloning Policy Profiles

To clone a policy profile:

1. Select **Security Director > Firewall Policies > Policy Profiles**.  
The Policy Profiles page appears.
2. Select the policy profile that you want to clone, right-click, and select **Clone Policy Profile**.  
The Clone Policy Profile page appears.
3. Make the appropriate changes to the security policy and click **Clone**.



**NOTE:** You can also clone the policy profile by right-clicking the policy profile and selecting **Clone Policy Profile**.

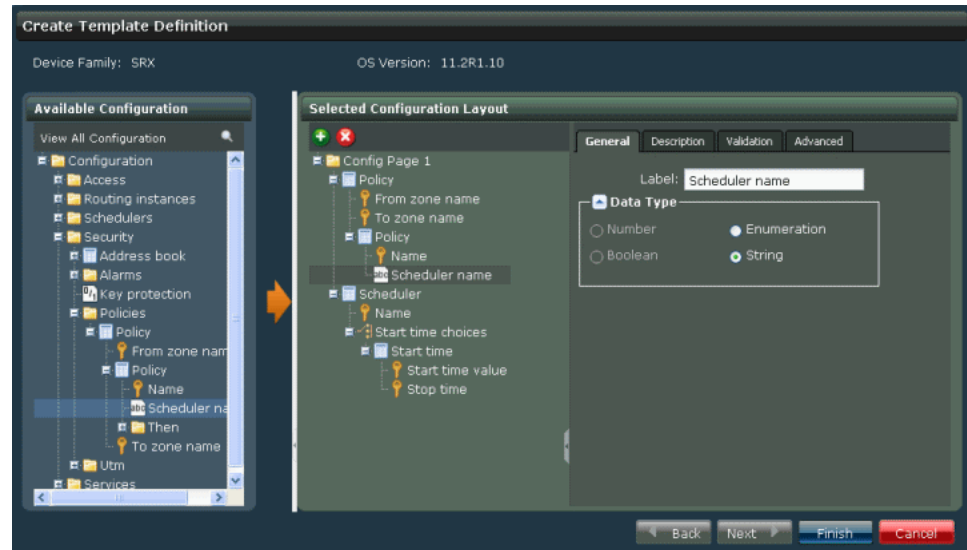
## Creating Template Definitions

To create a Template Definition:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage Template Definitions**.  
The Manage Template Definitions page appears. This page displays all the template definitions you have created.
2. Click the plus sign (+) to create the template definition.  
The Create Template Definition page appears.
3. Enter the name of the template definition in the Name field.
4. Enter a description for the template definition in the Description field.
5. Select the SRX Series schema version from the SRX Schema Version drop-down menu.
6. Click **Next**.  
This page displays two sections: the Available Configuration pane on the left and the Selected Configuration Layout pane on the right. The Available Configuration pane displays the different configuration nodes. The Select Configuration Layout pane displays a default rule with “\$FromZone” for source zone and “\$ToZone” for destination zone.
7. Select the rule from the configuration node you want to add in the template definition and click the right arrow.

8. Modify the rule in the Select Configuration Layout pane, as shown in [Figure 115 on page 250](#).

Figure 115: Create Template Definition Page



9. Click **Finish**.

The new template definition is created.



**NOTE:** Do not modify the existing From zone name, To zone name, and Policy fields. This is because the actual values are selected from the firewall rule where this template is applied and not from the Security Director Template Definition.

#### Related Documentation

- [Managing Template Definitions on page 250](#)

## Managing Template Definitions

You can delete, or modify template definitions listed in the Manage Template Definitions page.

To open the Manage Template Definitions page:

- Select **Security Director > Firewall Policies > Policy Profiles > Manage Template Definition**.

The Manage Template Definitions page appears.

You can right-click the template definition to manage it.

You can perform the following tasks on the Manage Template Definitions page:

- [Deleting Template Definitions on page 251](#)
- [Modifying Template Definitions on page 251](#)

## Deleting Template Definitions

To delete a template definition:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage Template Definition**.

The Manage Template Definitions page appears. This page displays all the template definitions you have created.

2. Select the template definition you want to delete, right-click and select **Delete Template Definitions**.



**NOTE:** You can also delete the template definition by right-clicking the template definition and selecting **Delete Template Definitions**.

## Modifying Template Definitions

To modify a template definition:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage Template Definitions**.

The Manage Template Definitions page appears. This page displays all the template definitions you have created.

2. Select the template definition you want to modify, right-click and select **Modify Template Definition**.

The Modify Template Definitions page appears. You can make the modifications on this page.



**NOTE:** You can also modify the template definition by right-clicking the template definition and selecting **Modify Template Definition**.

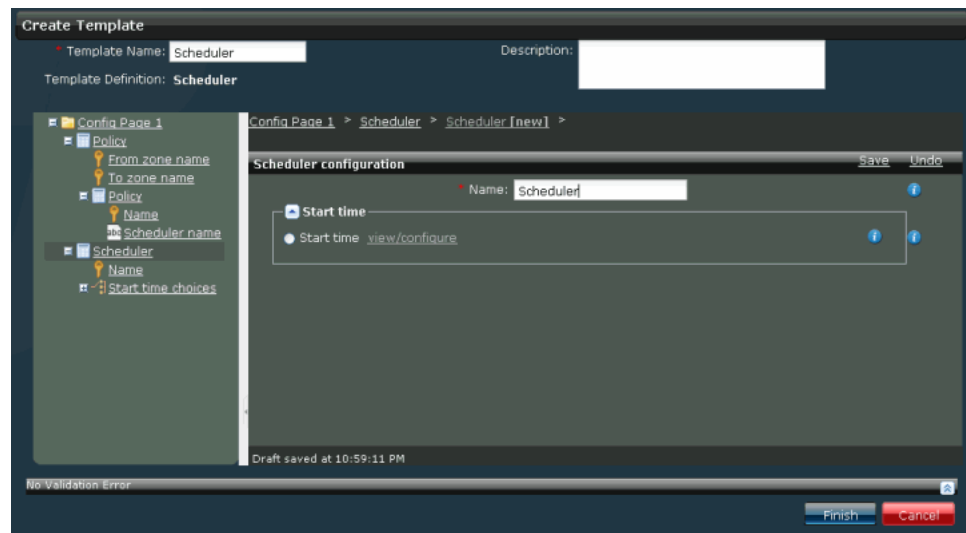
3. Click **Modify**.

## Creating Templates

To create a template:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage SD Templates**.  
The Manage SD Templates page appears. This page displays all the templates you have created.
2. Click the plus (+) sign to create a policy template.  
The Select Template Definition page appears. You can create a template on this page.
3. Select an appropriate template definition and click **Next**.  
You can create a template on this page.
4. Enter the name of the template in the Template Name field.
5. Enter a description for the template in the Description field.
6. Select the configuration node from the left hand pane.
7. Select the appropriate value in the configuration node.
8. Modify the rule in the right pane, as shown in [Figure 116 on page 252](#).

**Figure 116: Create Template Page**



9. Click **Finish**.



**NOTE:** For logical systems, you must not use policy templates for defining policy shared objects. These objects must be defined using either Platform templates or Config Editor. You can subsequently refer the created objects in the rule options of the policy template.

- Related Documentation**
- [Managing Templates on page 253](#)

## Managing Templates

You can delete or modify templates listed on the Manage SD Templates page.

To open the Manage SD Templates page:

- Select **Security Director > Firewall Policies > Policy Profiles > Manage SD Templates**.

The Manage SD Templates page appears.

You can right-click the template to manage it.

You can perform the following tasks on the Manage SD Templates page:

- [Deleting Templates on page 253](#)
- [Modifying Templates on page 253](#)

## Deleting Templates

To delete a template:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage SD Templates**.

The Manage SD Templates page appears. This page displays all the templates you have created.

2. Select the template you want to delete, right-click, and select **Delete Templates**.



**NOTE:** You can also delete the template by right-clicking the template and selecting **Delete Templates**.

## Modifying Templates

To modify a template:

1. Select **Security Director > Firewall Policies > Policy Profiles > Manage SD Templates**.

The Manage SD Templates page appears. This page displays all the templates you have created.

2. Select the template you want to modify, right-click, and select **Modify Template**.

The Modify Templates page appears. You can make the modifications on this page.



**NOTE:** You can also modify the template by right-clicking the template and selecting **Modify Template**.

3. Click **Modify**.



## PART 8

# Configuring VPNs

- [Creating and Managing IPsec VPNs on page 257](#)
- [Creating and Managing Extranet Devices on page 287](#)
- [Creating and Managing VPN Profiles on page 291](#)



# Creating and Managing IPsec VPNs

- [IPsec VPN Overview on page 257](#)
- [Creating IPsec VPNs on page 259](#)
- [Importing an Existing VPN Environment of SRX Series Devices on page 273](#)
- [Publishing IPsec VPNs on page 281](#)
- [Managing IPsec VPNs on page 282](#)

## IPsec VPN Overview

---

You can create site-to-site, hub-and-spoke, and full-mesh VPNs in the VPN Creation page. All VPNs in the system appear in the Tabular view. The left pane of the Tabular view displays the VPNs, and the right pane of the Tabular view displays the devices used for the respective VPN. If you want to use a custom VPN profile, you must configure a VPN profile before creating a VPN.

You can configure the following parameters for an IPsec VPN:

- Endpoints for a site-to-site VPN and full-mesh VPN
- Spokes and hubs for a hub-and-spoke VPN
- External Interface, Tunnel Zone, and Protected networks/zones for each device
- Routing settings
- VPN endpoint configuration

You can also customize endpoint-specific settings like VPN Name, IKE ID, and profile for each tunnel.

After the VPN configuration is saved, you can provision this VPN on the security devices.



NOTE: Security Director views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.

Security Director ensures that the tunnel interfaces are exclusively assigned to the individual logical systems of a device. No tunnel interface is assigned to more than one logical system of the same device.



NOTE:

- Only route-based VPNs are supported for the logical systems. Policy-based VPNs are not supported.

Proxy ID is supported for both route-based and policy-based VPNs.

In Security Director, route-based VPNs support OSPF, and RIP routing along with static routing. Static routing requires that the administrators specify the list of host or network addresses at each site is part of the VPN. For example, in a retail scenario, where thousands of spokes can be part of a VPN, the static routing approach generates a huge configuration at each device. Static routing requires the administrator to manually configure each route. Problems occur as the infrastructure changes or when the administrator does not have access to the addresses for the protected network. Keeping routes up-to-date manually creates tremendous overhead.

Security Director supports dynamic routing in VPN addressing. Security Director supports the dynamic routing protocols Open Shortest Path First (OSPF) and Routing Information Protocol (RIP). Security Director simplifies VPN address management by enabling the administrator to export static routes to a remote site over a tunnel, allowing the static route networks to participate in the VPN. However, only devices on the hub side can export static default routes to the device side. Devices at the spoke side cannot export static default routes over a tunnel.

If you select OSPF or RIP export, the OSPF or RIP network outside the VPN network are imported into VPN network through OSPF or RIP routing protocols.



---

**NOTE:**

- All host-inbound-traffic-system-service settings are copied from zone to interfaces.
  - If system-service is configured on the interface level, only IKE is configured, and no zone-level configuration is taken into account.
  - If any-service or IKE is configured at the zone level, no configuration is made at the interface level.
  - The host-inbound-traffic system-service except configuration settings, are also copied from the zone-level to the interface level, if there is no system-service configuration on the interface level.
- 

**Related Documentation**

- [Creating IPsec VPNs on page 259](#)
- [Managing IPsec VPNs on page 282](#)
- [Publishing IPsec VPNs on page 281](#)
- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

---

## Creating IPsec VPNs

---

1. [Creating IPsec VPNs on page 260](#)

## Creating IPsec VPNs

1. In the left pane, under Security Director application, select **VPN**.

The VPN Tabular view appears, as shown in [Figure 117 on page 260](#). VPNs from only the current domain are listed on the landing page.

Figure 117: VPN Landing Page

Device	External Interface	Tunnel Zone	Protected Zone/Network	Routing Instance	IP Address	Proxy ID
10-205-119-1...	fe-0/0/1.0 (10.1.1.2.9abc-100)	VPN	Zones Template_1_Zone_1	tst-custom-0	10.1.1.2	10.205.119.105

2. In the VPNx pane, click the plus sign (+) to create a VPN.

The Create VPN page appears, as shown in [Figure 118 on page 260](#).

Figure 118: Create VPN Page

Name:

Description:

Tunnel Mode: ☒ Route Based ☐ Policy Based ☐ Multi-ProxyID

Type: ☒ Site To Site ☐ Full Mesh ☐ Hub And Spoke

VPN Profile:

Preshared Key: ☒ Auto-generate ☐ Manual

☒ Generate Unique key per tunnel

Navigation:

3. In the Name field, enter a name for the new VPN.
4. In the Description field, enter a description for the new VPN.

5. Select the Tunnel Mode as either Route Based or Policy Based.
6. If you have selected Route Based:
  - a. Security Director provides an option to configure Multi-Proxy ID, also known as Traffic Selector, for route-based VPNs. To configure multi-proxy ID, select the **Multi-ProxyID** check box.
  - b. Select the option button next to the type of VPN you want to create. For the Hub and Spoke type, you can select an option Auto VPN, also known as Zero Touch Hub (ZTH). This is a SRX Series feature which enables the administrators to add or remove spoke devices dynamically without performing any configuration changes on the hub devices. The Auto VPN option is supported on devices running Junos OS Release, 12.1-X45. This Option is applicable only for the route-based VPNs and only with PKI certificate-based authentication. Because this feature is supported only on devices running Junos OS Release, X45, all other devices will not be available for Spoke or Hub selection.

If the multi-proxy ID option is selected, you cannot select ZTH option for Hub and Spoke.



**NOTE:** The Auto VPN feature is not supported on logical systems and the extranet devices. Therefore they are filtered out from device association during Auto VPN design or modification.

- c. Select the VPN profile from the VPN Profile menu. You can create certificate-based VPNs by choosing the VPN profiles created with an authentication type of either RSA signature or DSA signature. If you select a VPN profile with certificate-based authentication, the preshared key options are automatically hidden. You can synchronize the certificate for any device. For more details, see [“Updating Devices with Pending Services” on page 567](#).

You can use the available Tooltip view to see information about the VPN profiles. To see the tooltip for a VPN profile, move the mouse over the profile for which details are required. The tooltip displays the following high-level information, as shown in [Figure 119 on page 262](#).

- Phase 1
  - Authentication
  - Mode
  - Proposal(s)
- Phase 2
  - Proposal(s)
  - Perfect Forward Secrecy

Figure 119: VPN Profile Tooltip

**VPN Wizard**

Name:

Description:

Tunnel Mode: ☒ Route Based ☐ Policy Based ☐ Multi-ProxyID

Type: ☒ Site To Site ☐ Full Mesh ☐ Hub And Spoke

VPN Profile:

Preshared Key: ☒ Auto-generate ☐ Manual

☒ Generate Unique key per tunnel

**VPN Profile Details**

Name: MainModeProfile  
Description: Predefined Main mode profile with Standard proposal set

Phase1 Settings	Phase2 Settings
Mode: Main	Proposal: Predefined
IKE Id: P Address	ProposalSet Type: Standard
Authentication Type: Preshared Key	Perfect Forward Secrecy: None
Proposal: Predefined	Establish tunnel immediately: false
ProposalSet Type: Standard	Enable VPN Monitor: false
Enable NAT Traversal: true	DF bit: None
Keep Alive Interval (secs): 10	Idle time(secs): 60
Enable DPD: true	Install time: 1
Always Send DPD: false	Enable Anti Replay: false
DPD Interval (secs): 10	
DPD Threshold: 5	

Previous Next Cancel



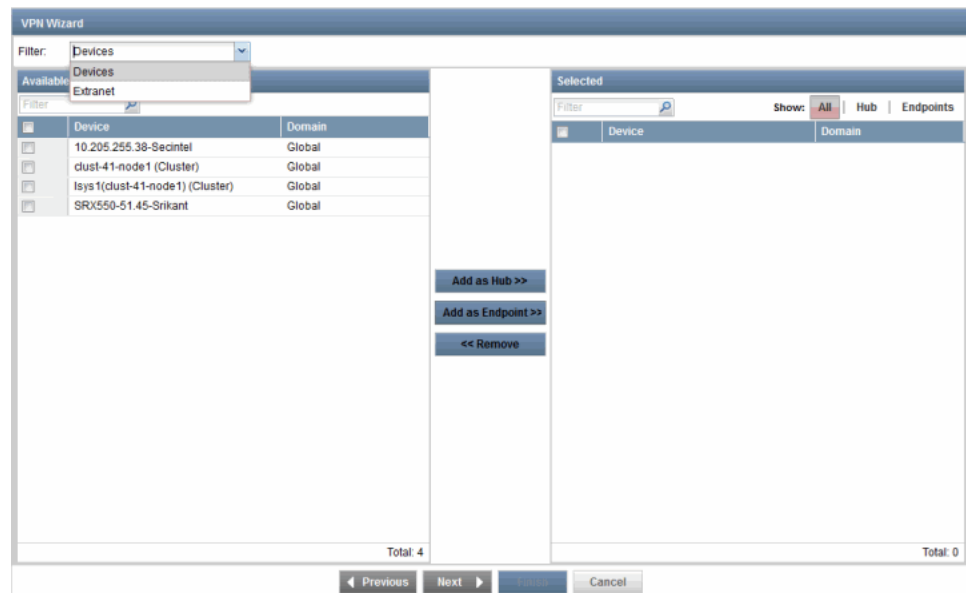
**NOTE:** If you choose to create a full-mesh VPN, you can choose only the MainModeProfile as the VPN profile.

- d. Select the option button next to the type of preshared key you want to use.
  1. If you select Auto-generate as the option for preshared key, select the Generate Unique key per tunnel check box to generate a unique key per tunnel, as shown in [Figure 118 on page 260](#). If you select only the auto-generate option, Security Director generates a single key for both the tunnels.
  2. If you select Manual as the option for the preshared key, enter the manual key in the Manual Key field.
- e. Click **Next**.

This page displays the Available and Selected panes.

- f. Select the device from the Available column, and click **Add as Endpoint**, as shown in [Figure 120 on page 263](#).

Figure 120: Create VPN: Add as Endpoint Page



**NOTE:** All the devices are auto filtered based on the mapping Junos Schema.

All devices from the current and child domains, with view parent enabled, are listed in the Available column. Devices from the child domain with view parent disabled, are not shown.

If the Multi-ProxyID option is selected, the following filter criteria are applied for the device selection:

- SRX Series devices mapped with older than 12.1X46 junos-es schema version are not shown.
- Logical systems are not shown.
- Routing option is not applicable.

g. Click **Next**.

h. Select the interface type in the Tunnel Settings pane.

- If you select **Numbered** as the Tunnel setting, enter the IP subnet in the IP Subnet field.

For the multi-proxy ID configuration, the Numbered tunnel option is hidden for Hub and Spoke and Full Mesh VPNs, because the multipoint is not supported with multi-proxy ID.

i. Select the routing option in the Routing options pane. If you select **OSPF**, the following check boxes are available:

- Export Static Routes—To export static routes.

- Export RIP Routes—To export RIP routes.
- Area—Numeric field where you enter the area ID.

If you select **RIP**, the following check boxes are available:

- Export Static Routes—To export static routes.
- Export OSPF Routes—To export OSPF routes.

If you select **Static Routing**, the following check box are available

- Allow spoke to spoke to communication—To enable spoke-to-spoke communication with static routes. You can enable this option only for a hub-and-spoke VPN with static routing when you create or modify the VPN. By default, this option is not checked, and you can check or uncheck this option during the modify workflow.
- Export Static Routes—To export static routes.
- Export RIP Routes—To export RIP routes.
- Export OSPF Routes—To export OSPF routes.

The routing options are hidden for the multi-proxy ID configuration,. You cannot select any routing options.

- j. In the Global Settings pane, under Endpoint Configurations, enter the external interface in the External Interface field.
- k. In the Global Settings pane, under Endpoint Configurations, enter the tunnel zone in the Tunnel Zone field.
- l. In the Global Settings pane, under Endpoint Configurations, enter the zone type in the Protected Network Zone field.

If you have chosen to create a hub-and-spoke VPN, you will see Hub Configuration and Spoke Configuration. Enter the appropriate values in the External Interface, Tunnel Zone, and Protected Network Zone fields in these panes, as shown in [Figure 121 on page 265](#).

The tunnel is shared accordingly based on the value specified for number of spoke devices per tunnel interface. The network specified in IP Subnet field is further subnet.

Figure 121: Create VPN: Hub and Spoke Configuration

The screenshot shows the 'VPN Wizard' configuration interface. It is divided into three main sections: Tunnel Settings, Route Settings, and Global Settings.

- Tunnel Settings:** The 'Interface Type' is set to 'Unnumbered' (radio button selected).
- Route Settings:**
  - 'Routing Options' are set to 'Static Routing' (radio button selected).
  - 'Allow spoke to spoke communication' is checked.
  - 'Area ID' is set to '0'.
  - 'Max Retransmission Time' is set to '50'.
  - There are checkboxes for 'Export Static Routes', 'Export RIP Routes', 'Export OSPF Routes', and 'Export Static Routes' (repeated).
  - 'No Routing' is also an option under Routing Options.
- Global Settings:**
  - A message states: 'Please select default values to be used for all devices in VPN. Per-device settings can be modified in the next step.'
  - A table with three columns: 'Type', 'External Interface', and 'Protected Network Zone'.

The table in Global Settings has two rows: 'Hub' and 'Spoke'. Each row has three cells, each containing a 'Click to configure...' link.

At the bottom of the wizard, there are navigation buttons: 'Previous', 'Next', and 'Cancel'.



**NOTE:** Upgrading a Full Mesh, and Numbered VPN with number of peer devices per tunnel value is not available. This value is reset to All and you must modify Tunnel Settings or Route Settings to reflect this change.

Upgrading the Hub And Spoke Numbered VPN with number of peer devices per tunnel value is available. But this might not work in static routing option because of the routing behavior with multiple tunnels having same subnet. You must modify the Tunnel Settings to reflect the subnet split enhancement feature added in Security Director Release 12.2.

These two scenarios are true only when you upgrade Security Director from Release 12.1 to Release 12.2.

- m. For the certificate-based VPNs, another Certificate column appears, displaying the certificate information. Under the Certificate column, you can choose one of the certificate names available from the device. The same certificate is used for all devices. If the certificate specified does not exist in some of the devices, you can choose a device-specific certificate in the next step, as shown in [Figure 122 on page 266](#). If a certificate is not configured, an error message appears.
- n. If you have selected **Static Routing**, enter the values in the External Interface, Tunnel Zone, and Protected Network Zone fields for the type Endpoint.
- o. If you have selected **No Routing**, enter the external interface in the External Interface field, and tunnel zone in the Tunnel Zone field for the type Endpoint.
- p. You can configure the custom routing instance for every device level, as shown in [Figure 122 on page 266](#). This is an optional field and is blank by default. This option

is available only for route-based VPNs (for example, static routing, no routing, and the dynamic protocols (OSPF and RIP)). You can add the routing instance while creating a new VPN or modifying an existing VPN.

The Global Settings pane does not include an option for selecting the routing instance. You must manually select the routing instance for each endpoint in the tabular view.

- q. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in [Figure 122 on page 266](#). The page displays error indicators if the options you have configured do not map to the device. You can also click the **Show all Errors** check box to view all errors in the configuration. If errors are present, you must modify the configuration to eliminate them before you can proceed to the next step.

**Figure 122: Create VPN Page Showing Custom Routing Instance Option**

Device	External interface	Tunnel Zone	Protected Zone/Network	Routing Instance
10-205-119-1...	fe-0/0/1.0 (109.1.12.9abc:109)	VPN	Zones Template_1_Zone_1	test-custom-ri
105-Router-S...	ge-0/0/0.0 (10.205.119.105)	VPN	Addresses 106.2.2.0-24	test-custom-ri



**NOTE:** For the multi-proxy ID configuration, the Protected Zone/Networks address is selected as Traffic Selectors.

- r. Click **Finish**.

When the multi-proxy ID is selected, the single Proxy ID column is hidden. Because, you cannot have both multi-proxy ID and single proxy-ID existing together. At the tunnel level, you can select the required local or remote proxy ID pair in the Traffic Selector column. However, at the global level, the Protected Zone/Network address is the traffic selector.

If the traffic selectors are configured at one tunnel end point level, automatically the same is configured on the corresponding remote end point however, the local IP and remote IP values are swapped for the remote end point.



**NOTE:** You can customize the IKE address and local or remote IKE ID for preshared key based VPNs. By default, the IKE address chooses the External Interface IP address. The IKE address can be modified to assign a different address. The Main Mode Profile is enhanced to support IKE ID types such as IP Address, hostname and user-at-hostname similar to Aggressive mode. With this you can modify the IKE ID of each endpoint in the VPN.

7. If you have selected Policy Based:
  - a. The only Type option available is Site To Site.
  - b. Select the VPN profile from the VPN Profile menu.



**NOTE:** If you choose to create a full-mesh VPN, you can choose only the Main mode profile as the VPN profile.

- c. Select the option button next to the type of preshared key you want to use.
  1. If you select **Autogenerate**, select the **Generate Unique key per tunnel** check box to generate a unique key per tunnel.
  2. If you select **Manual**, enter the manual key in the **Manual Key** field.
- d. Click **Next**.

The page displays the Available and Selected panes.

- e. Select the device from the **Available** column, and click **Add as Endpoint**, as shown in Figure 123 on page 267.

**Figure 123: Create VPN Policy-Based—Add as Endpoint Page**

Device	Domain
10.205.255.38-Secintel	Global
dust-41-node1 (Cluster)	Global
SRX550-51.45-Srikant	Global

f. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in [Figure 124 on page 268](#). The page displays error indicators if the options you have configured do not map to the device. You can also click the **Show all Errors** check box to view all errors in the configuration. If errors are present, you must modify the configuration to eliminate them before you can proceed to the next step.

Select the external interface for the device from the list. For the certificate-based VPNs, select the certificate in the Certificate column.

**Figure 124: Create VPN Page—External Interface Selection**

The screenshot shows the 'VPN Wizard' window with the 'Endpoint Setting' tab selected. It features a table with two columns: 'Device' and 'External Interface'. The table lists two devices: '10-205-119-1...' with interface 'lo0.0 (9.9.9.9)' and '105-Router-S...' with interface 'ge-0/0/0.0 (10.205.119.105)'. The second row is highlighted. Above the table is a 'Show all errors' checkbox and a 'Filter Devices' search bar. At the bottom, there are navigation buttons: 'Previous', 'Next', 'Finish', and 'Cancel'. The status bar at the bottom right indicates 'Displaying 1 - 2 of 2'.

Device	External Interface
10-205-119-1...	lo0.0 (9.9.9.9)
105-Router-S...	ge-0/0/0.0 (10.205.119.105)

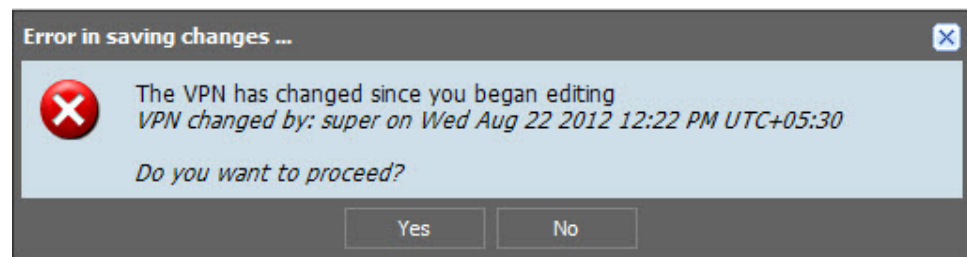
g. Click **Finish**.

Whenever you make any changes to the VPN, you will get an option to enter a comment before saving the VPN. You can enable or disable this option in Platform > Administration > Applications. To enable this option, right-click **Security Director**, and select **Modify Security Director Settings** option. Under Applications, select the **Enable save comments for policies** check box. By default, this option is disabled.

Entering comments is not mandatory but all entered comments are audit logged.

**NOTE:**

- In addition to the VPNs created and managed from Security Director, you can also select the IPsec VPNs available in the imported device. Security Director created VPNs will be bold in text to differentiate from the imported VPNs.
- You cannot delete a policy-based VPN if the VPN is used in a firewall rule.
- Policy-based VPN is not supported on SRX Series devices with logical systems. Security Director does not show logical systems when you select the policy-based VPN.
- If the same VPN is edited by multiple users, the following warning message is received to over write the changes saved by other users, as shown in [Figure 125 on page 269](#).

**Figure 125: VPN: Concurrent Save Error Message**

- If you create a policy-based VPN in the Global domain using child devices, you can select such VPN for tunnel action in a policy.

**Inline Addition of a New VPN Object**

To perform an inline addition of the new VPN object:

1. Click the **Protected Zone/Networks** column for the available device. The VPN Policy Inline Object Creation page appears, as shown in [Figure 126 on page 270](#). The page lists the zone or networks available for creating the VPN object. In this window, you can select all devices listed in the Available column by selecting **Page** and copying them to the Selected column. If you want to clear all selected devices, click **None**.

Figure 126: Inline Address Object Creation Page

The screenshot shows the 'Address' tab selected. The 'Available' list contains the following items:

Address	Type
10.159.4.0/24 (10.159.4.0/24)	Global
144.201.76.32 (144.201.76.32)	Global
Addr-66.0.192.112/28 (66.0.192.112/28)	Global
Addr-66.184.206.216 (66.184.206.216)	Global
ADDR-GROUP-v4 (group)	Global
bmtnwxr04-158.31.215.6 (158.31.215.6)	Global
bmtnwxr10-158.31.215.10 (158.31.215.10)	Global
bmtnwxrtemn1-158.31.215.5 (158.31.215.5)	Global

Total: 198

The 'Selected' list is empty. Total: 2

Below the lists are checkboxes for 'Host', 'Network', 'Range', and 'Other'. At the bottom are 'Ok' and 'Cancel' buttons.

2. Click the plus sign (+) to create the new address object.
3. Click **Create** to create the object, or click **Cancel** to discard the changes.

### Creating a Address Group

To create address group:

1. Click the second plus sign (+) to create the new address group. [Figure 127 on page 270](#) shows the page that appears.

Figure 127: Inline Address Group Creation for VPN Object

The screenshot shows the 'Address' tab selected. The 'Create Address Object' section has 'Object Type' set to 'Address Group'. The 'Name' field is empty and has a red error icon. The 'Description' field is empty. The 'Addresses' list contains the following items:

Address	Type
10.159.2.0/25 (10.159.2.0/25)	Global
10.159.3.0/24 (10.159.3.0/24)	Global
10.159.4.0/24 (10.159.4.0/24)	Global
144.201.76.32 (144.201.76....)	Global
Addr-66.0.192.112/28 (66.0....)	Global
Addr-66.184.206.216 (66.18....)	Global

Total: 211

Below the 'Addresses' list are checkboxes for 'Host', 'Network', 'Wildcard', 'Range', and 'Other'. At the bottom are 'Create' and 'Cancel' buttons.

2. Enter the name of an address group in the Name field.
3. In the Addresses field, you can select all addresses available in the Available column or select few addresses to create a new address group.
4. Click **Create** to create the address group or **Cancel** to discard the changes.

## Creating Auto VPN

Auto VPN, also known as Zero Touch Hub (ZTH), is an SRX Series feature that enables administrators to add or remove spoke devices dynamically without performing any configuration changes on the hub devices. Security Director supports the design and provisioning of Auto VPN on devices running Junos OS Release 12.1X45. The Auto VPN option is available only to route-based VPNs with PKI certificate-based authentication. Because Auto VPN is supported only on devices running Junos OS Release 12.1X45, all other devices will not be available for spoke or hub selection.



**NOTE:** The Auto VPN feature is not supported on logical systems or extranet devices. Therefore, these systems and devices are filtered out from device association during Auto VPN design or modification.

To create a auto VPN:

1. In the VPN Wizard window, select Tunnel Mode as Route Based and Type as Hub and Spoke.
2. Select Auto VPN check box that is available below the Hub and Spoke radio button.
3. For the Auto VPN selection, the VPN Profile lists only RSAPProfile.
4. Click **Next**.
5. Select the devices for Hub and Endpoint. In this device selection page, a validation is performed to filter out the following type of devices:
  - SRX Series devices which do not support Auto VPN feature (devices running versions earlier to Junos OS Release 12.1X45).
  - Logical systems
  - Extranet devices
6. Click **Next**.
7. Enter the IP subnet in the IP Subnet field.
 

In the Tunnel Settings, only numbered Interface Type is supported. Unnumbered tunnel type option is not available.
8. In the Route Settings section, select the required routing options such as OSPF, RIP, or No Routing.
9. In Global Settings sections, there are 2 new columns available for Auto VPNs such as Group IKE and Certificate. The Group IKE column is applicable only for hub devices.
10. Click **Certificate** column and select the required certificate from the drop-down menu.

Under the Certificate column you can choose any one of the certificate names available from the device. The same certificate is used for all other devices. If the specified certificate does not exist on some of the devices, a device specific certificate can be chosen in the later steps of VPN creation. An error message is displayed if you do not configure the certificate.

11. Click **Group IKE** column to enter the group IKE ID. A free text editor is displayed based on the IKE ID type chosen in the profile.

For IKE ID types FQDN and UFQDN, a normal text field type editor is displayed, whereas for DN KE ID type, a separate editor is provided to enter the container and wildcard informations.

In the Container and WildCard input fields, you can specify the values for CN ( Common Name) and OU ( Organization). The Container field can take multiple values for each field type, but the WildCard field can take only one value for each field.

12. Click **Next**.

The page that appears gives you a preview of the values entered for the Auto VPN. The page displays errors indicators if the options you have configured do no map to the device. You can also edit the values configured for certificate and group IKE ID. The Group IKE field is a mandatory field.

13. Click **Finish**.

The VPN Profile, Preshared Key, and Peer Device columns are hidden for Auto VPNs because they are not applicable. You cannot edit IKE Id field for DN IKE ID type, but you can edit for Hostname IKE ID type.

The new column IKE Address, which is available during creation of new VPN, lists the selected external interface IP address; this is the default value, which you can modify. The Main Mode profile supports IKE ID types such as IP addresses, hostname, and user-at-hostname, similar to Aggressive mode. Using these configuration options, you can modify the IKE ID of each endpoint in the VPN.

Security Director permits you to save VPNs that contain errors. Warnings messages are displayed for VPNs that contain errors, but you can proceed to save such VPNs as drafts. You cannot publish VPNs that are in the draft state. The tooltip for the VPN shows the state as draft; because it is a draft, the tooltip does not show the publish option.

Proxy ID is supported for both route-based and policy-based VPNs. Security Director supports only a single proxy ID. You can input a local (proxy) ID at a per device level in the modify workflow only, as shown in [Figure 117 on page 260](#). Security Director generates the local proxy ID and remote proxy ID at every endpoint settings level. By default, the **service** parameter for proxy ID is set to Any.

Proxy ID is an optional setting. You can choose to configure proxy IDs for a few devices only; Security Director does not generate a warning if you do not configure a proxy ID. The proxy ID setting is generated if both ends have a proxy ID configured. You can configure 0.0.0.0/0 as Proxy ID. By default, proxy ID is configured as Any.



**NOTE:** In the dual hub scenario, If there are two paths available to reach a particular network, you have an option to set the metric value for each path and set the priority. Based on the metric value, you can select the appropriate path to reach the network. This option is available only at the hub side and is available for both static and dynamic routing.

---



**NOTE:** When a default proposal definition is used (standard, compatible, and basic) in VPN profile for extranet devices, you might not be able to find out what is required for an extranet device. You must use custom proposals if you select an extranet device as an endpoint in VPN.



**NOTE:** When the Autogenerate preshared key option is used for VPN design that involves the extranet device as endpoint, you can view SRX Series device tunnel endpoint settings, edit and unmask the key, and save the key as a reference.

#### Related Documentation

- [IPsec VPN Overview on page 257](#)
- [Publishing IPsec VPNs on page 281](#)
- [Managing IPsec VPNs on page 282](#)
- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

## Importing an Existing VPN Environment of SRX Series Devices

Junos Space Security Director lets you import of your existing large and complex VPN configurations into Security Director. You do not have to recreate the same VPN environment to allow Security Director to manage it. During the VPN import, all VPN-related objects are also imported along with the VPN.

Security Director supports importing the following VPN configuration:

- Site-to-site, hub-and-spoke, and full-mesh topologies
- Preshared key-based VPNs
- Certificate-based VPNs, except AutoVPN
- Route-based and policy-based VPNs
- OSPF
- RIP
- Single proxy ID
- Traffic selectors
- Static route configurations that identify the protected network objects
- Static route configurations with spoke-to-spoke communication enabled
- Numbered and unnumbered tunnel interface types

- Route-metric configuration
- Static route configuration from a virtual router

To import a VPN:

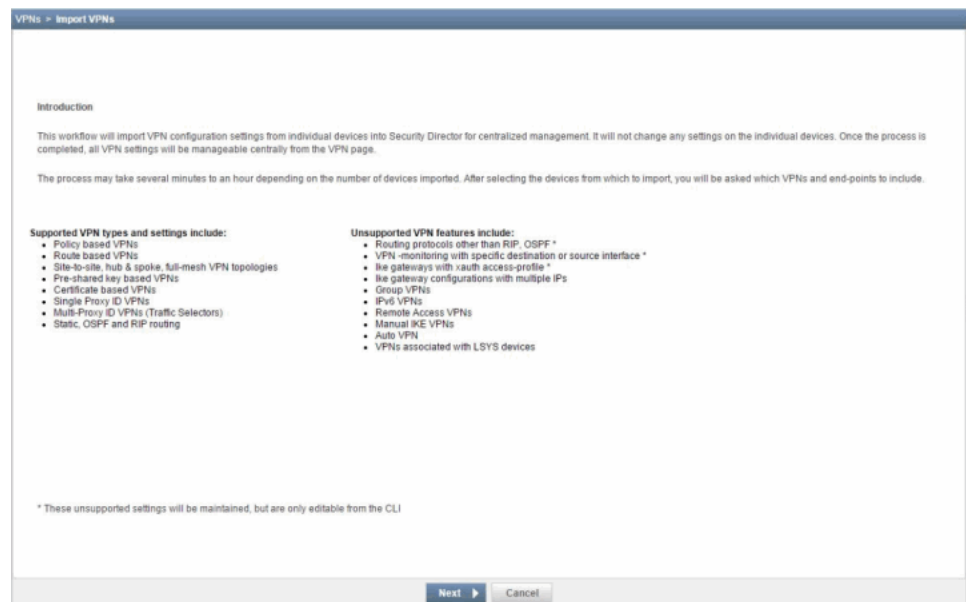
1. In the left pane, under the Security Director application, select **VPNs**.

The VPN Tabular view appears.

2. In the VPNs pane, from the Actions, select **Import VPN**.

You can also import a VPN from the Security Director Devices workspace. The Import VPN page appears, as shown in [Figure 128 on page 274](#). This workflow imports VPN configuration settings from the individual devices into Security Director for centralized management. It does not change any settings on the individual devices. Once the process is completed, all VPN settings are manageable centrally from the VPN page.

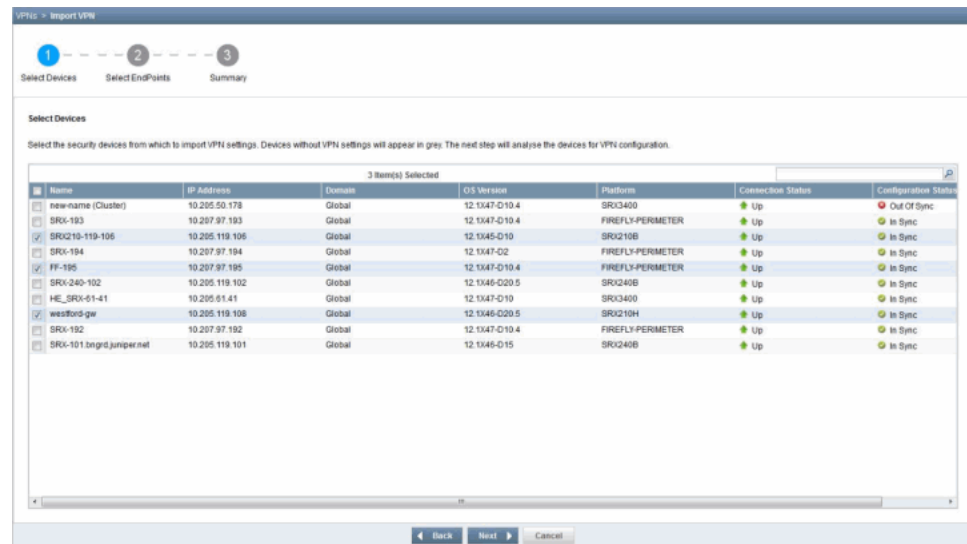
**Figure 128: Import VPN**



3. Click **Next**.

The Select Devices page appears, as shown in [Figure 129 on page 275](#).

Figure 129: Select Devices

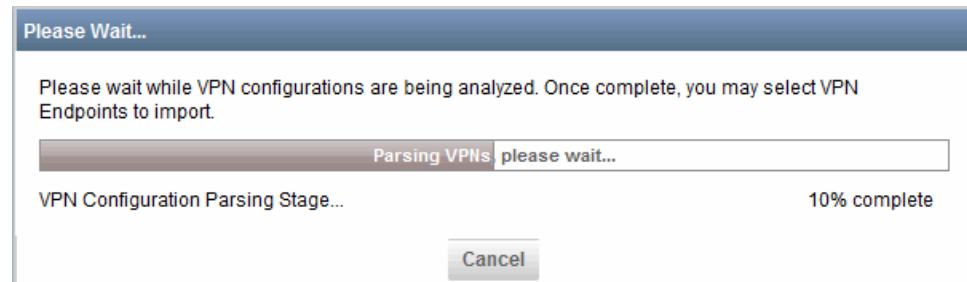


You can select one or more devices from which the VPN configuration must be imported. The filter option enables you to perform the free text search on the device name, IP address, and device platform.

4. Select the security device to import its VPN settings. Click **Next**.

A progress bar appears showing the analysis of the device configurations, as shown in [Figure 130 on page 275](#).

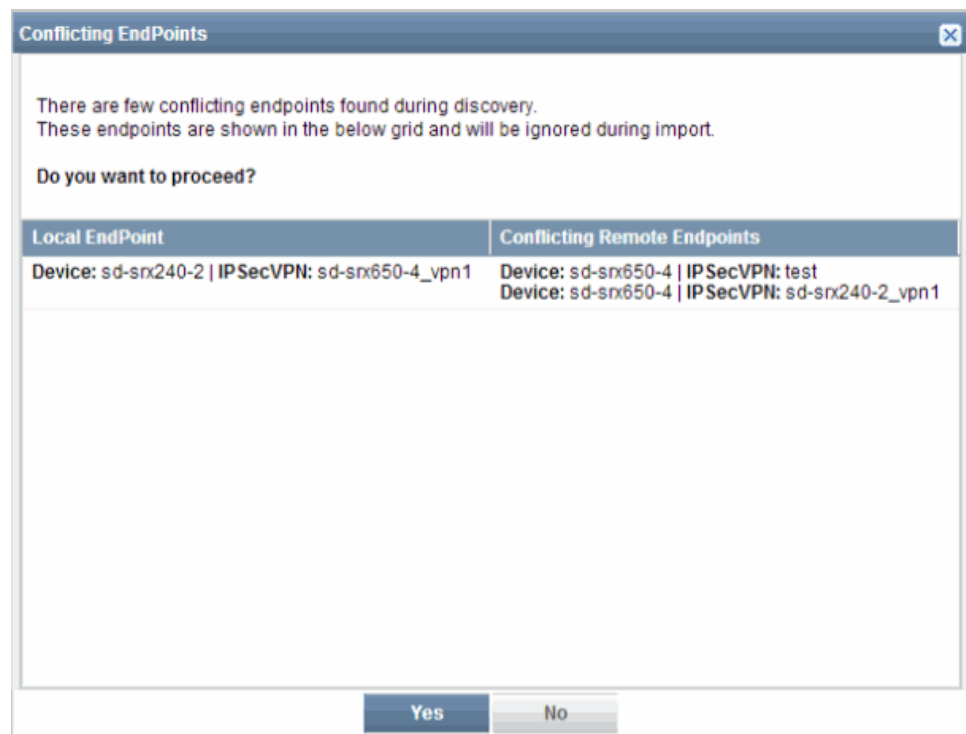
Figure 130: VPN Configuration Progress Bar



You can click **Cancel** to cancel the action.

5. After analyzing the VPN configuration, Security Director performs the configuration parsing and the endpoint correlation. During the endpoint correlation if any conflicting configurations are found, you can either proceed to ignore the conflicts during the import and log this detail as a job or cancel the operation, as shown in [Figure 131 on page 276](#). Click **Yes** to ignore the conflicts and import the remaining configuration or **No** to abort the import and proceed to the next step to select devices.

Figure 131: VPN Import-Conflicting EndPoints



The conflict occurs when the combination of IKE and IPsec parameters are same between the endpoints. The following points explain the scenarios under which the conflicts occur for different VPN configuration types:

- Preshared key and Main Mode
  - Preshared key
  - Local IKE ID of local endpoint and remote IKE ID of remote endpoint
  - Remote IKE ID of local endpoint and local IKE ID of remote endpoint
- Preshared key and Aggressive Mode
  - Preshared key
  - Local IKE ID of local endpoint and remote IKE ID of remote endpoint

OR

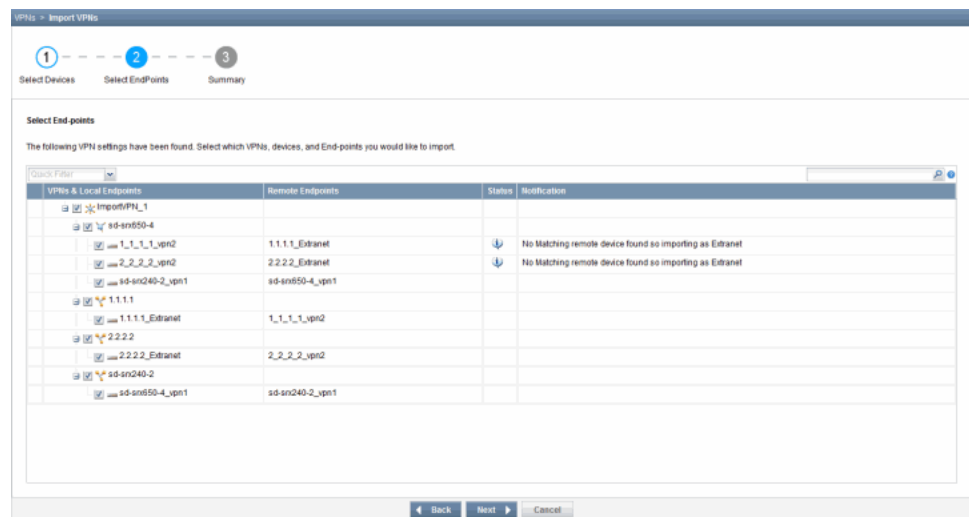
  - Remote IKE ID of local endpoint and local IKE ID of remote endpoint
- Certificate, Main Mode, and DN type IKE ID
  - Remote IKE ID of local endpoint and DN of the certificate of remote endpoint
  - DN of the certificate of the local endpoint and remote IKE ID of remote endpoint
- Certificate, Main Mode and other IKE ID type
  - Local IKE ID of the local endpoint and remote IKE ID of the remote endpoint

- Remote IKE ID of local endpoint and local IKE ID of remote endpoint
- Certificate, Aggressive Mode, and DN type IKE ID
  - Remote IKE ID of local endpoint and DN of the certificate of remote endpoint
  - DN of the certificate of the local endpoint and remote IKE ID of remote endpoint
- Certificate, Aggressive Mode, and other IKE ID type
  - Local IKE ID of local endpoint and remote IKE ID of remote endpoint
 OR
  - Remote IKE ID of local endpoint and local IKE ID of remote endpoint

If there are no conflicts, you can directly proceed to Step 6.

- The Select EndPoints page appears showing the VPN settings, as shown [Figure 132 on page 277](#).

**Figure 132: Select EndPoints Page**



All the imported VPNs will have autogenerated names, which you have the option to modify. Click the VPN name and enter the name. There is a predefined quick filter available to list all the errors and warnings. Click the drop-down list to select the required filter parameter.

The Select EndPoints page lists the VPNs discovered from the configuration and allows you to explore the devices, or endpoints for each of the discovered VPNs. You can also perform a free text search on the VPN name, device name, and endpoint names. [Table 30 on page 277](#) shows the description of each column.

**Table 30: Select End-Points Columns**

Column Name	Description
VPNs & Local Endpoints	Lists all the discovered VPNs and their associated devices and endpoints in a tree structure.

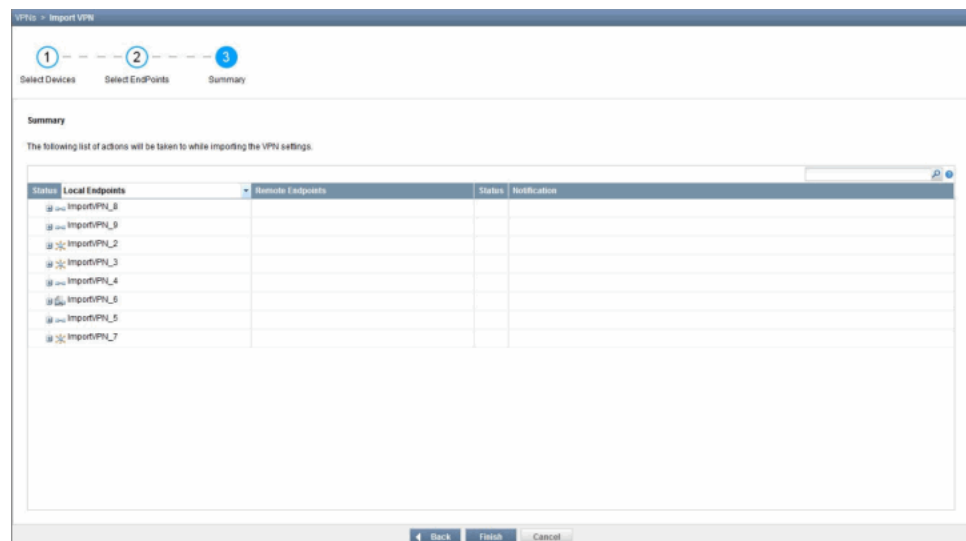
Table 30: Select End-Points Columns (*continued*)

Column Name	Description
Remote Endpoints	Shows matching endpoint details.
Warning	Displays any information, error, and warning messages detected during the import.

Select the VPNs, devices, and endpoints that you wish to import, and click **Next**. If you do not want to import certain VPNs, do not select them at this stage. Those unselected VPNs are not imported.

- The Summary page appears, as shown in [Figure 133 on page 278](#). All the VPNs listed on this page are saved in the Security Director database for further management.

Figure 133: Summary Page



Click **Finish**. A progress bar appears showing the progress of the import. Once the import is successful, you can manage the VPNs from the VPN landing page.

- The final summary page appears showing the number of VPNs, devices, and endpoints imported. To view the complete job details, click **full log details**. The Job Details page appears, as shown in [Figure 134 on page 279](#).

Figure 134: VPN Import Job Details

Job Details: 327728

User: super	Actual start time: Nov 26, 2014 10:16:19 AM IST
Job ID: 327728	Scheduled start time: Nov 26, 2014 10:16:18 AM IST
Job type: Import VPN	Percentage completion: 100
Job status: SUCCESS	End time: Nov 26, 2014 10:16:19 AM IST

**Import VPN Details**

Name	Status	Summary	Details
ImportVPN_8	SUCCESS	VPN Imported with 2 devices	<a href="#">View</a>
ImportVPN_9	SUCCESS	VPN Imported with 2 devices	<a href="#">View</a>
ImportVPN_2	SUCCESS	VPN Imported with 3 devices	<a href="#">View</a>
ImportVPN_3	SUCCESS	VPN Imported with 3 devices	<a href="#">View</a>
ImportVPN_4	SUCCESS	VPN Imported with 2 devices	<a href="#">View</a>
ImportVPN_6	SUCCESS	VPN Imported with 2 devices	<a href="#">View</a>
ImportVPN_5	SUCCESS	VPN Imported with 2 devices	<a href="#">View</a>
ImportVPN_7	SUCCESS	VPN Imported with 3 devices	<a href="#">View</a>

Page 1 of 1 | ☒ Auto Refresh | Displaying 1 - 8 of 8 | Show 100 items

Close

9. Click **Close**. All the imported VPN configurations appear on the VPN landing page.



**NOTE:** At any point of the import workflow, you can choose to exit. All your settings and progress are discarded.

You can also import VPNs from the Security Director Devices workspace. To import VPNs:

1. Select **Security Director > Security Director Devices**.

The Security Director Devices page appears, as shown in [Figure 135 on page 280](#).

Figure 135: VPN Import from Security Director Devices

Security Director Devices						
Actions		2 Items Selected				
Name	Domain	OS Version	Platform	Last updated	IP Address	Connection Status
10.205.50.177 (Cluster)	Global	12.1x47-Q10.4	SRX3400		10.205.50.178	Up
FF-195	Global	12.1x47-Q10.4	FIREFLY PERIMETER		10.207.97.195	Up
HE_SRX-61-41	Global	12.1x47-Q10			10.205.61.41	Up
inter-connect-lays(HE_SRX-61-41)	Global	12.1x47-Q10			10.205.61.41	Up
lays-1(10.205.50.177) (Cluster)	Global	12.1x47-Q10.4			10.205.50.178	Up
lays-2(10.205.50.177) (Cluster)	Global	12.1x47-Q10.4			10.205.50.178	Up
multu-2(10.205.50.177) (Cluster)	Global	12.1x47-Q10.4			10.205.50.178	Up
multu-3(10.205.50.177) (Cluster)	Global	12.1x47-Q10.4			10.205.50.178	Up
SRX-101.bngid.juniper.net	Global	12.1x46-Q15			10.205.119.101	Up
SRX-192	Global	12.1x47-Q10.4			10.207.97.192	Up
SRX-193	Global	12.1x47-Q10.4			10.207.97.193	Up
SRX-194	Global	12.1x47-Q2			10.207.97.194	Up
SRX-240-102	Global	12.1x46-Q20.5	SRX240B		10.205.119.102	Up
SRX210-119-106	Global	12.1x45-Q10	SRX210B		10.205.119.106	Up
VPN-lays-1(HE_SRX-61-41)	Global	12.1x47-Q10	SRX3400		10.205.61.41	Up
VPN-lays-2(HE_SRX-61-41)	Global	12.1x47-Q10	SRX3400		10.205.61.41	Up
westford-ge	Global	12.1x46-Q20.5	SRX210H		10.205.119.108	Up

2. Select the device to import its VPN configurations, right-click or from Actions select **Import VPNs**.

**NOTE:**

- The schema version of the device must be mapped to the Junos version to import all the VPN settings.
- You must republish the imported VPNs before modifying them further.
- VPN imported without IKE IDs configured on devices is not available for any modifications, unless you modify any VPN settings. On modifying these imported VPNs generate local or remote IKE IDs.
- Single-ProxyID, Multi-ProxyID, and the preshared key settings are imported at the tunnel level.
- By default, for the imported VPNs, the preshared key type is shown as Auto-generate. However, a new key is not generated for the already imported tunnels. If a new device is added to the VPN, only for that device, a new key is autogenerated.

**Related Documentation**

- [IPsec VPN Overview on page 257](#)
- [Creating IPsec VPNs on page 259](#)
- [Publishing IPsec VPNs on page 281](#)
- [Managing IPsec VPNs on page 282](#)
- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

## Publishing IPsec VPNs

To publish an IPsec VPN:

1. Select **Security Director > VPN > Publish VPN**.

The Services page appears with all VPNs. It also displays the publish states of all the VPNs.

2. Select the check box next to the VPN that you want to publish.



**NOTE:** You can search for a specific device on which the VPN is published by entering the search criteria in the search field in the top-right corner of the Services page. You can search the devices by their name, IP address, or the device OS version.



**NOTE:** If the VPN is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices, to view all devices on which the VPN is published.

3. Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later.
4. Click **Next**.

The Affected Devices page displays the devices on which this VPN will be published.

5. If you want to preview the configuration changes that will be pushed to the device, click **View** in the Configuration column corresponding to the device. A Configuration Preview progress bar is shown while the configuration pushed to the device is generated.

The CLI Configuration tab appears by default. You can view the configuration details in the CLI format.

6. View the XML format of the configuration by clicking the **XML Configuration** tab.
7. Click **Back**.
8. Click **Publish** if you want to only publish the configuration.

A new job is created and the job ID appears in the Job Information dialog box.

9. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The VPN is now moved into the Published state if the configuration is published to all devices involved in the VPN. If the configuration is not published to all devices involved in the VPN, the VPN is placed in the Partially Published state. If a VPN is created but not published, the VPN is placed in the Unpublished state. If any modifications are

made to the VPN configuration after it is published, the VPN is placed in the Republish Required state. You can view the states of the VPN by hovering over them.

A new job is created and the job ID appears in the Job Information dialog box.

10. Click the job ID to view more information about the job created. This action directs you to the Job Management workspace.

If you get an error message during the publish or if the VPN publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.



**NOTE:** You can also publish a VPN by right-clicking the VPN in the VPN Tabular view and selecting **Publish VPN**. You are redirected to the **Affected Devices** page.



**NOTE:** You can publish a VPN only if you have the permission for all the assigned devices.

#### Related Documentation

- [IPsec VPN Overview on page 257](#)
- [Creating IPsec VPNs on page 259](#)
- [Managing IPsec VPNs on page 282](#)
- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

---

## Managing IPsec VPNs

You can modify and delete the IPsec VPNs listed in the Manage VPNs page.

To open the Manage VPNs page:

- Select **Security Director > VPN**.

The Manage VPNs page appears. All IPsec VPNs created so far are listed by default in the graphical view.

You can perform the following tasks in the Manage VPNs page:

1. [Modifying IPsec VPNs on page 283](#)
2. [Modifying Endpoint Settings in a VPN on page 284](#)
3. [Deleting IPsec VPNs on page 285](#)

## Modifying IPsec VPNs

To modify an IPsec VPN:

1. Select **Security Director > VPN**.

The VPN Tabular view appears.

2. Select the IPsec VPN that you want to modify from the left pane and click the appropriate link from the **Modify: General Settings : Device Association : Tunnel Settings** link on the right pane.

This action redirects you to the section of the IPsec VPN that you want to modify.



### NOTE:

- You can modify all the parameters of the VPN except the type of VPN.
- You cannot modify general settings, tunnel or route settings, and device selection if permission label is applied to one or more devices.

You can enable or disable the Multi-ProxyID option for the route-based VPNs. In the General Settings tab, if you uncheck the Multi-Proxy ID check box, the routing options in the Tunnel/Route Settings tab is set to No Routing. You can change the routing options based on your requirement.

3. Click **Modify**.

4. Click **Save**.

To modify the global settings of the devices in a VPN:

1. Select **Security Director > VPN**.

The VPN Tabular view appears.

2. Select the IPsec VPN that you want to modify from the left pane.

This devices that are a part of the VPN are displayed in the right pane.

3. Click the **External Interface** field of the device whose external interface you want to modify, and select the new external interface.
4. Click the **Tunnel Zone** field of the device whose tunnel zone you want to modify, and select the new tunnel zone.
5. Click **OK**.
6. Click the **Protected Zone/Networks** field of the device that needs to be modified, and select the new network or zone.

When the multi-proxy ID is selected, at the tunnel level, you can select the required local or remote proxy ID pair in the Traffic Selector column. However, at the global level, the Protected Zone/Network address is the traffic selector.

7. Click **OK**.

8. Click the **Routing Instance** field of the device whose routing instance you want to modify, and select the new routing instance.
9. Click the **Proxy Id** field of the device while proxy ID you want to modify, and select the new proxy ID.

When the multi-proxy ID is selected, the single Proxy Id column is hidden. Because, you cannot have both multi-proxy ID and single proxy-ID existing together.

10. Click **OK**.

## Modifying Endpoint Settings in a VPN

To modify the endpoint settings in an IPsec VPN:

1. Select **Security Director > VPN**.

The VPN Tabular view appears.

2. Select the device in the IPsec VPN that you want to modify from the left pane.

The settings configured for the device are shown in the right pane. You can modify all settings of the device except the External Interface, Tunnel Interface, and Tunnel Zone settings.

3. For each endpoint device, you can modify the VPN Name, and Preshared Key fields, and customize the VPN. Click the required endpoint device in the left pane, and you will get an option to change these fields in the right pane.

You can customize Traffic Selectors at endpoint level that overrides the global settings.

4. Click **Save**.

To modify the general settings of a VPN:

1. Select **Security Director > VPN**.

The VPN Tabular view appears.

2. Select the IPsec VPN that you want to modify from the left pane.

This devices that are a part of the VPN are displayed in the right pane.

3. Click **General Settings** at the top of the VPN Tabular view.

The Modify General Settings window appears. You can modify the name and description of the VPN, VPN profile, and the Preshared key fields.

4. Click **Modify**.



**NOTE:** You can also modify the device associations and tunnel settings of a VPN by clicking the **Device Associations** and **Tunnel/Route Settings** links, respectively, on top of the VPN Tabular view.

---

## Deleting IPsec VPNs

To delete an IPsec VPN:

1. Select **Security Director > VPN**.

The VPN Tabular view appears.

2. Right-click the IPsec VPN you intend to delete and click the **Delete VPN**.

A confirmation window appears.

3. Click **Delete**.



**NOTE:** If you delete a VPN, the erase configuration is sent to all devices that were a part of the VPN during the next Update operation for the device.

---

### Related Documentation

- [IPsec VPN Overview on page 257](#)
- [Creating IPsec VPNs on page 259](#)
- [Publishing IPsec VPNs on page 281](#)
- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)



# Creating and Managing Extranet Devices

- [Creating Extranet Devices on page 287](#)
- [Managing Extranet Devices on page 288](#)

## Creating Extranet Devices

---

To create extranet devices:

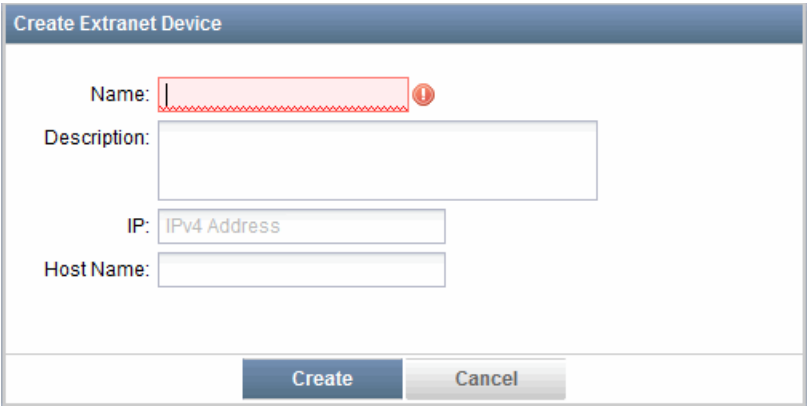
1. Select **Security Director > VPNs > Extranet Devices**.

The Extranet Devices page appears.

2. To create a new extranet device, click the plus sign (+).

The Create Extranet Device page appears, as shown in [Figure 136 on page 287](#).

**Figure 136: Create Extranet Device Page**



The screenshot shows a web form titled "Create Extranet Device". It has a blue header bar with the title. Below the header, there are four input fields: "Name:" (with a red border and a red exclamation mark icon), "Description:" (a large text area), "IP:" (with a placeholder "IPv4 Address"), and "Host Name:". At the bottom of the form are two buttons: "Create" (blue) and "Cancel" (gray).

3. In the Name field, enter a name for the new extranet device.
4. In the Description field, enter a description for the new extranet device.
5. In the IP field, enter the IP address.
6. In the Host Name field, enter the hostname.
7. Click **Create** to create the extranet device.

The new extranet device appears on the Extranet Devices page.

- Related Documentation**
- [Managing Extranet Devices on page 288](#)

---

## Managing Extranet Devices

You can modify, delete, and clone the extranet devices listed on the Extranet Devices page.

To open the Extranet Devices page:

- Select **Security Director > VPNs > Extranet Devices**.

The Extranet Devices page appears.

You can right-click an extranet device to manage it.

You can perform the following tasks on the Extranet Devices page:

- [Modifying an Extranet Device on page 288](#)
- [Deleting an Extranet Device on page 288](#)
- [Cloning an Extranet Device on page 289](#)

### Modifying an Extranet Device

To modify an extranet device:

1. Select **Security Director > VPNs > Extranet Devices**.

The Extranet Devices page appears.

2. Select the extranet device you want to modify, right-click, and select **Modify Extranet Device**.

This action redirects you to the Create Extranet Device page that you used to create a new extranet device. You can modify all the fields on this page.

3. Click **Modify** to save the changes made to this extranet device.

### Deleting an Extranet Device

To delete an extranet device:

1. Select **Security Director > VPNs > Extranet Devices**.

The Extranet Devices page appears.

2. Select the extranet device you want to delete, right-click, and select **Delete Extranet Devices**.

The Delete dialog box appears.

3. Select the extranet devices you want to delete, and click **Delete**.

## Cloning an Extranet Device

1. Select **Security Director > VPNs > Extranet Devices**.

The Extranet Devices page appears.

2. Select the extranet device you want to clone, right-click, and select **Clone Extranet Device**.

You are redirected to the Clone Extranet Device page.

3. Make the necessary modifications, and click **Clone**.

**Related Documentation**

- [Creating Extranet Devices on page 287](#)



# Creating and Managing VPN Profiles

- [VPN Profiles Overview on page 291](#)
- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

## VPN Profiles Overview

---

You can use a VPN Profile Wizard to create an object that specifies the VPN proposals, mode of the VPN, and other parameters used in a route-based IPsec VPN. You can also configure the Phase 1 and Phase 2 settings in a VPN profile.

When a VPN profile is created, Junos Space creates an object in the Junos Space database to represent the VPN profile. You can use this object to create route-based IPsec VPNs.



**NOTE:** You cannot modify or delete Juniper Networks defined VPN profiles. You can only clone them and create new profiles.

SRX Series devices support preshared key and PKI certificate-based authentication methods in IKE negotiation for IPsec VPNs. The RSA certificate and DSA certificate-based authentication are supported for IKE negotiation. The predefined VPN profile is available with both RSA and DSA certificates-based authentication. The PKI certificate list from the device is automatically retrieved during the device discovery and update-based syslog notifications.

### Related Documentation

- [Creating VPN Profiles on page 292](#)
- [Managing VPN Profiles on page 297](#)

## Creating VPN Profiles

To create a VPN profile:

1. Select **Security Director > VPNs > VPN Profiles**.

The VPN Profiles page appears with all the VPN profiles. The first two profiles listed here are Juniper Networks defined VPN profiles.

2. Click the plus sign (+) to create a new VPN profile.
3. Enter the name of the VPN profile in the Name field.
4. Enter the description of the VPN profile in the Description field.
5. Click the **Phase 1** tab.

Figure 137 on page 292 shows the Phase 1 tab.

Figure 137: VPN Profile: Phase 1

The screenshot shows the 'VPN Profile' configuration window with the 'Phase 1' tab selected. The 'Name' field is set to 'ssvpn' and the 'Description' field is empty. Under the 'Phase 1' tab, the 'Authentication Type' is set to 'Preshared Key'. The 'Mode' is set to 'Main' (radio button selected). The 'IKE Id' is set to 'Hostname'. The 'Proposals' are set to 'Predefined' (radio button selected). The 'Predefined Proposal Sets' are set to 'Basic'. The 'Advanced Settings' section is expanded, showing 'Enable NAT Traversal' checked, 'Keep Alive Interval(secs)' set to 5, 'Enable DPD' unchecked, 'Always Send DPD' unchecked, 'DPD Interval(secs)' set to 10, and 'DPD Threshold' set to 5. At the bottom, there are 'Create' and 'Cancel' buttons.

6. Select the required authentication type from the Authentication Type drop-down menu. The following authentication types are supported:
  - Preshared key
  - RSA signature
  - DSA signature

- EC-DSA-Signature (256)
- EC-DSA-Signature (384)

For the certificate-based authentication method, the predefined proposal sets such as standard, basic, and compatible are not applicable. You must create a custom proposal for certificate-based authentication.

7. Select the VPN mode that you want to use by clicking the radio buttons next to Mode. The IKE ID type selection is enabled for main mode and also for authentication that is based on certificates. You can configure an IKE ID for the main mode VPN proposals using the available Hostname, User@hostname, and IPAddress IKE ID options.
  - If you select Aggressive as the VPN mode for the preshared key authentication type, an IKE ID drop-down menu appears. For the User@hostname IKE ID option, a separate User field appears. Enter an appropriate value in this field.
  - For RSA and DSA signature-authentication types, a distinguished name (DN) is available as an IKE ID option along with hostname and user@hostname. These options are available for both main and aggressive VPN modes.
8. Select the type of proposal as either Predefined or Custom by clicking the radio buttons next to Proposals.
9. To create custom VPN proposal, select the Customer radio button and perform the following steps:
  - a. Click **Add** to add a new VPN proposal.

The Create Phase 1 Proposal pop-up window appears.
  - b. Enter the name for the proposal in the Name field.
  - c. Select the appropriate DH group from the DH Group drop-down menu. The available DH groups are:
    - Group1
    - Group2
    - Group5
    - Group14
    - Group19
    - Group20
    - Group24
  - d. Select the appropriate authentication mechanism from the Authentication drop-down menu. The available authentication algorithms are MD5, SHA-1, SHA-256, and SHA-384.
  - e. Select the appropriate encryption mechanism from the Encryption drop-down menu. The available encryption methods are DES, 3DES, AES(128), AES(192), and AES(256).

- f. Select the life time interval from the Life Time (in seconds) selector.
  - g. Click **Create**.
10. Select the appropriate predefined proposal set from Predefined Proposal Sets drop-down menu. The available proposal sets are:
    - Basic
    - Standard
    - Compatible
    - SuiteB-GCM-128
    - SuiteB-GCM-256
  11. Expand the Advanced Settings pane by clicking the down arrow.

You can configure the advanced settings for Phase 1 here.
  12. Select the **Enable NAT Traversal** check box to enable this option.
  13. Select the appropriate keepalive interval from the Keep Alive Interval (secs) selector.
  14. Select the **Enable DPD** check box if you want to use this option.
  15. Select the **Always Send DPD** check box if you want to use this option.
  16. Select the appropriate dead peer detection interval from the DPD Interval (secs) selector.
  17. Select the appropriate dead peer detection threshold from the DPD Threshold selector.
  18. Click the **Phase 2** tab.

[Figure 138 on page 295](#) shows the Phase 2 tab.

Figure 138: VPN Profile: Phase 2

19. Select the option button next to the VPN proposal you want to use.

- To create a custom proposal, select Custom radio button. A separate window appears to enter the information. Click **Add** tab.

The Create Phase 2 Proposal window appears, as shown in [Figure 139 on page 295](#).

Figure 139: Create Phase 2 Proposal

- Enter name of the custom proposal in the Name field.

- Select the authentication from the Authentication drop-down menu. The available authentication algorithms are MD5, SHA-1, SHA-256(96), and SHA-256(28).
- Select the required protocol from the Protocol drop-down menu.
- Select the necessary encryption from the Encryption drop-down menu. The available encryption methods are , , , and .
  - DES
  - 3DES
  - AES(128)
  - AES(192)
  - AES(256)
  - AES-GCM(128)
  - AES-GCM(192)
  - AES-GCM(256)
- Select the Life Time in seconds.
- Select the Life Size in kilo bytes.
- Click **Create** to create a new IPsec custom proposal.

You can also click **Modify** tab to modify any value, or delete the custom proposal by clicking **Delete** tab.

20. Select an appropriate option from Perfect Forward Privacy drop-down menu. The available options are:

- Group1
- Group2
- Group5
- Group14
- Group19
- Group20
- Group24

21. Expand the Advanced Settings pane by clicking the down arrow.

22. Select the **Establish tunnel immediately** check box if you want to enable this option.

23. Select the **Enable VPN Monitor** check box if you want to enable this option.

This is a per-VPN option.

24. Select the appropriate option from the DF Bit drop-down menu.

25. Select the appropriate idle time interval from the Idle time (secs) selector.

26. Select the appropriate value from the Install Time selector.

27. Select the **Enable Anti Replay** check box if you to enable this option.
28. Click **Create**.

- Related Documentation**
- [VPN Profiles Overview on page 291](#)
  - [Managing VPN Profiles on page 297](#)

---

## Managing VPN Profiles

You can delete, modify, or clone VPN profiles listed in the VPN Profiles page.

To open the VPN Profiles page:

- Select **Security Director > VPNs > VPN Profiles**.

The VPN Profiles page appears.

You can right-click the VPN profile to manage it.

You can perform the following tasks on the VPN Profiles page:

- [Deleting VPN Profiles on page 297](#)
- [Modifying VPN Profiles on page 297](#)
- [Cloning VPN Profiles on page 298](#)

### Deleting VPN Profiles

To delete a VPN profile:

1. Select **Security Director > Object Builder > VPN Profiles**.  
The VPN Profiles page appears.
2. Select the VPN profile you want to delete, right-click, and select **Delete VPN Profiles**.  
The Delete Profile confirmation window appears.
3. Click **Delete**.



**NOTE:** You can also delete the VPN profile by right-clicking the VPN profile and selecting **Delete VPN Profiles**.

### Modifying VPN Profiles

To modify a VPN profile:

1. Select **Security Director > VPNs > VPN Profiles**.  
The VPN Profiles page appears.
2. Select the VPN profile you want to modify, right-click, and select **Modify VPN Profile**.

You are redirected to the Modify VPN Profile page.

3. Click **Modify**.



**NOTE:** You can also modify the VPN profile by right-clicking the VPN profile and selecting **Modify VPN Profile**.



**NOTE:** If the VPN profile you have created is used as part of a VPN, you cannot modify IKE mode and IKE ID fields.

## Cloning VPN Profiles

To clone a VPN profile:

1. Select **Security Director > VPNs > VPN Profiles**.

The VPN Profiles page appears.

2. Select the VPN profile you want to clone, right-click, and select **Clone VPN Profile**.

You are redirected to the Clone VPN Profile page. By default, a generic name is given to the cloned VPN profile.



**NOTE:** You can also modify the VPN profile by right-clicking the VPN profile and selecting **Modify VPN Profile**.

3. Click **Clone**.

- Related Documentation**
- [VPN Profiles Overview on page 291](#)
  - [Creating VPN Profiles on page 292](#)

## PART 9

# Using Security Intelligence Solution

- [Understanding Security Intelligence Solution on page 301](#)
- [Creating and Managing Spotlight Secure Connectors on page 303](#)
- [Creating and Managing Information Sources on page 313](#)
- [Creating and Managing Security Intelligence Profiles on page 317](#)
- [Creating and Managing Security Intelligence Policies on page 323](#)
- [Creating and Managing Dynamic Address Groups on page 327](#)
- [Creating a Backup of the Connector Configuration on page 331](#)



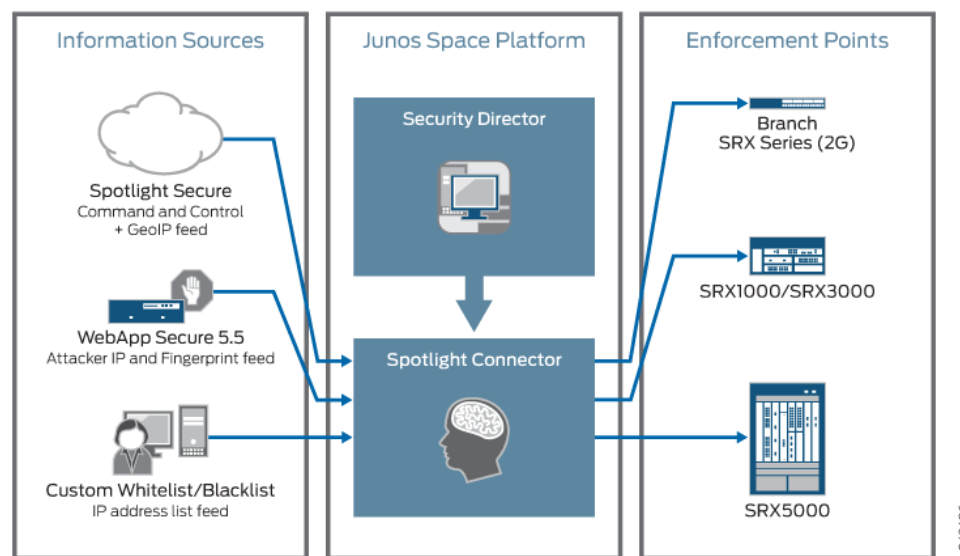
# Understanding Security Intelligence Solution

- [Security Intelligence Overview on page 301](#)

## Security Intelligence Overview

Juniper Networks offers the Security Intelligence solution, a set of services that provides feeds to SRX Series devices for automatically filtering traffic on both the network and the application layers. Junos Space Security Director is the management application for this solution, as shown in [Figure 140 on page 301](#).

Figure 140: Security Intelligence Solution



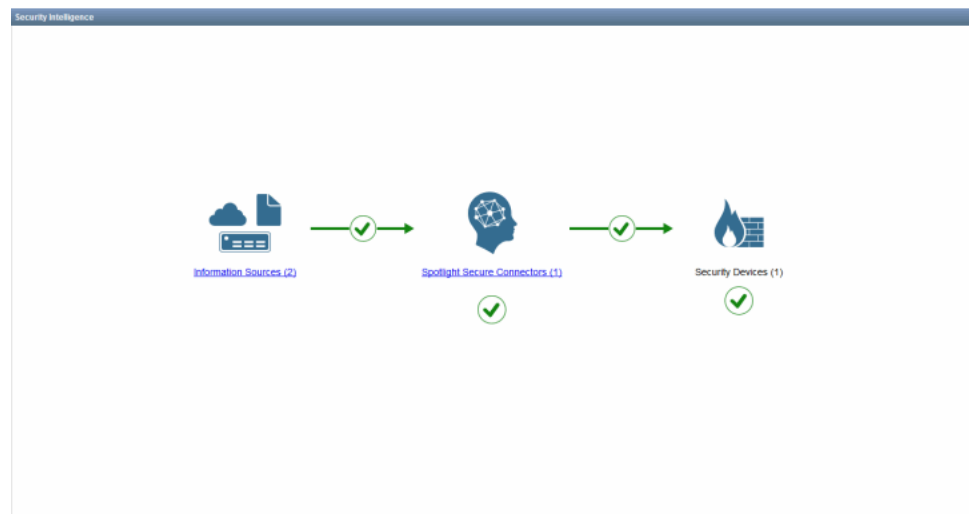
The Security Intelligence Spotlight Connector is an on-premise component that serves as an intermediary between SRX Series devices and various sources of security intelligence. These connectors run as virtual machines (VMs) inside the Junos Space Fabric. Security Director manages the SRX Series devices and the Security Intelligence connectors.

Security Director facilitates the following Security Intelligence management functions:

- Solution configuration management—Points connector(s) to Security Intelligence information sources and points SRX Series devices to connectors.
- Policy management of Security Intelligence profiles, policies, dynamic addresses, and firewall rules.
- Connector to information sources feed update status and SRX Series devices to connector feed update status.

To view the Security Intelligence dashboard, select **Security Director > Security Intelligence**. The Security Intelligence landing page shows the feed status summary and connection status for the connectors and associated security devices, as shown in [Figure 141 on page 302](#).

**Figure 141: Security Intelligence Page**



The green tick mark shows the connection status summary. Mouse over the tick mark to see the respective feed summary. The green mark indicates that the connection is working fine, yellow mark indicates if there are any warnings in the connection, and red mark indicates if the connection is failed. You can click Information Sources or Connectors to directly go to their landing pages.

The tick mark shown in between Information Source, Connectors, and Security Devices indicates the feed update status. The tick marks below the Connectors and Security Devices icon indicate connection status.

#### Related Documentation

- [Creating a Spotlight Secure Connector on page 303](#)
- [Managing Spotlight Secure Connectors on page 305](#)
- [Creating an Information Source on page 313](#)
- [Managing Information Sources on page 315](#)

## CHAPTER 21

# Creating and Managing Spotlight Secure Connectors

- Creating a Spotlight Secure Connector on page 303
- Managing Spotlight Secure Connectors on page 305

## Creating a Spotlight Secure Connector

To create a Spotlight Secure Connector:

1. Select **Security Director > Security Intelligence**.

The Security Intelligence landing page appears, as shown in [Figure 142 on page 303](#). This page shows the feed status of spotlight secure connectors and devices.

Figure 142: Spotlight Secure Connector Landing Page

Name	Management IP	Feed Status	Associated Devices	Cluster Status	Virtual IP	Privilege	Cluster Members	Connection Status	Software Version	Configuration
Connector-Node1	10.207.97.201	OK	0	Yes	10.207.97.205	Yes	Connector-Node1, Connector-node2	Up	0.17.4.1	In Sync
Connector-node2	10.207.97.202	OK	0	Yes	10.207.97.205	No	Connector-Node1, Connector-node2	Up	0.17.4.1	In Sync

2. Under Security Intelligence in the left pane, select **Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, showing the existing spotlight secure connectors and the following information for each spotlight secure connector:

- Connector name
- Management IP
- Feed status
- Associated devices
- Cluster status
- Virtual IP
- Primary
- Cluster members
- Connection status
- Software version
- Configuration



**NOTE:** The cluster has two nodes and both must be discovered separately. Any action applied to a single node, automatically reflects on the other node as well.

3. Click the plus sign (+) to add a new spotlight secure connector.

A pop-up window appears to enable you to create a new spotlight secure connector, as shown in [Figure 143 on page 304](#). The administrator must first add the spotlight secure connector VMs to the Network Management Platform fabric as specialized or alien nodes.

**Figure 143: Add Connector Page**



4. Select **Network Management Platform > Administration > Fabric**.
5. Click the plus sign (+) to create a new spotlight secure connector.  
Add Node to Fabric page appears.
6. In the Name field, enter the name of the spotlight secure connector.
7. In the IP address field, enter the IP of the spotlight secure connector.
8. Select the **Add as a specialized node** check box to provide the login credentials (username and password) of the specialized node.

9. Select the **Schedule at a later time** check box if you want to schedule and add the fabric node later.
10. Click **Add** to add a new spotlight secure connector.

This connector is displayed on the Spotlight Secure Connectors landing page.

**Related  
Documentation**

- [Managing Spotlight Secure Connectors on page 305](#)

---

## Managing Spotlight Secure Connectors

To open the Spotlight Secure Connectors page:

- Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connector.

- Right-click the spotlight secure connector to manage it, or select the required options from Actions.

You can perform the following management tasks on the Spotlight Secure Connectors page:

- [Adding Spotlight Secure Connector Global Settings on page 305](#)
- [Uploading Trusted Server CAs on page 307](#)
- [Associating Devices to Spotlight Secure Connectors on page 307](#)
- [Updating Spotlight Secure Connector Configuration on page 310](#)
- [Deleting Spotlight Secure Connectors on page 310](#)
- [Viewing Spotlight Secure Connector Feed Status on page 310](#)
- [Upgrading Spotlight Secure Connector Software or Package on page 311](#)

### Adding Spotlight Secure Connector Global Settings

To add spotlight secure connector global settings:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Click the Spotlight Secure Connector - Global Settings icon in the toolbar.

The Spotlight Secure Connector - Global Settings page appears, as shown in [Figure 144 on page 306](#).

Figure 144: Global Connector Settings

Spotlight Secure Connector - Global Settings

Spotlight Secure Connector Global Settings apply to all Spotlight Secure Connectors.

Connection Syslog E-mail Auto-upgrade

Device Connector Auth Token: JqrYXLVbV31VZv0yuoTkT9Up6vM3Ta6 ? Generate

WebApp Secure Auth Token: hXU5SbWMusL0d6rN2puqSyqaQzfAmxst ? Generate

Save Cancel

3. Under the Connection tab, configure the following parameters:

- To generate a 32-character token for the Device Connector Auth Token field, click **Generate**.
- To generate a 32-character token for the WebApp Secure Auth Token field, click **Generate**.

You can edit the auto-generated token; however, make sure that it still contains 32 characters.

4. Under the Syslog tab, configure the following parameters:

- Select the **Enabled** check box to enable the syslog collection.
- In the Address field, provide the address to use to collect the syslog data.
- In the Log Verbosity drop-down list, select the required option. The available options are:
  - Error
  - Warning
  - Info
  - Debug

5. Under the E-mail tab, configure the following parameters:

- Select the **Enabled** check box to enable the E-mail functionality.
- In the Host field, enter the hostname.

- In the Port field, select the required port number.
  - In the Username field, enter the username.
  - In the Password field, enter the password information.
  - In the From Address field, enter the From address.
  - in the To Address field, enter the To address.
  - Select the **Use TLS** check box.
6. Under the Auto-upgrade tab, you can configure the following parameters:
    - To automatically upgrade the spotlight secure connector once a week, select the **Weekly Auto-upgrade** check box.
    - From the Day of the Week drop-down list, select the required day to perform the automatic upgrade.
    - From the Time of the Day drop-down list, select the time.
  7. Click **Save** to save the spotlight secure connector settings.

## Uploading Trusted Server CAs

To upload the trusted server CA certificates:

1. Select **Security Intelligence > Spotlight Secure Connectors**.  
The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.
2. Click the Trusted Server CAs icon.  
The Trusted Server CAs page appears, listing the already uploaded certificates.
3. To upload the new certificate, click the plus sign (+).  
The Upload Trusted Server CA Certificate pop-up window appears.
4. To select the certificate file to upload, click **Select file**.
5. To upload the certificate files, click **Upload**.

## Associating Devices to Spotlight Secure Connectors

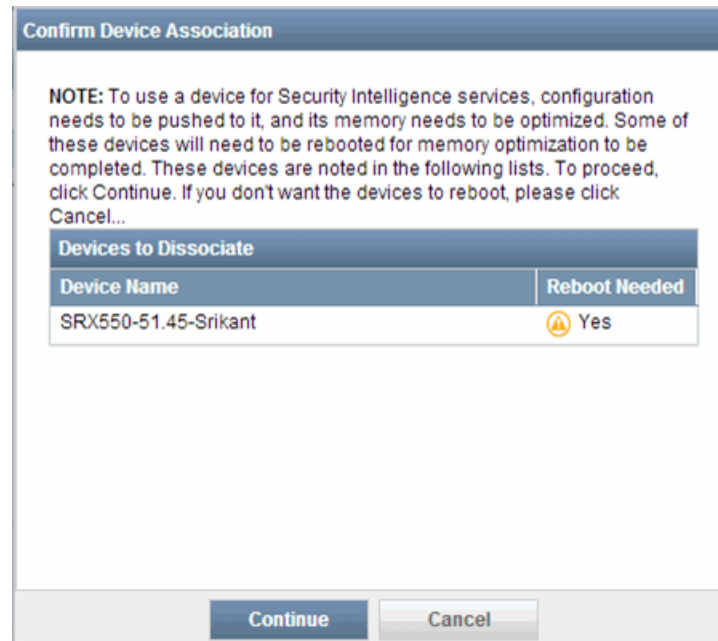
To associate a device with a spotlight secure connector:

1. Select **Security Intelligence > Spotlight Secure Connectors**.  
The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.
2. Right-click the spotlight secure connector, or, from the Actions, select **Associate Devices**.  
The Device Association page appears.

3. Select the required devices from the Available column, and move them to the Selected column.

If you assign a SRX550 or SRX650 device, the following message about the memory optimization is shown, as shown in [Figure 145 on page 308](#).

Figure 145: Confirm Device Association



4. To associate the selected devices with the spotlight secure connector, click **Save**.

When a device is associated with a spotlight secure connector or disassociated from a spotlight secure connector, a job is created in Security Director to push the spotlight secure connector configuration information to the device.

You can view the associated devices on the Spotlight Secure Connectors landing page. Click the Associated Devices column for the respective spotlight secure connector, and all the devices are listed, as shown in [Figure 146 on page 309](#).

Figure 146: Connector-Device List

Connector-SD-QA - Device List				
The following devices are configured to retrieve Security Intelligence from Connector-SD-QA.				
<input type="checkbox"/>	Security Device Name	Connection Status	Feed Update Status	Last Connection Time
<input checked="" type="checkbox"/>	Node-119.2	Down	Failure	Sep 11, 2014 05:46:49 AM UTC
<input type="checkbox"/>	10.205.255.38-Secintel	Up	OK	Sep 11, 2014 09:38:15 AM UTC
<input type="checkbox"/>	clust-41-node1	Up	OK	Sep 11, 2014 09:38:12 AM UTC
Update Feed				
Done				

You can view the feed update status of the security device. Select the required device and click the Feed Update Status. A window appears showing the feed status of the device, as shown in [Figure 147 on page 309](#).

Figure 147: Security Device Feed Status

10.205.255.38-Secintel - Feed Status				
Feed Name	Category	Status	Detailed Status	Last update time
TEST	BLACKLIST	OK	Store succeeded	2014-09-10 10:31:34.0
WL1	BLACKLIST	OK	Store succeeded	2014-09-10 10:31:34.0
BL2	WHITELIST	OK	Store succeeded	2014-09-10 10:31:34.0
JWAS1.cookie	JWAS	OK	Store succeeded	2014-09-10 10:41:31.0
JWAS1.ip_addr	JWAS	OK	Store succeeded	2014-09-10 10:41:31.0
Refresh Status				
Done				

You can update the feed to any listed device. Select the required Security Device, and click Update Feed option provided in the bottom of the Device List page, as shown in [Figure 146 on page 309](#).

A job window appears showing the status of the feed update. Click **View** under the Message column to view the update feed message.

## Updating Spotlight Secure Connector Configuration

If the configuration of a spotlight secure connector is out of sync from Security Director, administrator can choose to push or update the latest configuration to a spotlight secure connector.

To update the configuration:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Right-click the spotlight secure connector, or, from the Actions, select **Update Spotlight Secure Connector Configuration**.

A confirmation message appears confirm the update.

3. Click **Continue**.

The Job Details page appears, showing the spotlight secure connector update details.

4. In the Message column, click **View** to view the spotlight secure connector configuration.

When Device connector auth-token changes, both Update connector and Update connector settings to device jobs begin. The later job updates the auth-token information alone in the device.

## Deleting Spotlight Secure Connectors

To delete a spotlight secure connector:

1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

2. Right-click the spotlight secure connector and select **Delete Spotlight Secure Connector**, or click the minus sign (-).

3. You cannot directly delete a spotlight secure connector from the Security Intelligence workspace. A pop-up window appears to enable you to delete the spotlight secure connector.

4. Go to Network Management Platform > Administration > Fabric.

Select the required node, and click the minus sign (-).

5. The required spotlight secure connector is deleted.

## Viewing Spotlight Secure Connector Feed Status

To view the feed status of a spotlight secure connector:

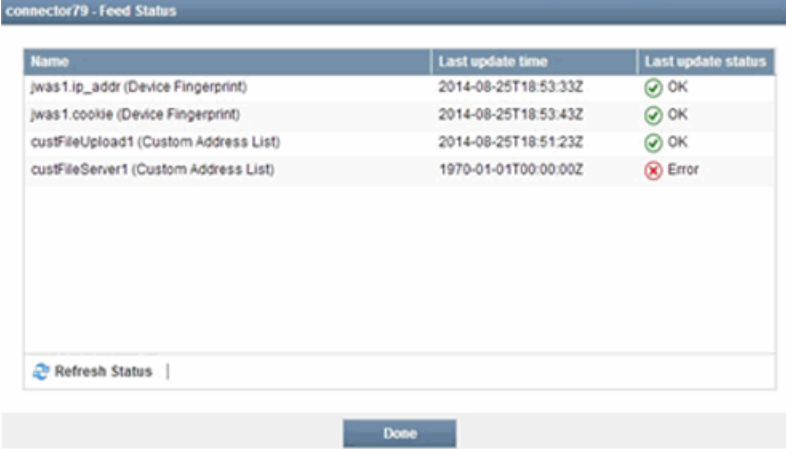
1. Select **Security Intelligence > Spotlight Secure Connectors**.

The Spotlight Secure Connectors landing page appears, listing the existing spotlight secure connectors.

- Click the **Feed Status** column for the required spotlight secure connector.

A Feed Status page appears showing the feed name, last updated time, and the last updated status, as shown in [Figure 148 on page 311](#).

**Figure 148: Spotlight Secure Connector Feed Status**



The screenshot shows a window titled "connector79 - Feed Status". Inside, there is a table with three columns: "Name", "Last update time", and "Last update status". The table contains four rows of data. Below the table, there is a "Refresh Status" button with a circular arrow icon, and at the bottom of the window, there is a "Done" button.

Name	Last update time	Last update status
jwas1.ip_addr (Device Fingerprint)	2014-08-25T18:53:33Z	OK
jwas1.cookie (Device Fingerprint)	2014-08-25T18:53:43Z	OK
custFileUpload1 (Custom Address List)	2014-08-25T18:51:23Z	OK
custFileServer1 (Custom Address List)	1970-01-01T00:00:00Z	Error

- To close the window, click **Done**.

## Upgrading Spotlight Secure Connector Software or Package

To upgrade the new spotlight secure connector software package:

- Enable the auto upgrade option for the spotlight secure connector. Ensure the spotlight secure connector has connectivity to the spotlight secure connector software repository.
- If a spotlight secure connector does not have the latest software version and the spotlight secure connector has connectivity to the spotlight secure connector software package, administrator can upgrade the spotlight secure connector from the update link of the spotlight secure connector listing page.
- If Step 1 and Step 2 options are not available, administrator can upload the software image and apply to spotlight secure connectors for upgrade. In the first release, administrator must SCP the upgrade package to spotlight secure connector VMs and invoke the upgrade process by executing a set of specific commands. You require an active internet connection because the command downloads the latest spotlight secure connector release from the Juniper Networks cloud package server.

**Related Documentation** • [Creating a Spotlight Secure Connector on page 303](#)



## CHAPTER 22

# Creating and Managing Information Sources

- [Creating an Information Source on page 313](#)
- [Managing Information Sources on page 315](#)

### Creating an Information Source

---

To create an information source:

1. Select **Security Director > Security Intelligence**.

The landing page appears, showing the feed status of connectors and devices.

2. Under Security Intelligence, in the left pane, select **Information Sources**.

The Information Sources landing page appears, as shown in [Figure 149 on page 313](#).

**Figure 149: Information Sources Landing Page**

Name	Domain	Source	Feed Category	Description	Address
<input checked="" type="checkbox"/> VUL-test	Global	Custom File Upload	Custom Address List		
<input checked="" type="checkbox"/> Cloud-check	Global	Spotlight Intelligence Cloud	Command & Control, GeoIP		

3. To create a new information source, click the plus sign (+).

The Add Information Source page appears, as shown in [Figure 150 on page 314](#).

Figure 150: Add Information Source

**Add Information Source**

Source: WebApp Secure

Group Name:

Description:

Adding a Juniper WebApp Secure feed requires the same settings provided above to be configured on each WebApp Secure Appliance that will be part of the group. The following additional information will also be needed:

Connector URL: `https://[Connector Hostname or IP Address]/api/jwas/manifest.json`

WebApp Secure Auth Token: `hXU5SbWMusL0d6rN2puqSyqaQzfAmxst`

To configure, do the following:

1. Log into the Juniper WebApp Secure Appliance.
2. Navigate to **Security Intelligence** under **Spotlight Secure** in the main menu.
3. Select the **Configure** button in the top right corner.
4. Set **Service Enabled** to **True**.
5. Enter the **Connector URL** and **Group Name** as described above.
6. Copy the **WebApp Secure Auth Token** shown above into the **Auth Token** field.
7. Select the **Test Connection Settings** link to verify the connection was made properly.

You may add multiple WebApp Secure Appliances to the same group.

Create Cancel

4. From the Source drop-down list, select the required source. The following sources are available:

- Spotlight Intelligence Cloud
- WebApp Secure
- Custom File Upload
- Custom File Server

The Spotlight Intelligence Cloud option is available only if the information source of Spotlight Intelligence Cloud type is not defined already. If the administrator has already created an information source of this type, the Spotlight Intelligence Cloud option is not shown in subsequent Add Information Source screen.

5. If you select WebApp Secure as the source, configure the following parameters:

- In the Group Name field, enter the name of the information source.
- In the Description field, enter a description of the information source.

If you select Custom File Upload as the source, configure the following parameters:

- In the Name field, enter the name of the information source.

- In the Description field, enter a description of the information source.
- To upload the custom file, click **Browse...**

You can click **View sample file** to view the sample custom file.

If you select Custom File Server as the source, configure the following parameters:

- In the Group Name field, enter the name of the information source.
- In the Description field, enter a description of the information source.
- In the Address field, enter the address of the customer host file server.
- In the Username field, enter the username of the given address.
- In the Password field, enter the password.
- From the Update Interval drop-down list, select the frequency of the update.

6. To create a new information source, click **Create**.

Once you create, update, or delete the information source, you must push the configuration to all the connected connectors.

#### Related Documentation

- [Managing Information Sources on page 315](#)

---

## Managing Information Sources

To open the Information Sources page:

- Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears, listing the existing sources.

- Right-click the information source to manage it, or select the required options from Actions.

You can perform the following management tasks on the Information Sources page:

- [Modifying an Information Source on page 315](#)
- [Deleting an Information Source on page 316](#)
- [Updating Feeds to Connectors on page 316](#)

### Modifying an Information Source

To modify an existing information source:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select the source and click the pencil icon to modify it.

The Modify Information Source page appears.

3. Modify the required fields, and click **Modify**.

## Deleting an Information Source

To delete an information source:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select the source, and click the minus sign (-).

A confirmation window appears before you can delete the source.

3. To delete the source, click **Delete**.

## Updating Feeds to Connectors

To update a feed to the connectors:

1. Select **Security Intelligence > Information Sources**.

The Information Sources landing page appears.

2. Select a source that has Spotlight Intelligence Cloud or Custom File Server as the source and right-click, or, from Actions, select **Update Feeds Now**.

All the connectors receive the feeds from the information sources based on the update interval for the feed category. You can use this option to get the feeds immediately.

3. A job is created to view the status of the feeds update.

**Related Documentation**

- [Creating an Information Source on page 313](#)

# Creating and Managing Security Intelligence Profiles

- [Creating Security Intelligence Profiles on page 317](#)
- [Managing Security Intelligence Profiles on page 320](#)

## Creating Security Intelligence Profiles

To create a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles, as shown in [Figure 151 on page 317](#).

Figure 151: Profiles Page

Profiles					
Security intelligence profiles define what actions you wish to take in response to various threats. All feeds that include Threat Scores can be used in Security Intelligence profiles. These profiles are used within Security Intelligence Policies. Global white and black lists are automatically applied across all Security Intelligence policies.					
Profile Name	Domain	Feed Category	Threshold Summary	Address List	Description
<input checked="" type="checkbox"/> Global White List	Global	Custom Address List			This global profile applies to all Security Intelligence Policies and can be used as a white list, permitting traffic and taking priority over the actions of other profiles
<input checked="" type="checkbox"/> Global Black List	Global	Custom Address List			This global profile applies to all Security Intelligence Policies and can be used as a black list, blocking traffic and taking priority over the actions of other profiles
<input checked="" type="checkbox"/> df-recs	Global	Device Fingerprint	Block Threshold Type: Recommended Actions Block Threshold Level: 5 Block Option: Close server & client connection Log Option: Log all traffic		
<input checked="" type="checkbox"/> cc-recs	Global	Command & Control	Block Threshold Type: Recommended Actions Block Threshold Level: 5 Block Option: Drop connections silently Log Option: Log all traffic		

2. To create a new Security Intelligence profile, click the plus sign (+).

The Create Security Intelligence Profile page appears, as shown in [Figure 152 on page 318](#).

Figure 152: Create Security Intelligence Profile Page

**Create Security Intelligence Profile**

Name: \*

Description:

Feed Category: Device Fingerprint

Blocking Threshold: ☒ Recommended ☐ Custom ☐ None

*Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions will dynamically block malicious or highly suspicious traffic based on the most current threat assessment provided through the dynamic feed.*

Current Recommended Block Threshold: 6

Block Options: For all the blocked traffic, take the following action:

☐ Drop connection silently

☒ Close connection (recommended)

*For all closed HTTP traffic, take the following action:*

☒ No Message

☐ Default Message

☐ Redirect URL

☐ Custom Message

Logging: ☐ Log only blocked traffic

☒ Log all traffic (recommended)

Create Cancel

3. In the Name field, enter the name of the profile.
4. In the Description field, enter a description of the profile.
5. From the Feed Category drop-down list, select a required feed category.  
The available categories are Device Fingerprint and Command & Control. By default, the feed category is set to Device Fingerprint.
6. Configure the Blocking Threshold field to either for the recommended values, or configure your own parameters.  
Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions provide the best balance between increased security and reduced false positives. Recommended actions dynamically blocks malicious or highly suspicious traffic based on the most current thread assessment provided through the dynamic feed
7. If the feed category is Device Fingerprint:
  - The recommended action for all the blocked traffic under Block Options is Close connection (recommended). When closing the HTTP traffic, the recommended action is not send any message to the user.
  - The recommended action for log events under Logging is Log all traffic (recommended).

You can customize the data to block traffic based on the threat score, as shown in Figure 153 on page 319.

Figure 153: Create Security Intelligence Profile-Custom Values

**Create Security Intelligence Profile**

**Blocking Threshold:** Recommended Custom None

Custom allows you to block traffic based on the Threat Score.

**Most aggressive**

**Default Security**

5

**Least aggressive**

- Provides the best balance between increased security and reduced [false positives](#).  
- Block malicious or suspicious traffic with a [threat score](#) of 5 or higher.

**Block Options:** For all the blocked traffic, take the following action:

☐ Drop connection silently

☒ Close connection (recommended)

For all closed HTTP traffic, take the following action:

☒ No Message

☐ Default Message

☐ Redirect URL

☐ Custom Message

**Logging:** ☐ Log only blocked traffic

☒ Log all traffic (recommended)

**Create** **Cancel**

**Outcome**

**Security**

Less More

**False Positive**

Less More

Under Blocking Options, you can customize the following action to be taken for all the closed HTTP traffic:

- No Message
- Default Message
- Redirect URL
- Customer Message

Under Logging section, you can customize the following log events:

- Log only blocked traffic
- Log all traffic (not recommended)
- Don't log any traffic

8. If the feed category is Command & Control:

- Under the Block Options, the recommended action for all the blocked traffic is log all traffic (recommended).
- Under Logging section, the recommended action is Log only blocked traffic.

You can customize Blocking Options and Logging fields to the required values.

9. Click **Create**.

A new profile is created and added to the Profiles page.



**NOTE:**

- On the Profiles page, the Global Black List and Global White List profiles are created by default.
  - The Security Intelligence profiles can be assigned only to the firewall policies.
- 

**Related  
Documentation**

- [Managing Security Intelligence Profiles on page 320](#)

---

## Managing Security Intelligence Profiles

You can modify and delete the profiles that are listed on the Profiles main page.

To open the Profiles page:

- Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

- Right-click a profile to manage it.

You can perform the following management tasks on the Profiles page:

- [Modifying a Security Intelligence Profile on page 320](#)
- [Deleting a Security Intelligence Profile on page 321](#)
- [Modifying a Global White List or Global Black List on page 321](#)

### Modifying a Security Intelligence Profile

To modify a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify Security Intelligence Profile**.

The Modify Security Intelligence Profile page appears.

3. On the Modify Security Intelligence Profile page you can modify the name, description, actions, and threat levels for the Custom Actions.
4. To modify the profile, click **Modify**.

## Deleting a Security Intelligence Profile

To delete a profile:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select the profile that you want to delete, and click the minus sign or right-click and select the **Delete Security Intelligence Profile(s)** option. A confirmation window appears before you can delete the profile.
3. To delete the profile, click **Delete**.

You can delete more than one profile at a time.

## Modifying a Global White List or Global Black List

To modify a global white list or a black list:

1. Select **Security Director > Security Intelligence > Profiles**.

The Profiles page appears, listing the existing profiles.

2. Select Global White List or Global Black List, right-click and select **Modify Security Intelligence Profile**.

The Modify Intelligence Profile window appears for a particular list.

3. Select the custom addresses available from the Available Address Lists. The Custom Address List feed category is assigned to these profiles.

### Related Documentation

- [Creating Security Intelligence Profiles on page 317](#)



## CHAPTER 24

# Creating and Managing Security Intelligence Policies

- [Creating Security Intelligence Policies on page 323](#)
- [Managing Security Intelligence Policies on page 324](#)

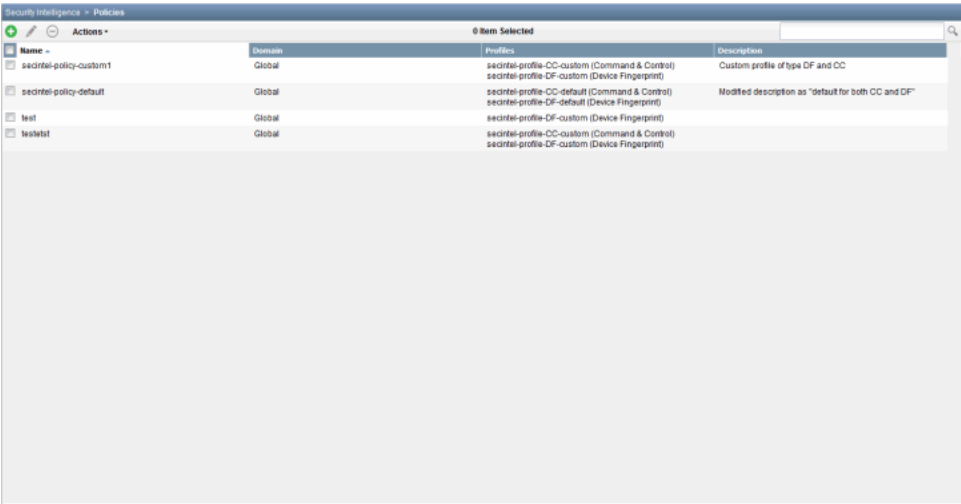
## Creating Security Intelligence Policies

To create a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing all the existing policies, as shown in [Figure 154 on page 323](#).

**Figure 154: Policies Page**



Name	Domain	Profiles	Description
<input type="checkbox"/> secintel-policy-custom1	Global	secintel-profile-CC-custom (Command & Control) secintel-profile-DF-custom (Device Fingerprint)	Custom profile of type DF and CC
<input type="checkbox"/> secintel-policy-default	Global	secintel-profile-CC-default (Command & Control) secintel-profile-DF-default (Device Fingerprint)	Modified description as "default for both CC and DF"
<input type="checkbox"/> test	Global	secintel-profile-DF-custom (Device Fingerprint)	
<input checked="" type="checkbox"/> testdel1	Global	secintel-profile-CC-custom (Command & Control) secintel-profile-DF-custom (Device Fingerprint)	

2. To create a new Security Intelligence policy, click the plus sign (+).

The Create Policy page appears, as shown in [Figure 155 on page 324](#).

Figure 155: Create Policy Page

The screenshot shows the 'Create Policy' dialog box. It includes a 'Name' field, a 'Description' field, and a 'Profiles' section with two dropdown menus: 'Command & Control' and 'Device Fingerprint'. Below these is a 'Custom Address List' section with links for 'Global White List' and 'Global Black List'. At the bottom are 'Create' and 'Cancel' buttons.

3. In the Name field, enter the name of the policy.
4. In the Description field, enter a description of the policy.
5. Under the Profiles section, configure the following profile categories:
  - Command & Control
  - Device Fingerprint
6. To view and modify the custom address list of the Global White List and Global Black List profiles, click **View**.  
 The Modify Security Intelligence Profile page appears to enable you to view or modify the profile.
7. Click **Create**.

A new Security Intelligence policy is created and listed in the Policies page.

**Related Documentation** • [Managing Security Intelligence Policies on page 324](#)

## Managing Security Intelligence Policies

You can modify and delete the policies that are listed on the Policies main page.

To open the Policies page:

- Select **Security Director > Security Intelligence > Policies**.  
 The Policies page appears, listing the existing policies.
- Right-click a policy to manage it.

You can perform the following management tasks on the Policies page:

- [Modifying a Security Intelligence Policy on page 325](#)
- [Deleting a Security Intelligence Policy on page 325](#)

## Modifying a Security Intelligence Policy

To modify a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing the existing policies.

2. Select the policy that you want to modify, and click the pencil icon or right-click and select **Modify Policy**.

The Modify Policy page appears.

3. On the Modify Policy page you can modify the name, description, profiles, and custom address list.
4. To modify the policy, click **Modify**.

## Deleting a Security Intelligence Policy

To delete a policy:

1. Select **Security Director > Security Intelligence > Policies**.

The Policies page appears, listing the existing policies.

2. Select the policy that you want to delete, and click the minus sign or right-click and select the **Delete Security Intelligence Policy(ies)** option. A confirmation window appears before you can delete the policy.

3. To delete the policy, click **Delete**.

You can delete more than one policy at a time.

### Related Documentation

- [Creating Security Intelligence Policies on page 323](#)



# Creating and Managing Dynamic Address Groups

- [Creating Dynamic Address Groups on page 327](#)
- [Managing Dynamic Address Groups on page 328](#)

## Creating Dynamic Address Groups

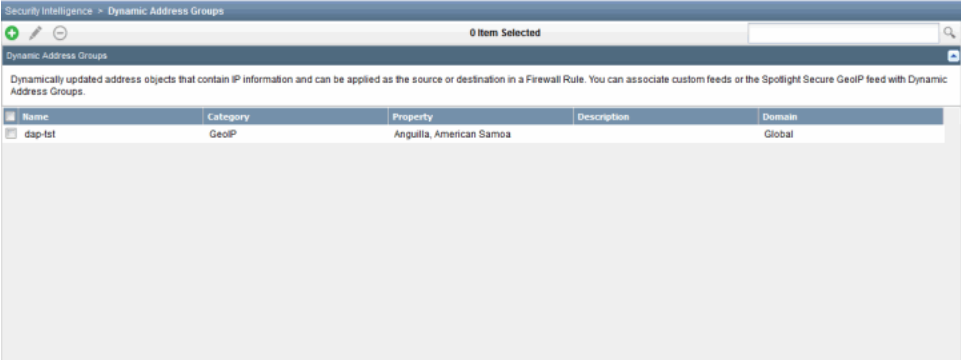
Dynamic address is an infrastructure that serves as a container for a list of IP addresses propagated from an external data feed. In Security Director, it is referenced by the firewall policy in the same way as the security legacy address entry. The only difference is that the content (such as IP addresses, prefixes, or ranges) contained in the Dynamic Address Entry (DAE) changes dynamically based on a periodic update retrieval from an external feed.

To create a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.

The Dynamic Address Groups page appears, as shown in [Figure 156 on page 327](#).

**Figure 156: Dynamic Address Groups Main Page**



Name	Category	Property	Description	Domain
dap-tst	GeoIP	Anguilla, American Samoa		Global

2. To create a new dynamic address group, click the plus sign (+).

The Create Dynamic Address Group page appears, as shown in [Figure 157 on page 328](#).

Figure 157: Create Dynamic Address Page

The screenshot shows a web form titled "Create Dynamic Address Group". It includes the following elements:

- Name:\***: A text input field.
- Description:**: A larger text area for a description.
- Feed:\***: A dropdown menu with the text "Select feed" and a downward arrow.
- Create**: A blue button.
- Cancel**: A grey button.

3. In the Name field, enter the name of the dynamic address group.
4. In the Description field, enter a description.
5. From the Feed drop-down list, select the external data feed.
6. Click **Create**.

A new dynamic address is created. This can be used only in the firewall policy.

**Related Documentation**

- [Managing Dynamic Address Groups on page 328](#)

## Managing Dynamic Address Groups

You can modify and delete the dynamic addresses that are listed on the Dynamic Address Groups main page.

To open the Dynamic Address Groups page:

- Select **Security Director > Security Intelligence > Dynamic Address Groups**.  
The Dynamic Address Groups page appears, listing the existing dynamic addresses.
- Right-click a dynamic address to manage it.

You can perform the following management tasks on the Dynamic Address Groups page:

- [Modifying a Dynamic Address Group on page 328](#)
- [Deleting an Address from a Dynamic Address Group on page 329](#)

### Modifying a Dynamic Address Group

To modify a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.  
The Dynamic Address Groups page appears.
2. Select the dynamic address that you want to modify, and click the pencil icon or right-click and select **Modify SecIntel Dynamic Address**.

The Modify Dynamic Address page appears, as shown in [Figure 158 on page 329](#).

**Figure 158: Modify Dynamic Address Page**

3. On the Modify Dynamic Address page, you can modify the name, description, feed, and countries list in addition to modifying the dynamic address.
4. Click inside the Countries field, and select the required countries from the drop-down list.  
The IP addresses shown from the countries in the list are included.
5. If you select the Negate Selected Countries option, the IP addresses from all the countries, except those listed in the Countries field, are included.
6. To modify a dynamic address, click **Modify**.

## Deleting an Address from a Dynamic Address Group

To delete a dynamic address from a dynamic address group:

1. Select **Security Director > Security Intelligence > Dynamic Address Groups**.  
The Dynamic Address Groups page appears.
2. Select the dynamic address that you want to delete, and click the minus sign(-) or right-click and select the **Delete SecIntel Dynamic Addresses** option. A confirmation window appears before you can delete the address.
3. To delete the address, click **Delete**.

You can delete more than one dynamic address at a time.

**Related Documentation**

- [Creating Dynamic Address Groups on page 327](#)



# Creating a Backup of the Connector Configuration

- [Creating a Backup or Restoring the Connector Settings on page 331](#)

## Creating a Backup or Restoring the Connector Settings

---

You can create a backup of the connector configuration and restore the connector settings. To create a backup:

1. Select **Security Intelligence > Backup/Restore**.  
The Backup/Restore page appears, listing the current versions.
2. To create a backup of the connector configuration, click the plus sign (+).  
The Backup Connector Setting page appears.
3. In the Description field, enter a description of the new version.
4. Click **Backup**.
5. The Snapshot Policy page appears, showing the status of the backup. Click **Close**.  
A new version is created and listed on the Backup/Restore page.

To restore the connector configuration:

1. On the Backup/Restore page, select a version and right-click, or, from Actions, select **Restore**.  
The Connector Settings - Restore Summary page appears. This page shows a summary of the connector settings before you restore the configuration.
2. Click **Restore**.  
The selected version is rolled back to the previous version, and the Rollback Policy page lists a summary of the rollback.
3. To view the summary of the rolled-back version, click **Summary Report**.

You can also delete the versions.

**Related Documentation** • [Security Intelligence Overview on page 301](#)

## PART 10

# Configuring UTM Policies

- [Creating and Managing UTM Policies on page 335](#)
- [Creating and Managing Antispam Profiles on page 349](#)
- [Creating and Managing Antivirus Profiles on page 355](#)
- [Creating and Managing Content Filtering Profiles on page 363](#)
- [Creating and Managing Web Filtering Profiles on page 371](#)
- [Creating and Managing URL Patterns on page 383](#)
- [Creating and Managing Custom URL Category Lists on page 389](#)
- [Creating and Managing UTM Device Profiles on page 395](#)



## CHAPTER 27

# Creating and Managing UTM Policies

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)

### UTM Overview

---

Unified Threat Management (UTM) is a term used to describe the consolidation of several security features into one device, to protect against multiple threat types. The advantage of UTM is a streamlined installation and management of these multiple security capabilities.

The following security features are provided as part of the UTM solution:

- **Antispam**—The antispam feature examines transmitted e-mail messages to identify e-mail spam. 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 drops the message or tags the message header or subject field with a preprogrammed string. The antispam feature uses a constantly updated spam block list (SBL). Sophos updates and maintains the IP-based SBL. The antispam feature is a separately licensed subscription service.
- **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. Kaspersky Lab provides the internal scan engine. The full file-based antivirus scanning feature is a separately licensed subscription service.
- **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 full 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. The express antivirus scanning feature is a separately licensed subscription service.

- Content filtering—Content filtering blocks or permits certain types of traffic based on the MIME type, file extension, protocol command, and embedded object type. Content filtering does not require a separate license.
- Web filtering—Web filtering lets you manage Internet usage by preventing access to inappropriate Web content.

The following types of Web filtering solutions are available:

- Integrated Web filtering—The decision-making process for blocking or permitting Web access is done on the device after it identifies the category for a URL either from user-defined categories or from a category server (Websense provides the CPA server). The integrated Web filtering feature is a separately licensed subscription service.
- Redirect Web filtering—The redirect Web filtering solution 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. Redirect Web filtering does not require a separate license.
- Juniper local Web filtering—The decision-making process for blocking or permitting Web access is done on the device after it identifies the category for a URL from user-defined categories stored on the device. With local filtering, there is no additional Juniper license or remote category server required.

Security Director supports creation of SRX Series UTM policies. You can refer to the UTM policies in the firewall policy rules.

**Related  
Documentation**

- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)

---

## Creating a UTM Policy Using UTM Wizard

---

The UTM policy wizard provides a step-by-step procedures to create a new UTM policy. You can configure multiple profiles for web filtering, antivirus, antispam, and content filtering by launching the respective wizards from the UTM wizard.

To create a new UTM policy:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears, as shown in [Figure 159 on page 337](#).

**Figure 159: UTM Policies Landing Page**

Name	Domain	Anti-Spam	Anti-Virus	Content Filtering	Web Filtering	Description
av-policy	SYSTEM		HTTP: av-defaults, FTP Upload: av-defaults, FTP Download: av-defaults, RMAP: av-defaults, SMTP: av-defaults, POP3: av-defaults			
av-wf-policy	SYSTEM		HTTP: av-defaults, FTP Upload: av-defaults, FTP Download: av-defaults, RMAP: av-defaults, SMTP: av-defaults, POP3: av-defaults		wf-cpa-default	
Praveen yethapu	Global		HTTP: av-defaults, FTP Upload: av-defaults, FTP Download: av-defaults, RMAP: av-defaults, SMTP: av-defaults, POP3: av-defaults		test	test
test	Global		HTTP: av-defaults, FTP Upload: av-defaults, FTP Download: av-defaults, RMAP: av-defaults, SMTP: av-defaults, POP3: av-defaults		wf-enhanced-default	
wf-policy	SYSTEM				wf-cpa-default	

2. To create a new UTM policy, click the plus sign (+).

The Create UTM Policy page appears, as shown in [Figure 160 on page 337](#).

**Figure 160: UTM Policy Wizard**

**Create UTM Policy**

Welcome to the Create UTM Policy Tool

This tool will help you create a Unified Threat Management (UTM) policy. UTM policies can include multiple profiles for Web Filtering, Anti-Virus, Anti-Spam and Content Filtering, some or all of which can be configured. You will have the opportunity to create profile objects as needed.

Once you have created a UTM policy, it can be assigned to various firewall rules in the policy table.

**Next** **Cancel**

3. Click **Next**.

You must select the required profile check box, as show in [Figure 161 on page 338](#). Depending on the profile that you have chosen, the respective wizard is launched for the configuration.

Figure 161: Different UTM Policy Profiles

Create UTM Policy

1 — 2 — 3 — 4 — 5 — 6

General Web Filtering Anti-Virus Anti-Spam Content Filtering Summary

Start by selecting the types of profiles you would like to assign to this UTM policy

☐ Web Filtering Profile ?

☐ Anti-Virus Profile ?

☐ Anti-Spam Profile ?

☐ Content Filtering Profile ?

◀ Back Next ▶ Cancel

4. Select the required profile and click **Next**.

You can configure the following profiles for a new UTM policy:

- [Creating a Web Filtering Profile on page 339](#)
- [Creating an Antivirus Profile on page 341](#)
- [Creating an Antispam Profile on page 343](#)
- [Creating a Content Filtering Profile on page 345](#)

## Creating a Web Filtering Profile

To create a web filtering profile:

1. Select the Web Filtering Profile check box, and click **Next**.

The web filtering wizard appears, as shown in [Figure 162 on page 339](#).

**Figure 162: Web Filtering Wizard**

**Create UTM Policy**

1 — 2 — 3 — 4 — 5 — 6  
 General — Web Filtering — Anti-Virus — Anti-Spam — Content Filtering — Summary

Let's start by providing some details about this UTM policy:

**General UTM Policy Information:**

Name:  (29 characters maximum.)

Description:

**Traffic Options:**

Connection limit per client:

Action when connection limit is reached: ☒ None ☐ Log and Permit ☐ Block

2. Under the General UTM Policy Information section, enter the following information:
  1. In the Name field, enter the name of the profile.
  2. In the Description field, enter a description for the new profile.
3. Under the Traffic Options section, enter the following information:
  1. In the Connection limit per client field, enter the connection limit . The default is 2000.
  2. In the Action when connection limit is reached drop-down list, enter the action that must be taken once the connection limit is reached. The available actions are None, Log and Permit, and Block.
4. Click **Next**.
5. Assign a web filtering profile to apply to this UTM policy for the HTTP traffic, from the HTTP drop-down list.

Another web filtering profile can be created inline by clicking **Create Another Profile**.  
 See [“Creating a Web Filtering Profile” on page 371](#)

6. Click **Next**.

The summary of the new profile is shown, as shown in Figure 163 on page 340.

Figure 163: Web Filtering Profile Summary

Create UTM Policy

1 — 2 — 3 — 4 — 5 — 6

General Web Filtering Anti-Virus Anti-Spam Content Filtering Summary

Please review the UTM policy you have created

General UTM Policy Information

Name web-ft

Connection limit per client 1000

Action when connection limit is reached Log and Permit

Web Filtering Profiles by Traffic Protocol

HTTP dycom-web-filter (Global)

Back Finish Cancel

7. Click **Finish**.

A new web filtering profile is created.

## Creating an Antivirus Profile

To create an antivirus profile:

1. Select the Anti-Virus Profile check box, and click **Next**.

The antivirus wizard appears, as shown in [Figure 164 on page 341](#).

**Figure 164: Antivirus Wizard**

**Create UTM Policy**

1 — 2 — 3 — 4 — 5 — 6  
General Web Filtering Anti-Virus Anti-Spam Content Filtering Summary

Let's start by providing some details about this UTM policy:

**General UTM Policy Information:**

Name:   
29 characters maximum.

Description:

**Traffic Options:**

Connection limit per client:

Action when connection limit is reached: ☒ None ☐ Log and Permit ☐ Block

2. Under the General UTM Policy Information section, enter the following information:
  1. In the Name field, enter the name of the profile.
  2. In the Description field, enter a description for the new profile.
3. Under the Traffic Options section, enter the following information:
  1. In the Connection limit per client field, enter the connection limit . The default is 2000.
  2. In the Action when connection limit is reached drop-down list, enter the action that must be taken once the connection limit is reached. The available actions are None, Log and Permit, and Block.
4. Click **Next**.
5. Select **Apply to all the Protocols** check box, if you want to apply the selected Default Profile to all the protocols. This is an option.
6. If the Apply to all the Protocols check box is not selected, different profiles can be chosen for different protocols.

To assign different profiles to different protocols, configure the following protocols:

- HTTP
- FTP Upload
- FTP Download
- IMAP
- SMTP
- POP3

You can create another antivirus profile inline from the drop-down list of these protocols, or by clicking **Create Another Profile**. See [“Creating an Antivirus Profile” on page 355](#)

7. Click **Next**.

The summary of the new profile is shown, as shown in [Figure 165 on page 342](#).

**Figure 165: Antivirus Profile Summary**

The screenshot shows the 'Create UTM Policy' window with a progress bar at the top indicating six steps: 1. General, 2. Web Filtering, 3. Anti-Virus (current step), 4. Anti-Spam, 5. Content Filtering, and 6. Summary. Below the progress bar, the text 'Please review the UTM policy you have created' is displayed. The 'General UTM Policy Information' section shows: Name: antv-pr, Connection limit per client: 1000, and Action when connection limit is reached: Log and Permit. The 'Anti-Virus Profiles by Traffic Protocol' section lists the following profiles: HTTP (av-defaults (SYSTEM)), FTP Upload (eav-defaults (SYSTEM)), FTP Download (sophos-av-defaults (SYSTEM)), IMAP (eav-defaults (SYSTEM)), SMTP (av-defaults (SYSTEM)), and POP3 (av-defaults (SYSTEM)). At the bottom of the window are three buttons: 'Back', 'Finish', and 'Cancel'.

8. Click **Finish**.

A new antivirus profile is created.

## Creating an Antispam Profile

To create an antispam profile:

1. Select the Anti-Spam Profile check box, and click **Next**.

The antispam wizard appears, as shown in [Figure 166 on page 343](#).

**Figure 166: Antispam Profile Wizard**

**Create UTM Policy**

1 — 2 — 3 — 4 — 5 — 6  
 General — Web Filtering — Anti-Virus — Anti-Spam — Content Filtering — Summary

Let's start by providing some details about this UTM policy:

**General UTM Policy Information:**

Name:

Description:

**Traffic Options:**

Connection limit per client:

Action when connection limit is reached: ☐ None ☒ Log and Permit ☐ Block

2. Under the General UTM Policy Information section, enter the following information:
  1. In the Name field, enter the name of the profile.
  2. In the Description field, enter a description for the new profile.
3. Under the Traffic Options section, enter the following information:
  1. In the Connection limit per client field, enter the connection limit . The default is 2000.
  2. In the Action when connection limit is reached drop-down list, enter the action that must be taken once the connection limit is reached. The available actions are None, Log and Permit, and Block.
4. Click **Next**.
5. Select the antispam profile from the SMTP drop-down list.  
 You can create another antispam profile inline from the SMTP drop-down list, or by clicking **Create Another Profile**. See [“Creating an Antispam Profile” on page 349](#)
6. Click **Next**.

The summary of the new profile is shown, as shown in [Figure 167 on page 344](#).

Figure 167: Antispam Profile Summary

Create UTM Policy

1 — 2 — 3 — 4 — 5 — 6

General Web Filtering Anti-Virus Anti-Spam Content Filtering Summary

Please review the UTM policy you have created

General UTM Policy Information

Name anti-spm

Connection limit per client 1000

Action when connection limit is reached Block

Anti-Spam Profile by Traffic Protocol

SMTP as-defaults (SYSTEM)

Back Finish Cancel

7. Click **Finish**.

A new antispam profile is created.

## Creating a Content Filtering Profile

To create a new content filtering profile:

1. Select the Content Filtering Profile check box, and click **Next**.

The content filtering wizard appears, as shown in [Figure 168 on page 345](#).

**Figure 168: Content Filtering Profile Wizard**

**Create UTM Policy**

1 — 2 — 3 — 4 — 5 — 6  
General Web Filtering Anti-Virus Anti-Spam Content Filtering Summary

Let's start by providing some details about this UTM policy:

**General UTM Policy Information:**

Name:  29 characters maximum.

Description:

**Traffic Options:**

Connection limit per client:

Action when connection limit is reached: ☒ None ☐ Log and Permit ☐ Block

2. Under the General UTM Policy Information section, enter the following information:
  1. In the Name field, enter the name of the profile.
  2. In the Description field, enter a description for the new profile.
3. Under the Traffic Options section, enter the following information:
  1. In the Connection limit per client field, enter the connection limit . The default is 2000.
  2. In the Action when connection limit is reached drop-down list, enter the action that must be taken once the connection limit is reached. The available actions are None, Log and Permit, and Block.
4. Click **Next**.
5. Select **Apply to all the Protocols** check box, if you want to apply the selected Default Profile to all the protocols. This is an option.
6. If the Apply to all the Protocols check box is not selected, different profiles can be chosen for different protocols.

To assign different profiles to different protocols, configure the following protocols:

- HTTP
- FTP Upload
- FTP Download
- IMAP
- SMTP
- POP3

You can create another content filtering profile inline from the drop-down list of these protocols, or by clicking **Create Another Profile**. See [“Creating a Content Filtering Profile” on page 363](#)

7. Click **Next**.

The summary of the new profile is shown.

8. Click **Finish**.

A new content filtering profile is created.

**Related  
Documentation**

- [UTM Overview on page 335](#)
- [Managing UTM Policies on page 346](#)

---

## Managing UTM Policies

---

You can modify, delete, and clone the UTM policies that are listed on the UTM Policies main page.

To open the UTM Policies page:

- Select **Security Director > UTM Policies**.

The UTM Policies page appears.

- Right-click the policy to manage it, or select the required options from Actions.

You can perform the following management tasks on the UTM Policies page:

- [Modifying a UTM Policy on page 347](#)
- [Deleting a UTM Policy on page 347](#)
- [Cloning a UTM Policy on page 347](#)
- [Finding UTM Policy Usage on page 347](#)
- [Showing Unused UTM Policies on page 348](#)
- [Deleting All Unused UTM Policies on page 348](#)

## Modifying a UTM Policy

To modify a UTM policy:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. Select the policy that you want to modify, and click the pencil icon or right-click and select **Modify UTM Policy**.

The Modify UTM Policy page appears.

3. On the Modify UTM Policy page, you can modify the name, description, connection limit, action to be taken once the connection reaches the limit, and antispam, antivirus, content filtering, and Web filtering profiles.
4. To modify the UTM policy, click **Modify**.

## Deleting a UTM Policy

To delete a UTM policy:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. Select the policy that you want to delete, and click the minus sign (-) or right-click and select the **Delete UTM Policies** option. A confirmation window appears before you can delete the UTM policy.

3. To delete the UTM policy, click **Delete UTM Policies**.

You can select more than one policy to delete.

## Cloning a UTM Policy

To clone a UTM policy:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. Select the policy that you want to clone, right-click it, and select **Clone UTM Policy**.

The Clone UTM Policy page appears.

3. On the Clone UTM Policy page, modify the required fields.
4. Click **Clone**.

The cloned UTM policy is created.

## Finding UTM Policy Usage

To find UTM policy usage:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. Select the policy for which you want to find the usage, right-click it, and select **Find Usage**.

The usage window appears showing the usage of the selected policy.

## Showing Unused UTM Policies

To show unused UTM policies:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. From Actions, select **Show Unused**.

All unused UTM policies are listed.

## Deleting All Unused UTM Policies

To delete unused UTM policies:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused policies.

Click **Yes** to confirm the deletion. All unused UTM policies are deleted.

- Related Documentation**
- [UTM Overview on page 335](#)
  - [Creating a UTM Policy Using UTM Wizard on page 336](#)

## CHAPTER 28

# Creating and Managing Antispam Profiles

- [Creating an Antispam Profile on page 349](#)
- [Managing Antispam Profiles on page 351](#)

## Creating an Antispam Profile

To create an antispam profile:

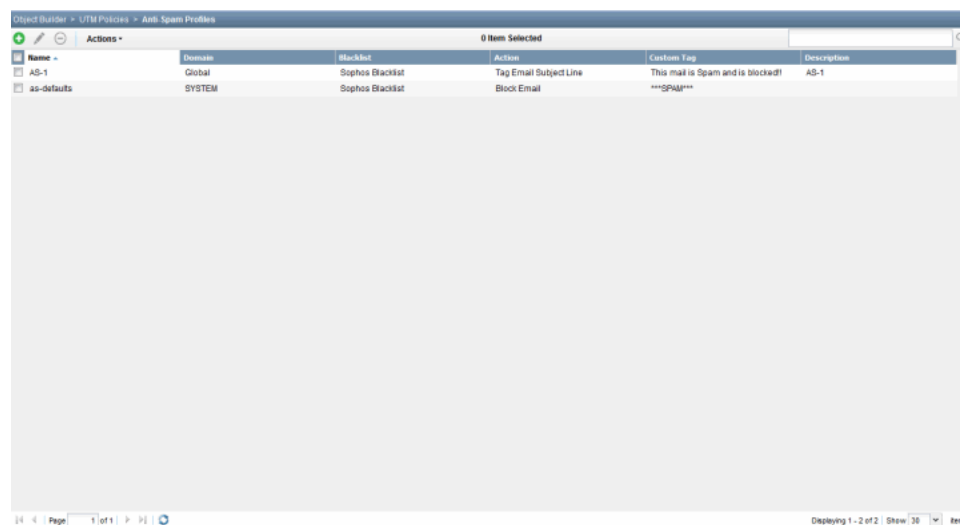
1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under the UTM Policies, select **Anti-Spam Profiles**.

The Anti-Spam Profiles page appears listing the existing profiles, as shown in [Figure 169 on page 349](#).

Figure 169: Anti-Spam Profiles Page



Name	Domain	Blacklist	Action	Custom Tag	Description
AS-1	Global	Sophos Blacklist	Tag Email Subject Line	This mail is Spam and is blocked!	AS-1
as-defaults	SYSTEM	Sophos Blacklist	Block Email	===Spam===	

3. To create a new antispam profile, click the plus sign (+).

The Create Anti-Spam Profile page appears, as shown in [Figure 170 on page 350](#).

Figure 170: Create Anti-Spam Profile Page

4. In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
5. In the Description field, enter a description for the new profile.
6. To use the server-based spam filtering, select the **Use Sophos Blacklist** check box. Otherwise, local spam filtering is used.  
  
This check box is selected by default. To configure the local spam filter, refer to Creating a Device Profile topic.
7. From the Default Action drop-down list, select one of the following default actions:
  - Tag Email Subject Line
  - Tag SMTP Header
  - Block Email
  - None
8. In the Custom Tag field, enter the custom defined tag information.
9. Click **Create**.

A new antispam profile is created and listed on the Anti-Spam Profiles page.

#### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing Antispam Profiles on page 351](#)

## Managing Antispam Profiles

---

You can modify, delete, and clone the antispam profiles that are listed on the Anti-Spam Profile main page.

To open the Anti-Spam Profile page:

- Select **UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the Anti-Spam Profiles page:

- [Modifying an Antispam Profile on page 351](#)
- [Deleting an Antispam Profile on page 351](#)
- [Cloning an Antispam Profile on page 352](#)
- [Finding Antispam Profile Usage on page 352](#)
- [Showing Unused Antispam Profiles on page 352](#)
- [Deleting All Unused Antispam Profiles on page 352](#)

### Modifying an Antispam Profile

To modify an antispam profile:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. Select the profile that you want to modify and click the pencil icon or right-click and select **Modify Anti-Spam Profile**.

The Modify Anti-Spam Profile page appears.

3. On the Modify Anti-Spam Profile page, you can modify name, description, use Sophos blacklist, default action, and custom tag.
4. To modify the antispam profile, click **Modify**.

### Deleting an Antispam Profile

To delete an antispam profile:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. Select the profile that you want to delete, and click the minus sign (-) or right-click and select the **Delete Anti-Spam Profiles** option. A confirmation window appears before you can delete the profile.
3. To delete the antispam profile, click **Delete**.

## Cloning an Antispam Profile

To clone an antispam profile:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. Select the profile that you want to clone, right-click, and select **Clone Anti-Spam Profile**.

The Clone Anti-Spam Profile page appears.

3. On the Clone Anti-Spam Profile page, modify the required fields.
4. Click **Clone**.

The cloned antispam profile is created.

## Finding Antispam Profile Usage

To find the antispam profile usage:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. Select the profile for which you want to find the usage, right-click it and select **Find Usage**.

The usage window appears, showing the usage of the selected profile.

## Showing Unused Antispam Profiles

To show the unused antispam profiles:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. From Actions, select **Show Unused**.

The antispam profiles that are not used by any UTM policies are listed.

## Deleting All Unused Antispam Profiles

To delete the unused antispam profiles:

1. Select **Security Director > UTM Policies > Anti-Spam Profiles**.

The Anti-Spam Profile page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused profiles.

To confirm the deletion, click **Yes**. All unused antispam profiles are deleted.

- Related Documentation**
- [UTM Overview on page 335](#)
  - [Creating a UTM Policy Using UTM Wizard on page 336](#)
  - [Managing UTM Policies on page 346](#)
  - [Creating an Antispam Profile on page 349](#)



# Creating and Managing Antivirus Profiles

- [Creating an Antivirus Profile on page 355](#)
- [Managing Antivirus Profiles on page 359](#)

## Creating an Antivirus Profile

The antivirus profile defines the content to scan for any malware and the action to be taken when a malware is found. Once you create a profile, you can assign it to UTM policies. Within the UTM policy you can apply either the same or different antivirus profiles to web, file transfer, and e-mail traffic.

To create an antivirus profile:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under UTM Policies, select **Anti-Virus Profiles**.

The Anti-Virus Profiles page appears listing all the existing antivirus profiles, as shown in [Figure 171 on page 355](#).

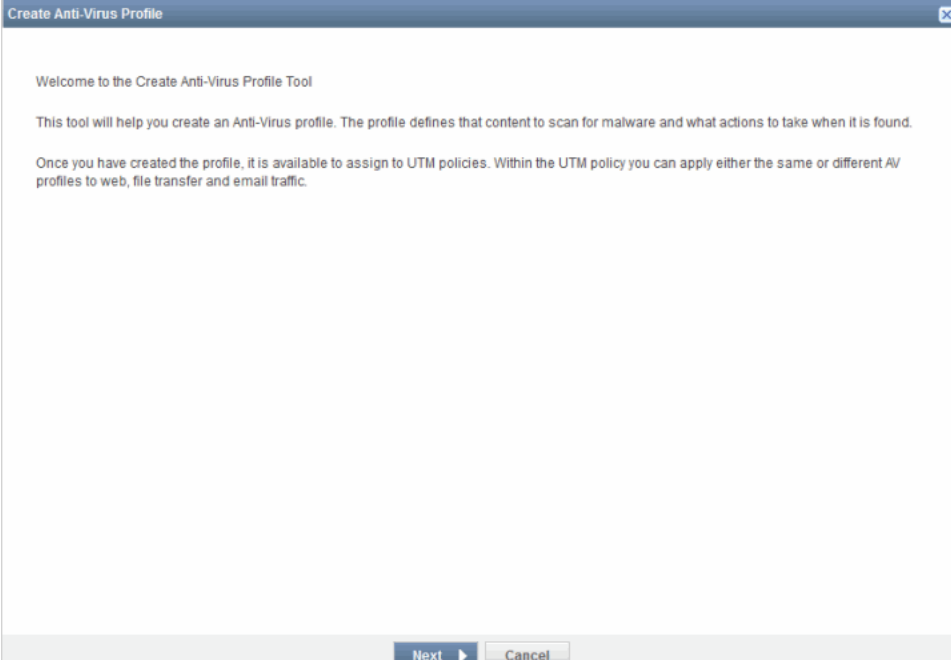
**Figure 171: Anti-Virus Profiles Main Page**

Name	Domain	Profile Type	Content Size Limit	Tracking Timeout	Description
<input type="checkbox"/> av-defaults	SYSTEM	Kaspersky	10000		
<input type="checkbox"/> esv-defaults	SYSTEM	Juniper Express	10000		
<input type="checkbox"/> sophos-av-defaults	SYSTEM	Sophos	10000		

3. To create a new antivirus profile, click the plus sign (+).

The Create Anti-Virus Profile page appears, as shown in [Figure 172 on page 356](#). Click **Next**.

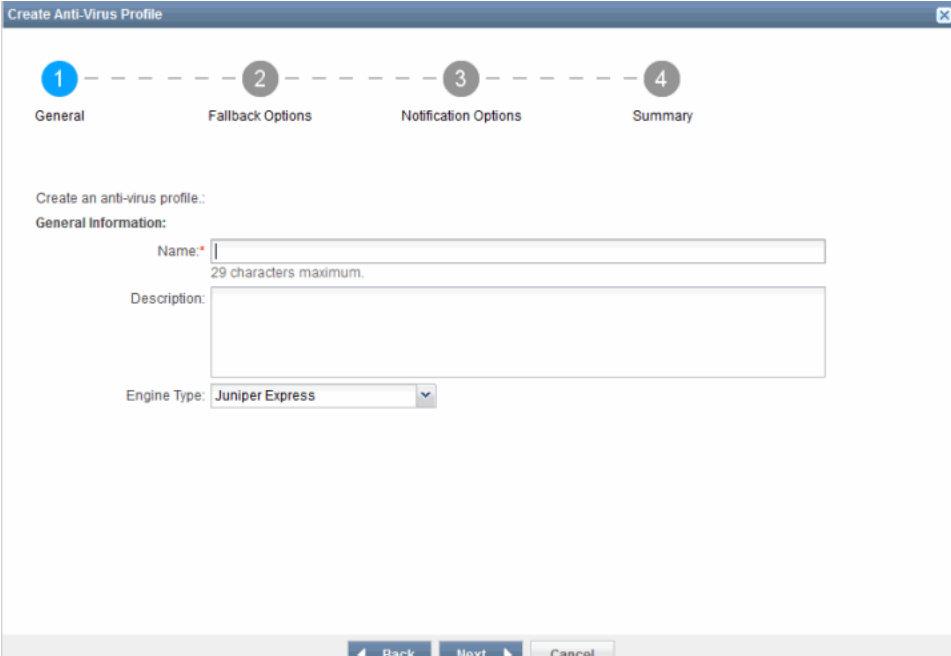
Figure 172: Create Anti-Virus Profile Page



The screenshot shows a window titled "Create Anti-Virus Profile". Inside, there is a welcome message: "Welcome to the Create Anti-Virus Profile Tool". Below this, it explains the tool's purpose: "This tool will help you create an Anti-Virus profile. The profile defines that content to scan for malware and what actions to take when it is found." It also states: "Once you have created the profile, it is available to assign to UTM policies. Within the UTM policy you can apply either the same or different AV profiles to web, file transfer and email traffic." At the bottom right, there are two buttons: "Next" and "Cancel".

4. The General Information page appears, as shown in [Figure 173 on page 356](#).

Figure 173: Antivirus Profile-General Information



The screenshot shows the "General Information" page of the "Create Anti-Virus Profile" tool. At the top, there is a progress bar with four steps: 1 (General, highlighted in blue), 2 (Fallback Options), 3 (Notification Options), and 4 (Summary). Below the progress bar, the text "Create an anti-virus profile.:" is followed by "General Information:". There are three input fields: "Name:" with a text box and a note "29 characters maximum.", "Description:" with a larger text box, and "Engine Type:" with a dropdown menu currently showing "Juniper Express". At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Under the General Information section, enter the following information:

1. In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
2. In the Description field, enter a description for the new profile.
3. From the Engine Type drop-down list, select the required engine types.

The available engine types are Juniper Express, Kaspersky, and Sophos. By default, Juniper Express is selected.

5. Click **Next**.

The Fallback Options page appears. In some scenarios, it might not be possible to scan the objects when they pass through the SRX Series devices. In the Fallback Options section, you can define the action to be taken when there is a failure or the default action if no specific options are configure.

For Juniper Express or Sophos:

Under the Fallback Options section, enter the following information:

1. Set Content Size to either Log and Permit or Block.
2. In the Content Size Limits field, enter the content size limit kilobytes. The limit range must be with in 20 - 40,000 KB.
3. Set Engine Error to either Log and Permit or Block.

Engine Error combines the errors engine not ready, timeout, too many requests, and out of resources into a single fallback option.

4. Set Default Action to either Log and Permit or Block.
5. Click **Next**.

The Notification Options page appears. The fallback option is used when the antivirus system experiences and error and must fallback to one of the previously configured actions to deny(block) or permit the object. Using the notification options, you can configure the user notification information to notify the user if the fallback occurs or a virus is deleted.

Under the Notification Options section, enter the following information:

On the Fallback Deny tab, select the **Notify mail sender if their message was blocked** check box, and configure the following fields:

- Select the Notification Type as either Protocol or Message.
- In the Custom Message Subject field, enter the custom defined message subject.
- In the Custom Message field, enter the custom message.
- To display the hostname, select the **Display Hostname** option.

- To allow administrator e-mails to be sent, select the **Allow Email** option.
- In the Administrator Email Address field, enter the e-mail address of the administrator who will receive the e-mail messages.

On the Fallback Non-Deny tab, select the **Warn mail recipient if the mail they received wasn't blocked despite problems** check-box, and configure the following fields:

- Enter the custom defined message subject in the Custom Message Subject field.
- Enter the custom message in the Custom Message field.

On the Virus Detected tab, select the **Notify mail sender if their message was blocked** check-box, and configure the following fields:

- Select the Notification Type as either Protocol or Message.
- In the Custom Message Subject field, enter the custom defined message subject .
- In the Custom Message field, enter the custom message.

If the Engine Type is Kaspersky:

Under the Fallback options, enter the following information:

- Set the Content Size to either Permit, Log and Permit, or Block.
- In the Content Size Limits field, enter the content size limit in kilo bytes.
- Set the Engine Error to either Permit, Log and Permit, or Block.

Engine error combines the errors engine not ready, timeout, too many requests, and out of resources into a single fallback option.

- Set the Password Protected to either Permit, Log and Permit, or Block.
- Set the Corrupt File to either Permit, Log and Permit, or Block.
- Set the Decompress Layer to either Permit, Log and Permit, or Block.
- Set the Default Action to either Permit, Log and Permit, or Block.
- In the File Extensions field, enter the file extensions to scan. Enter multiple file extensions separated by commas.
- Click **Next**.

The Notification Options page appears. The fallback option is used when the antivirus system experiences an error and must fallback to one of the previously configured actions to deny(block) or permit the object. Using the notification options, you can configure the user notification information to notify the user if the fallback occurs or a virus is deleted.

Under the Notification Options section, enter the following information:

On the Fallback Deny tab, select the **Notify mail sender if their message was blocked** check box, and configure the following fields:

- Select the Notification Type as either Protocol or Message.
- In the Custom Message Subject field, enter the custom defined message subject.
- In the Custom Message field, enter the custom message.
- To display the hostname, select the **Display Hostname** option.
- To allow administrator e-mails to be sent, select the **Allow Email** option.
- In the Administrator Email Address field, enter the e-mail address of the administrator who will receive the e-mail messages.

On the Fallback Non-Deny tab, select the **Warn mail recipient if the mail they received wasn't blocked despite problems** check-box, and configure the following fields:

- Enter the custom defined message subject in the Custom Message Subject field.
- Enter the custom message in the Custom Message field.

On the Virus Detected tab, select the **Notify mail sender if their message was blocked** check-box, and configure the following fields:

- Select the Notification Type as either Protocol or Message.
- In the Custom Message Subject field, enter the custom defined message subject .
- In the Custom Message field, enter the custom message.

6. Click **Next**. The summary of the antivirus profile configuration is shown.

7. Click **Finish**.

A new antivirus profile is created.

#### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing Antivirus Profiles on page 359](#)

---

## Managing Antivirus Profiles

You can modify, delete, and clone the antivirus profiles that are listed on the Anti-Virus profile main page.

To open the Anti-Virus Profile page:

- Select **UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following managing tasks on the Anti-Virus Profiles page:

- [Modifying an Antivirus Profile on page 360](#)
- [Deleting an Antivirus Profile on page 360](#)
- [Cloning an Antivirus Profile on page 360](#)
- [Finding Antivirus Profile Usage on page 361](#)
- [Showing Unused Antivirus Profiles on page 361](#)
- [Deleting All Unused Antivirus Profiles on page 361](#)

## Modifying an Antivirus Profile

To modify an antivirus profile:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify Anti-Virus Profile**.

The Modify Anti-Virus Profile page appears.

3. On the Modify Anti-Virus Profile page, you can modify name, description, engine type, trickling timeout, scan, fallback and notification options.
4. Click **Modify** to modify the antivirus profile.

## Deleting an Antivirus Profile

To delete an antivirus profile:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

2. Select the profile that you want to delete, and click the minus sign (-) or right-click and select the **Delete Anti-Virus Profiles** option. A confirmation window appears before you can delete the profile.
3. Click **Delete** to delete the antivirus profile.

## Cloning an Antivirus Profile

To clone an antivirus profile:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

2. Select the profile that you want to clone, right-click it and select **Clone Anti-Virus Profile**.

The Clone Anti-Virus Profile page appears.

3. Modify any required field data in the Clone Anti-Virus Profile page.
4. Click **Clone**.

The cloned antivirus profile is created.

## Finding Antivirus Profile Usage

To find antivirus profile usage:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

2. Select the profile for which you want to find the usage, right-click it, and select **Find Usage**.

The usage window appears, showing the usage of the selected profile.

## Showing Unused Antivirus Profiles

To show unused antivirus profiles:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profile page appears.

2. From Actions, select **Show Unused**.

The antivirus profiles that are not used by any UTM policies are listed.

## Deleting All Unused Antivirus Profiles

To delete the unused antivirus profiles:

1. Select **Security Director > UTM Policies > Anti-Virus Profiles**.

The Anti-Virus Profiles page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused profiles.

To confirm the deletion, click **Yes**. All unused antivirus profiles are deleted.

### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Creating an Antivirus Profile on page 355](#)



# Creating and Managing Content Filtering Profiles

- [Creating a Content Filtering Profile on page 363](#)
- [Managing Content Filtering Profiles on page 367](#)

## Creating a Content Filtering Profile

A content filtering profile specifies the kind of traffic to block or permit based on the MIME type, file extension, and protocol commands.

To create a content filtering profile:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under UTM Policies, select **Content Filtering Profiles**.

The Content Filtering Profiles page appears, listing the existing profiles, as shown in [Figure 174 on page 363](#).

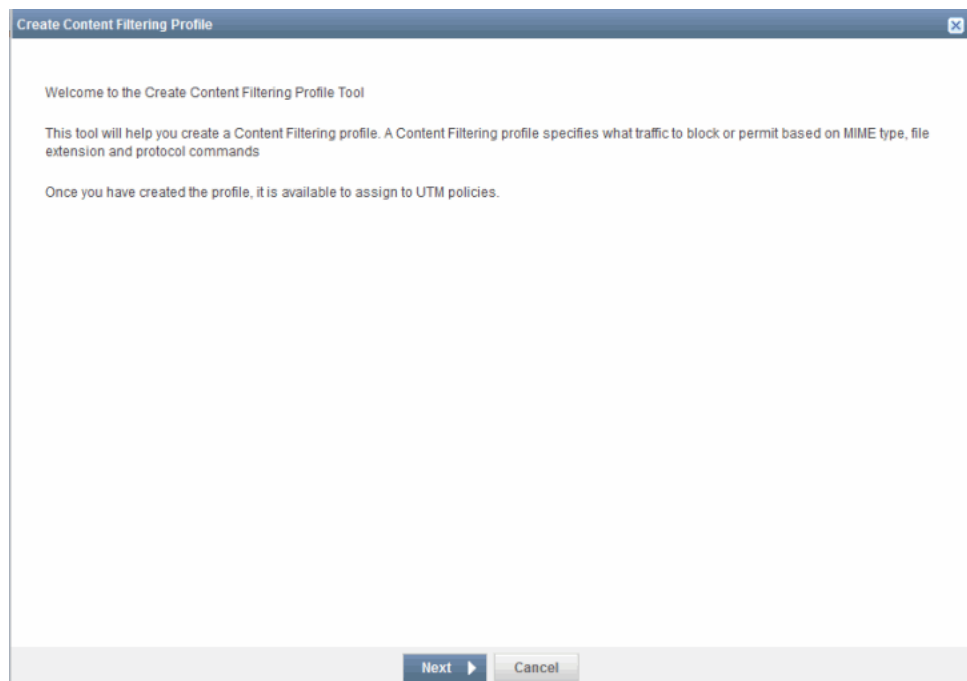
**Figure 174: Content Filtering Profiles Main Page**

Name	Domain	Permit Command List	Block Command List	Modification Type	Description
custom-content-filtering	SYSTEM	user/pass, port type, mpis-unicast, ip, mpis-unicast, DHCP, BGPE, GRP, OSPF, Multicast streams	user/pass, port type, RIP	message	

3. To create a new content filtering profile, click the plus sign (+).

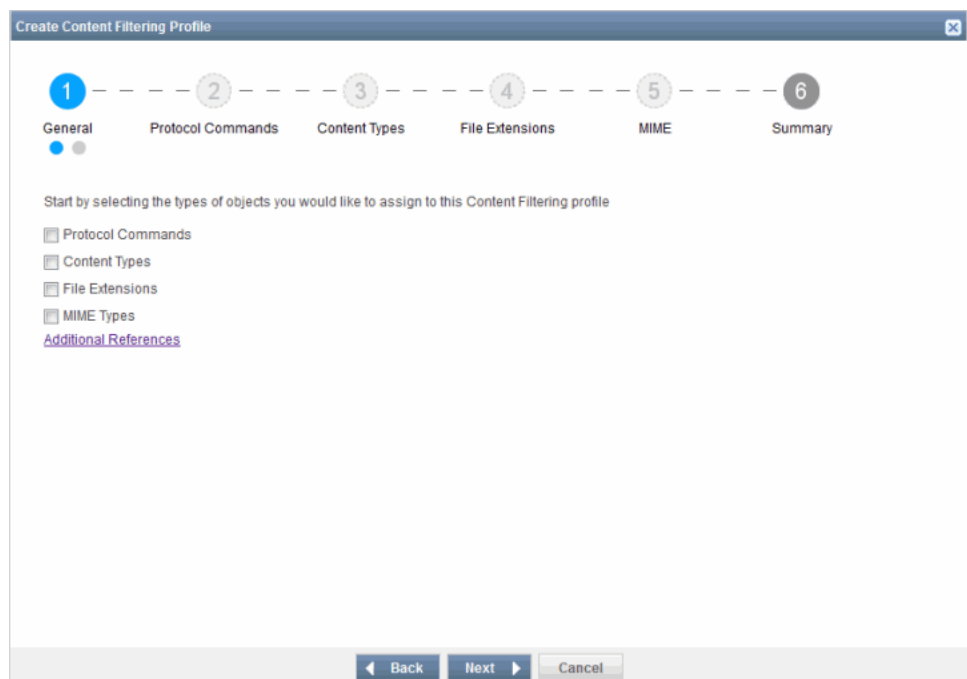
The Create Content Filtering Profile page appears, as shown in [Figure 175 on page 364](#).

Figure 175: Create Content Filtering Profile Page



4. Click **Next**. The General information page appears, as shown in Figure 176 on page 364.

Figure 176: Content Filtering Profile Wizard



You can select the following types of objects to assign to the content filtering profile:

- Protocol Commands
  - Content Types
  - File Extensions
  - MIME Types
5. Select the required object type check-box and click **Next**. For all the object types, you must configure the following common general information:

Under the General Information section, enter the following information:

1. In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
2. In the Description field, enter a description for the new profile.
3. If you want to notify the sender, select **Notify Mail Sender**.
4. Select Notification Type as either Protocol or Message from the drop-down list.
5. In the Custom Notification Message field, enter the notification message.

For the Protocol Commands object:

- Click **Next**. The Protocol Commands page appears.

Under the Protocols Commands section, configure the following parameters :

The content filtering blocks specific commands for HTTP, FTP, SMTP, IMAP, and POP3 protocols. Enter the commands that you wish to block and/or permit.

- In the Command Block List field, enter the protocol commands to be blocked. Separate protocols command with commas.
- In the Command Permit List field, enter the protocol commands to be permitted. Separate protocols command with commas.

Different protocols use different commands to communicate between servers and clients. By blocking or allowing certain commands, you can control the traffic on the protocol command level.

- Click **Next**. The summary page appears listing the protocol commands configuration.
- Click **Finish**.

For the Content Types object:

- Click **Next**. The Content Types page appears.

The content filtering can block files with a specific file extensions over HTTP. You can select the following content types you wish to block:

- ActiveX
- Windows executable (.exe)

- Http Cookie
- Java Applet
- ZIP files
- Click **Next**. The summary of the content type object configuration is shown in the Summary page.
- Click **Finish**.

For the File Extensions object type:

- Click **Next**. The File Extensions page appears.

The content filtering blocks files with specific file extensions over HTTP, FTP, SMTP, IMAP, and POP3 connections. Enter the file extensions that you wish to block.

- In the Extension block List field, enter the list of all files extensions to be blocked. Separate file extensions with commas.

Because file names are available during file transfers, using file extensions is a highly practical way to block or allow file transfers. The content filter list contains a list of file extensions to be blocked.

- Click **Next**. The summary of the file extensions object configuration is shown in the Summary page.
- Click **Finish**.

For the MIME object type:

- Click **Next**. The MIME Types page appears.

The content filtering blocks or permits special MIME types over HTTP, FTP, SMTP, IMAP, and POP3 connections. Enter the MIME types that you wish to block or permit.

- In the MIME Block List field, enter MIME(s) that needs to be blocked . Separate MIME(s) with commas.

The block MIME list contains the MIME type traffic that is to be blocked by the content filter.

- In the MIME Permit List field, enter MIME(s) that need to be permitted.
- Click **Next**. The summary of the MIME types configuration is shown in the Summary page.
- Click **Finish**.

#### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing Content Filtering Profiles on page 367](#)

---

## Managing Content Filtering Profiles

---

You can modify, delete, and clone the content filtering profiles that are listed on the Content Filtering Profile main page.

To open the Content Filtering Profile page:

- Select **UTM Policies > Content Filtering Profiles**.

The Content Filtering Profile page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the Content Filtering Profiles page:

- [Modifying the Content Filtering Profile on page 367](#)
- [Deleting the Content Filtering Profile on page 367](#)
- [Cloning the Content Filtering Profile on page 368](#)
- [Finding Content Filtering Profile Usage on page 368](#)
- [Showing Unused Content Filtering Profiles on page 368](#)
- [Deleting All Unused Content Filtering Profiles on page 368](#)

### Modifying the Content Filtering Profile

To modify the content filtering profile:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profiles page appears.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify Content Filtering Profile**.

The Modify Content Filtering Profile page appears.

3. On the Modify Content Filtering Profile page, you can modify name, description, notification options, protocol commands, content types, file extensions, and MIME types.
4. To modify the content filtering profile, click **Modify**.

### Deleting the Content Filtering Profile

To delete the content filtering profile:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profile page appears.

2. Select the profile that you want to delete, and click the minus sign or right-click and select the **Delete Content Filtering Profiles** option. A confirmation window appears before you can delete the profile.
3. To delete the content filtering profile, click **Delete**.

## Cloning the Content Filtering Profile

To clone the content filtering profile:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profile page appears.

2. Select the profile that you want to clone, right-click it and select **Clone Content Filtering Profile**.

The Clone Content Filtering Profile page appears.

3. On the Clone Content Filtering Profile page, modify any required field data.
4. Click **Clone**.

The cloned content filtering profile is created.

## Finding Content Filtering Profile Usage

To find Content Filtering profile usage:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profile page appears.

2. Select the profile for which you want to find the usage, right-click it, and select **Find Usage**.

The usage window appears, showing the usage of the selected profile.

## Showing Unused Content Filtering Profiles

To show unused content filtering profiles:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profile page appears.

2. From Actions, select **Show Unused**.

The content filtering profiles that are not used by any UTM policies are listed.

## Deleting All Unused Content Filtering Profiles

To delete the unused content filtering profiles:

1. Select **Security Director > UTM Policies > Content Filtering Profiles**.

The Content Filtering Profiles page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused profiles.

To confirm the deletion, click **Yes**. All unused content filtering profiles are deleted.

- Related Documentation**
- [UTM Overview on page 335](#)
  - [Creating a UTM Policy Using UTM Wizard on page 336](#)
  - [Managing UTM Policies on page 346](#)
  - [Creating a Content Filtering Profile on page 363](#)



## CHAPTER 31

# Creating and Managing Web Filtering Profiles

- [Creating a Web Filtering Profile on page 371](#)
- [Managing Web Filtering Profiles on page 379](#)

### Creating a Web Filtering Profile

Web Filtering profiles define a set of permissions and actions to take based on web connections and the predefined website categories. You can also create the custom URL categories and URL pattern lists during this process.

To create a Web filtering profile:

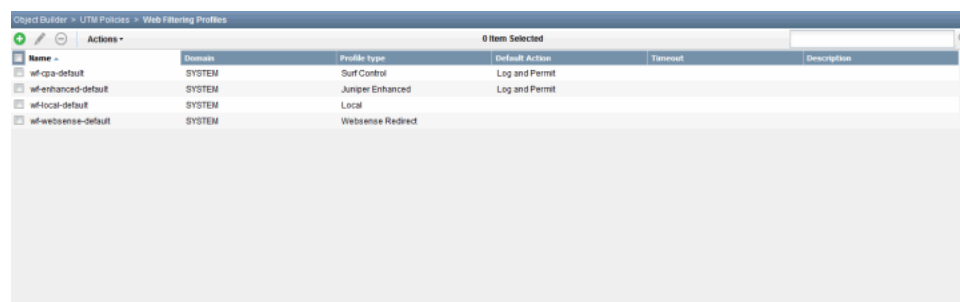
1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under UTM Policies, select **Web Filtering Profiles**.

The Web Filtering Profiles page appears, listing the existing profiles, as shown in [Figure 177 on page 371](#).

**Figure 177: Web Filtering Profiles Main Page**

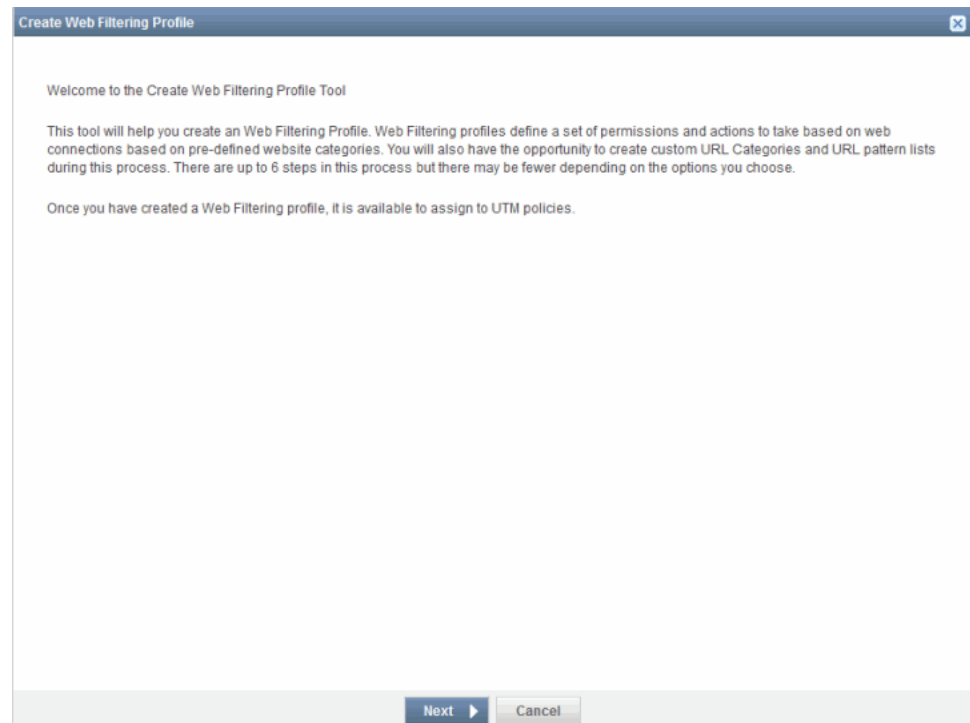


Name	Domain	Profile Type	Default Action	Timeout	Description
wfcpa-default	SYSTEM	Self Control	Log and Permit		
wfenhanced-default	SYSTEM	Juniper Enhanced	Log and Permit		
wflocal-default	SYSTEM	Local			
wfwebense-default	SYSTEM	Webense Redirect			

3. To create a new web filtering profile, click the plus sign (+).

The Create Web Filtering Profile page appears, as shown in [Figure 178 on page 372](#).

Figure 178: Create Web Filtering Profile



4. Click **Next**.

The General information page appears, as shown in [Figure 179 on page 373](#).

Figure 179: Create Web Filtering Profile

**Create Web Filtering Profile**

1 General    2 URL Categories    3 Fallback Options    4 Summary

Time to fill out some general information about the web filtering profile you wish to create:

**General Information:**

Name:\*   
29 characters maximum.

Description:

Engine Type:\*

Default Action:

Safe Search: ☒

Custom Block Message:

Custom Quarantine Message:

5. For the Juniper Enhanced engine type:

Under the General section, enter the following information:

- In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
- In the Description field, enter a description for the new profile.
- From the list, select the required Engine Type.

The following engine types are available:

- Juniper Enhanced
- Surf Control
- Websense Redirect
- Select Default Action from the drop-down list. This option is available only for Juniper Enhanced and Surf Control engine types.
- By default, the Safe Search option is selected. This option is available only for the Juniper Enhanced engine type.
- In the Custom Block Message field, enter a custom message to be sent when HTTP requests are blocked.

If a message begins with http: or https:, that message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages.

- In the Quarantine Custom Message field, enter the quarantine message.
- Click **Next**. The URL Categories page appears.

Assign URL categories to different actions such as deny, log and permit, permit, and quarantine.

- Under the Deny Action List section, click **Add URL Categories**.

The Select URL Categories page appears, as shown in [Figure 180 on page 374](#).

**Figure 180: Select URL Categories**

Select URL categories to apply to the deny list:

Show: ☒ All categories ☐ Custom URL categories ☐ WebSense URL categories

Available URL Categories	
Name	Domain
Enhanced_Abortion	SYSTEM
Enhanced_Abused_Drugs	SYSTEM
Enhanced_Adult_Content	SYSTEM
Enhanced_Adult_Material	SYSTEM
Enhanced_Advanced_Malware...	SYSTEM
Enhanced_Advanced_Malware...	SYSTEM
Enhanced_Advertisements	SYSTEM
Enhanced_Advocacy_Groups	SYSTEM
Enhanced_Alcohol_and_Tobacco	SYSTEM
Enhanced_Alternative_Journals	SYSTEM
Enhanced_Bandwidth	SYSTEM
Enhanced_Blogs_and_Person...	SYSTEM

Total: 130

Create New URL Category

Select Cancel

You can show all the categories, only the custom URL categories, or only the websense URL categories in the Available URL Categories column.

You can create a new URL categories inline. Click **Create New URL Categories** to create a new URL category. The Create URL Category page appears, as show in [Figure 181 on page 375](#). To know more about creating new URL categories, see [“Creating a Custom URL Category List” on page 389](#).

Figure 181: Inline Creation of a New URL Category

A URL Category is a user-defined list of URL Patterns.:

URL Category Name:\*

Description:

Select URL Pattern

Available Patterns	
Pattern	Domain
<input type="checkbox"/> blocked_sites	Global
<input type="checkbox"/> dycom_sites	Global
<input type="checkbox"/> white-list	Global

Total: 3

Create a New Pattern

Create Cancel

From this page, you can also create a new pattern. To create a new pattern, click Create a New Pattern option at the end of the page. The Create URL Pattern page appears, as shown in [Figure 182 on page 376](#). To know more about creating a new URL pattern, see ["Creating a URL Pattern" on page 383](#).

Figure 182: Inline Creation of a New URL Pattern

Create URL Pattern

A URL Pattern is a list of URLs (including wildcards) that can be used as a whitelist or blacklist. If Juniper Enhanced Web Filtering is configured, URL Patterns can also be assigned to custom URL Categories.

Name:

Description:

Add URLs:  Add

Filter  ? Delete

URL List

Total: 0

Create Cancel

- Similarly for Log & Permit Action List, Permit Action List, and Quarantine Action List sections, you can click the respective **Add URL Categories** option and select the required URL categories.
- Click **Next**. The Fallback Options page appears.  
The URLs can be processed using their reputation score, if there is no category available. Choose the action that you wish to take for the uncategorized URLs based on their reputation score.
- In the Fallback Options section, select the Default Action as either Log and Permit or Block.
- Under the Global Reputation Actions section:
  - The Uncategorized URL Actions check-box is selected by default. This option is to use the global reputation.
  - Select Very Safe as Log and Permit, Permit, Block, or Quarantine. By default, Permit is selected.
  - Select Moderately Safe as Log and Permit, Permit, Block, or Quarantine. By default, Permit is selected.
  - Select Fairly Safe as Log and Permit, Permit, Block, or Quarantine. By default, Log and Permit is selected.

- Select Suspicious as Log and Permit, Permit, Block, or Quarantine. By default, Log and Permit is selected.
- Select Harmful as Log and Permit, Permit, Block, or Quarantine. By default, Block is selected.

- Click **Next**.

The Summary page appears to review the configuration parameters selected to create a new web filtering profile.

- After reviewing, click **Finish**.

A new web filtering profile is created.

6. If the Engine Type is Surf Control, configure the following parameters:

Under the General Information section, enter the following information:

- In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
- In the Description field, enter a description for the new profile.
- From the list, select the required Engine Type.
- Select Default Action from the drop-down list. This option is available only for Juniper Enhanced and Surf Control engine types.
- By default, the Safe Search option is selected. This option is available only for the Juniper Enhanced engine type.
- In the Custom Block Message field, enter a custom message to be sent when HTTP requests are blocked.

If a message begins with http: or https:, that message is considered a block message URL. Messages that begin with values other than http: or https: are considered custom block messages.

- Click **Next**. The Assign URL categories to actions page appears.

Assign URL categories to different actions such as deny, permit, and log and permit.

- Under the Deny Action List section, click **Add URL Categories**.

The Select URL Categories page appears, as shown in [Figure 180 on page 374](#).

You can show all the categories, only the custom URL categories, or only the surfcontrol URL categories in the Available URL Categories column. Click **Create New URL Categories** to create a new URL category. You can inline create new URL categories and new URL pattern, as explained in Step 5.

- Similarly for Log & Permit Action List, Permit Action List, and Quarantine Action List sections, you can click the respective **Add URL Categories** option and select the required URL categories.
- Click **Next**. The Fallback Options page appears.

The URLs can be processed using their reputation score, if there is no category available. Choose the action that you wish to take for the uncategorized URLs based on their reputation score.

- In the Fallback Options section, select the Default Action as either Log and Permit or Block.

- Click **Next**.

The Summary page appears to review the configuration parameters selected to create a new web filtering profile.

- After reviewing, click **Finish**.

A new web filtering profile of engine type Surf Control is created.

7. If the Engine Type is Websense Redirect, configure the following parameters:

Under the General Information section, enter the following information:

- In the Name field, enter the name of the profile. The asterisk indicates that it is a mandatory field.
- In the Description field, enter a description for the new profile.
- From the list, select the required Engine Type.
- In the Account field, enter the user account associated with this Websense Web filtering profile.
- In the Server field, enter the hostname or IP address of the Websense server.
- In the Port field, enter the port number to use to communicate with the Websense server. The default port value is 15868.
- In the Socket field, enter the number of sockets used for communications between the client and server. The default value is 8. Leave blank for the default value.
- Enter the Timeout value in seconds. This determines the number of seconds to wait for a response from the Websense server.
- In the Custom Block Message field, enter the custom text to include in the Website not permitted response page.
- Click **Next**. The Fallback Options page appears.

The URLs can be processed using their reputation score, if there is no category available. Choose the action that you wish to take for the uncategorized URLs based on their reputation score.

- In the Fallback Options section, select the Default Action as either Log and Permit or Block.

- Click **Next**.

The Summary page appears to review the configuration parameters selected to create a new web filtering profile.

- After reviewing, click **Finish**.

A new web filtering profile of engine type Websense Redirect is created.

- Related Documentation**
- [UTM Overview on page 335](#)
  - [Creating a UTM Policy Using UTM Wizard on page 336](#)
  - [Managing UTM Policies on page 346](#)
  - [Managing Web Filtering Profiles on page 379](#)

---

## Managing Web Filtering Profiles

You can modify, delete, and clone the Web filtering profiles that are listed on the Web Filtering Profile main page.

To open the Web Filtering Profile page:

- Select **UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the Web Filtering Profiles page:

- [Modifying a Web Filtering Profile on page 379](#)
- [Deleting a Web Filtering Profile on page 380](#)
- [Cloning a Web Filtering Profile on page 380](#)
- [Finding Web Filtering Profile Usage on page 380](#)
- [Showing Unused Web Filtering Profiles on page 380](#)
- [Deleting All Unused Web Filtering Profiles on page 381](#)

### Modifying a Web Filtering Profile

To modify a Web filtering profile:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profiles page appears.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify Web Filtering Profile**.

The Modify Web Filtering Profile page appears.

3. On the Modify Web Filtering Profile page, you can modify the name, description, engine type, default action, timeout, custom block message, quarantine custom message, fallback options, site reputation actions, and URL category action list.
4. To modify the Web filtering profile, click **Modify**.

## Deleting a Web Filtering Profile

To delete a Web filtering profile:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

2. Select the profile that you want to delete, and click the minus sign or right-click and select the **Delete Web Filtering Profiles** option. A confirmation window appears before you can delete the profile.
3. To delete the Web filtering profile, click **Delete**.

## Cloning a Web Filtering Profile

To clone a Web filtering profile:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

2. Select the profile that you want to clone, right-click it, and select **Clone Web Filtering Profile**.

The Clone Web Filtering Profile page appears.

3. Modify any required field data in the Clone Web Filtering Profile page.
4. Click **Clone**.

The cloned Web filtering profile is created.

## Finding Web Filtering Profile Usage

To find the Web filtering profile usage:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

2. Select the profile for which you want to find the usage, right-click it, and select **Find Usage**.

The usage window appears, showing the usage of the selected profile.

## Showing Unused Web Filtering Profiles

To show unused Web filtering profiles:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

2. From Actions, select **Show Unused**.

The Web profiles that are not used by any UTM policies are listed.

## Deleting All Unused Web Filtering Profiles

To delete unused Web filtering profiles:

1. Select **Security Director > UTM Policies > Web Filtering Profiles**.

The Web Filtering Profile page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused policies.

Click **Yes** to confirm the deletion. All unused Web filtering profiles are deleted.

### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Creating a Web Filtering Profile on page 371](#)



# Creating and Managing URL Patterns

- [Creating a URL Pattern on page 383](#)
- [Managing URL Patterns on page 385](#)

## Creating a URL Pattern

A URL pattern is a list of URLs organized into a group. You can later assign this list to a URL category.

To create a URL pattern:

1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under the UTM Policies, select **URL Patterns**.

The URL Patterns page appears, listing the existing patterns, as shown in [Figure 183 on page 383](#).

**Figure 183: URL Patterns Main Page**



Name	Domain	Value	Description
ip-black-list	SYSTEM	http://*.sex.com,http://*.gamble.com,http://*.flashgames.com	
ip-major-black-list	SYSTEM	http://*.sex.com,http://*.gamble.com,http://*.flashgames.com	
ip-minor-black-list	SYSTEM	http://*.sex.com,http://*.gamble.com,http://*.flashgames.com	
ip-white-list	SYSTEM	http://*.work.com,http://*.taxes.com,http://*.networking.com	

3. To create a new web filtering profile, click the plus sign (+).

The Create URL Pattern page appears, as shown in [Figure 184 on page 384](#).

Figure 184: Create URL Pattern Page

4. In the Name field, enter the name of the URL pattern. The asterisk indicates that it is a mandatory field.
5. In the Description field, enter a description for the new URL pattern.
6. To create the URL pattern, enter URL(s) in the URL List field, and click **Add**. Separate multiple URLs

The URL List field supports the \*, ., [, ], and ? wildcard characters. Precede all wildcard character with http://. You can only use \* if it is at the beginning of the URL followed by a period, and you can only use ? at the end of the URL.

The following wildcard syntaxes are supported:

- http://\*.juniper.net
- http://www.juniper.ne?
- http://www.juniper.n??.

The following wildcard syntaxes are not supported:

- \*.juniper.net
- www.juniper.ne?

- [http://\\*juniper.net](#)
- [http://\\*](#)

All URLs entered in the URL List field are added to the URL List column. You can search for any particular URLs in the Search field.

If you want to delete any URL from the list, select the URL and click **Delete**.

7. Click **Create**.

A new URL pattern is created.

#### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing URL Patterns on page 385](#)

## Managing URL Patterns

You can modify, delete, and clone the URL patterns that are listed on the URL Pattern main page.

To open the URL Pattern page:

- Select **UTM Policies > URL Patterns**.

The URL Pattern page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the URL Patterns page:

- [Modifying a URL Pattern on page 385](#)
- [Deleting a URL Pattern on page 386](#)
- [Cloning a URL Pattern on page 386](#)
- [Finding URL Pattern Usage on page 386](#)
- [Showing Unused URL Patterns on page 386](#)
- [Delete All Unused URL Patterns on page 387](#)

### Modifying a URL Pattern

To modify a URL pattern:

1. Select **Security Director > UTM Policies > URL Patterns**.

The URL Pattern page appears.

2. Select the URL pattern that you want to modify, and click the pencil icon or right-click and select **Modify URL Pattern**.

The Modify URL Pattern page appears.

3. On the Modify URL Pattern page, you can modify the name, description, and URL list.  
You can also perform the inline modification of the URL pattern.
4. To modify the URL pattern, click **Modify**.

## Deleting a URL Pattern

To delete a URL pattern:

1. Select **Security Director > UTM Policies > URL Patterns**.  
The URL Pattern page appears.
2. Select the URL pattern that you want to delete, and click the minus sign or right-click and select the **Delete URL Patterns** option. A confirmation window appears before you can delete the profile.
3. To delete the URL pattern, click **Delete**.

## Cloning a URL Pattern

To clone a URL pattern:

1. Select **Security Director > UTM Policies > URL Patterns**.  
The URL Pattern page appears.
2. Select the URL pattern that you want to clone, right-click it, and select **Clone URL Pattern**.  
The Clone URL Pattern page appears.
3. On the Clone URL Pattern page, modify any required field data.
4. Click **Clone**.  
The cloned URL pattern is created.

## Finding URL Pattern Usage

To find the URL pattern usage:

1. Select **Security Director > UTM Policies > URL Patterns**.  
The URL Pattern page appears.
2. Select the URL pattern for which you want to find the usage, right-click it, and select **Find Usage**.  
The usage window appears, showing the usage of the selected pattern.

## Showing Unused URL Patterns

To show the unused URL patterns:

1. Select **Security Director > UTM Policies > URL Patterns**.

The URL Pattern page appears.

2. From Actions, select **Show Unused**.

The URL patterns that are not used by any UTM policies are listed.

## Delete All Unused URL Patterns

To delete the unused URL patterns:

1. Select **Security Director > UTM Policies > URL Patterns**.

The URL Patterns page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused patterns.

Click **Yes** to confirm the deletion. All unused URL patterns are deleted.

### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Creating a URL Pattern on page 383](#)



## CHAPTER 33

# Creating and Managing Custom URL Category Lists

- [Creating a Custom URL Category List on page 389](#)
- [Managing Custom URL Category Lists on page 391](#)

## Creating a Custom URL Category List

A URL category is a list of URL patterns grouped under a single title.

To create a new custom URL category list:

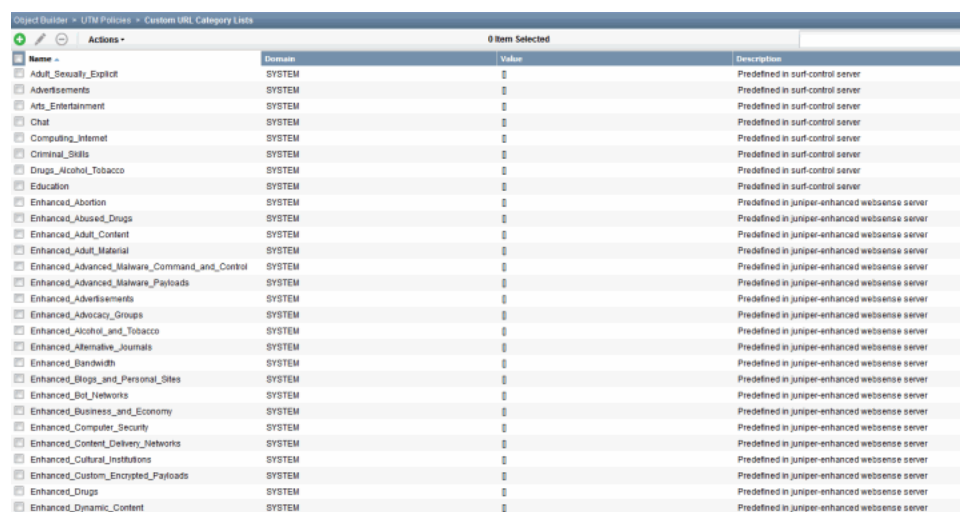
1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under UTM Policies, select **Custom URL Category Lists**.

The Custom URL Category Lists page appears, listing the existing URL categories, as shown in [Figure 185 on page 389](#).

Figure 185: Custom URL Category Lists Main Page



Name	Domain	Value	Description
<input type="checkbox"/> Adult_Explicit	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Advertisements	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Ads_Entertainment	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Chat	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Computing_Internet	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Criminal_Skills	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Drugs_Alcohol_Tobacco	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Education	SYSTEM		Predefined in surf-control server
<input type="checkbox"/> Enhanced_Abortion	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Abused_Drugs	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Adult_Content	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Adult_Material	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Advanced_Malware_Command_and_Control	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Advanced_Malware_Payloads	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Advertisements	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Advocsy_Groups	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Alcohol_and_Tobacco	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Alternative_Journals	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Bandwidth	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Blogs_and_Personal_Sites	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Bot_Networks	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Business_and_Economy	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Computer_Security	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Content_Delivery_Networks	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Cultural_Institutions	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Custom_Encrypted_Payloads	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Drugs	SYSTEM		Predefined in juniper-enhanced websense server
<input type="checkbox"/> Enhanced_Dynamic_Content	SYSTEM		Predefined in juniper-enhanced websense server

3. To create a new custom URL category list, click the plus sign (+).

The Create Custom URL Category List page appears, as shown in [Figure 186 on page 390](#).

**Figure 186: Create Custom URL Category List Page**

4. In the URL Category Name field, enter the name of the URL category list. The asterisk indicates that it is a mandatory field.
5. In the Description field, enter a description for the new URL category list.
6. From the Available Values column, select the required URL patterns and move them to the Selected Values column.

If you want to select the complete list, click **Page**.

7. Click **Create**.

A new custom URL category list is created.

**Related  
Documentation**

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing Custom URL Category Lists on page 391](#)

## Managing Custom URL Category Lists

---

You can modify, delete, and clone the custom URL category lists that are listed on the Custom URL Category List main page.

To open the Custom URL Category List page:

- Select **UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the Custom URL Category List page:

- [Modifying a Custom URL Category List on page 391](#)
- [Deleting a Custom URL Category List on page 391](#)
- [Cloning a Custom URL Category List on page 392](#)
- [Finding Custom URL Category List Usage on page 392](#)
- [Showing Unused Custom URL Category Lists on page 392](#)
- [Deleting All Unused Custom URL Category Lists on page 392](#)

### Modifying a Custom URL Category List

To modify a custom URL category list:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. Select the category list that you want to modify, and click the pencil icon or right-click and select **Modify Custom URL Category List**.

The Modify Custom URL Category List page appears.

3. On the Modify Custom URL Category List page, you can modify the name, description, and custom URL category list.
4. To modify the custom URL category list, click **Modify**.

### Deleting a Custom URL Category List

To delete a custom URL category list:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. Select the category list that you want to delete, and click the minus sign or right-click and select the **Delete Custom URL Category List** option. A confirmation window appears before you can delete the category list.
3. To delete the custom URL category list, click **Delete**.

## Cloning a Custom URL Category List

To clone a custom URL category list:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. Select the category list that you want to clone, right-click it and select **Clone Custom URL Category List**.

The Clone Custom URL Category List page appears.

3. On the Clone Custom URL Category List page, modify any required field data .
4. Click **Clone**.

The cloned custom URL category list is created.

## Finding Custom URL Category List Usage

To find a custom URL category list usage:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. Select the list for which you want to find the usage, right-click it, and select **Find Usage**.

The usage window appears, showing the usage of the selected list.

## Showing Unused Custom URL Category Lists

To show unused custom URL category Lists:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. From Actions, select **Show Unused**.

The custom URL category lists are not used by any UTM policies are listed.

## Deleting All Unused Custom URL Category Lists

To delete unused custom URL category lists:

1. Select **Security Director > UTM Policies > Custom URL Category List**.

The Custom URL Category List page appears.

2. From Actions, select **Delete All Unused**. A confirmation window appears before you can delete the unused category lists.

To confirm the deletion, click **Yes**. All unused category lists are deleted.

- Related Documentation**
- [UTM Overview on page 335](#)
  - [Creating a UTM Policy Using UTM Wizard on page 336](#)
  - [Managing UTM Policies on page 346](#)
  - [Creating a Custom URL Category List on page 389](#)



# Creating and Managing UTM Device Profiles

- [Creating a UTM Device Profile on page 395](#)
- [Managing Device Profiles on page 398](#)

## Creating a UTM Device Profile

---

A new profile object is available for UTM global options for a device. This object, the UTM device profile, has configurable properties and refers to the profiles for the following Security Director profile objects:

- Antivirus
- Web filtering
- Antispam

Security Director puts no restriction on creating a policy profile based on the global configurations. For example, if you select a antivirus global options type as Sophos, you can still create other profile types such as Kaspersky and others.

To create a new UTM device profile:

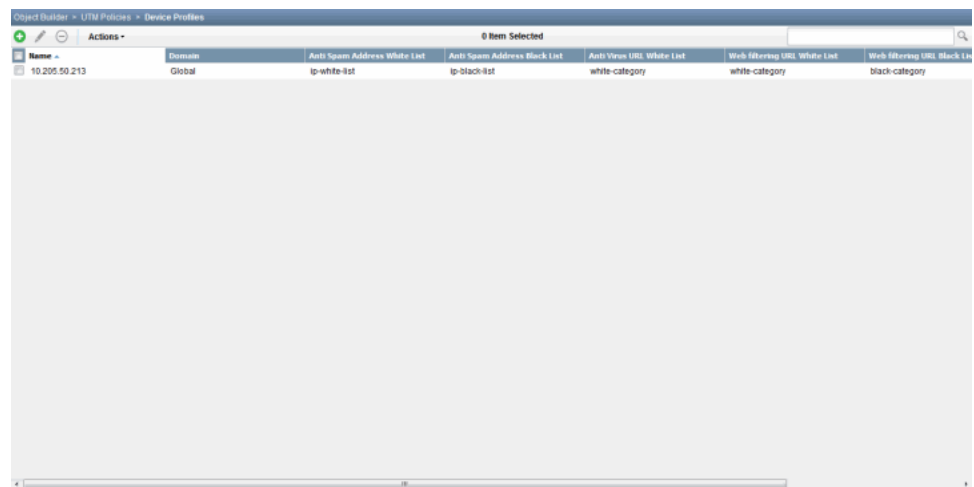
1. Select **Security Director > UTM Policies**.

The UTM Policies page appears.

2. In the left pane, under UTM Policies, select **Device Profiles**.

The Device Profiles page appears, listing the existing profiles, as shown in [Figure 187 on page 396](#).

Figure 187: Device Profiles Main Page



3. To create a new device profile, click the plus sign (+).

The Create UTM Device Profile page appears, as shown in [Figure 188 on page 397](#).

Figure 188: Create UTM Device Profile Page

**Create UTM Device Profile**

**GENERAL INFORMATION**

Name\*

Description

Device Selection

Available		Selected
Filter <input type="text"/> Select: Page   None		Filter <input type="text"/> Select: Page   None
10.207.97.195		
clust-41-node1 (Cluster)		
LSYS1(clust-41-node1) (Cluster)		
scale-vsrx		

Page 1 of 1

**Anti-Spam Profile** | Anti-Virus Profile | Web Filtering Profile

Address White List

Address Black List

Create Cancel

4. In the Name field, enter the name of the device profile. The asterisk indicates that it is a mandatory field.
5. In the Description field, enter a description for the new device profile.
6. To assign a device or devices to a profile, select the device or devices in the Available column, and move them to the Selected column.  
If a device is already assigned to a profiles, such devices are not listed in the Available column.
7. On the Anti-Spam Profile tab, configure the following parameters:
  - Select the address whitelist from the drop-down list of the Address White List field.
  - Select the address blacklist from the drop-down list of the Address Black List field.
8. On the Anti-Virus Profile tab, configure the following parameters:

- Enter MIME(s) in the MIME White List field.
  - Enter exception MIME(s) in the Exception MIME White List field.
  - Select the URL list from the URL White List drop-down list,
9. On the Web Filtering Profile tab, configure the following parameters:
- Select the URL whitelist from the drop-down list of the URL White List field.
  - Select the URL blacklist from the drop-down list of the URL Black List field.
10. Click **Create**.

A new UTM device profile is created.



**NOTE:** On the Device Profiles main page, In the Search field, you can search for a device with its IP address.

**Related  
Documentation**

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Managing Device Profiles on page 398](#)

---

## Managing Device Profiles

You can modify, delete, and clone the device profiles that are listed on the Device Profiles main page.

To open the Device Profiles page:

- Select **UTM Policies > Device Profiles**.

The Device Profiles page appears.

- Right-click the profile to manage it, or select the required options from Actions.

You can perform the following management tasks on the Device Profiles page:

- [Modifying a UTM Device Profile on page 399](#)
- [Deleting a UTM Device Profile on page 399](#)
- [Cloning a UTM Device Profile on page 399](#)
- [Showing Unused UTM Device Profiles on page 399](#)
- [Deleting All Unused UTM Device Profiles on page 400](#)

## Modifying a UTM Device Profile

To modify a device profile:

1. Select **Security Director > UTM Policies > Device Profiles**.

The Device Profiles page appears.

2. Select the profile that you want to modify, and click the pencil icon or right-click and select **Modify UTM Device Profile**.

The Modify UTM Device Profile page appears.

3. On the Modify UTM Device Profile page, you can modify name, description, and antispam, antivirus, and Web filtering profiles.
4. To modify the UTM device profile, click **Modify**.

## Deleting a UTM Device Profile

To delete a device profile:

1. Select **Security Director > UTM Policies > Device Profiles**.

The Device Profiles page appears.

2. Select the profile that you want to delete, and click the minus sign or right-click and select the **Delete UTM Device Profiles** option. A confirmation window appears before you can delete the device profile.
3. To delete the UTM device profile, click **Delete**.

You can select more than one profile to delete.

## Cloning a UTM Device Profile

To clone a device profile:

1. Select **Security Director > UTM Policies > Device Profiles**.

The Device Profiles page appears.

2. Select the profile that you want to clone, right-click it, and select **Clone UTM Device Profile**.

The Clone UTM Device Profile page appears.

3. On the Clone UTM Device Profile page, modify any required field data.
4. Click **Clone**.

The cloned UTM device profile is created.

## Showing Unused UTM Device Profiles

To show unused device profiles:

1. Select **Security Director > UTM Policies > Device Profiles**.

The Device Profile page appears.

2. From Actions, select **Show Unused**.

The device profiles that are not used by any UTM policies are listed.

## Deleting All Unused UTM Device Profiles

To delete unused device profiles:

1. Select **Security Director > UTM Policies > Device Profiles**.

The Device Profile page appears.

2. From Actions, select **Delete Unused**. A confirmation window appears before you can delete the device profile.

Click **Yes** to confirm the deletion. All device profiles that are not used by any UTM policies are deleted.

### Related Documentation

- [UTM Overview on page 335](#)
- [Creating a UTM Policy Using UTM Wizard on page 336](#)
- [Managing UTM Policies on page 346](#)
- [Creating a UTM Device Profile on page 395](#)

## PART 11

# Configuring NAT Policies

- [Understanding NAT on page 403](#)
- [Creating and Managing NAT Policies on page 409](#)
- [Creating and Managing NAT Pools on page 455](#)
- [Creating and Managing Port Sets on page 467](#)



# Understanding NAT

- [NAT Overview on page 403](#)
- [Global Address Book Overview on page 406](#)

## NAT Overview

---

Network Address Translation (NAT) is a form of network masquerading where you can hide devices between the zones or interfaces. A trust zone is a segment of the network where security measures are applied. It is usually assigned to the internal LAN. An untrust zone is the Internet. NAT modifies the IP addresses of the packets moving between the trust and untrust zones.

Whenever a packet arrives at the NAT device, 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 helps you hide internal IP addresses from the other networks and keep your network secure.

Using NAT also allows you to use more internal IP addresses. Because 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.

Junos Space Security Director supports three types of NAT:

- **Source NAT**—Translates the source IP address of a packet leaving the trust zone (outbound traffic). It translates the traffic originating from the device in the trust zone. Using source NAT, an internal device can access the network by using the IP addresses specified in the NAT policy.

The following use cases are supported with IPv6 NAT:

- Translation from one IPv6 subnet to another IPv6 subnet without Port Address Translation (PAT)
- Translation from IPv4 addresses to IPv6 prefixes along with IPv4 address translation
- Translation from IPv6 host(s) to IPv6 host(s) with or without PAT
- Translation from IPv6 host(s) to IPv4 host(s) with or without PAT
- Translation from IPv4 host(s) to IPv6 host(s) with or without PAT

- **Destination NAT**—Translates the destination IP address of a packet entering the trust zone (inbound traffic). It translates the traffic originating from a device outside the trust zone. Using destination NAT, an external device can send packets to a hidden internal device.

The following use cases are supported with IPv6 NAT:

- Mapping of one IPv6 subnet to another IPv6 subnet
- 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 webserver with a private IP address can access the Internet using a static, one-to-one address translation.

The following use cases are supported with IPv6 NAT:

- Mapping between one IPv6 subnet and 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 host(s) and IPv6 host(s)
- Mapping between IPv6 host(s) and IPv4 host(s)

[Table 31 on page 404](#) shows the persistent NAT support for different source NAT and destination NAT addresses.

**Table 31: 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 32 on page 405](#), and [Table 33 on page 405](#) show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 32: Translated Address Pool Selection for Source NAT

Source Address	Destination Addresses	Pool Address
IPv4	IPv4	IPv4
IPv4	IPv6 Subnet must be greater than 96.	IPv6
IPv6	IPv4	IPv4
IPv6	IPv6	IPv6

Table 33: Translated Address Pool Selection for Destination NAT And Static NAT

Source Address	Destination Addresses	Pool/Translated 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 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.

Junos Space Security Director provides you with a workflow where you can create and apply NAT policies on devices in a network.

Security Director views each logical system as any other security device and takes ownership of the security configuration of the logical system. In Security Director, each logical system is managed as a unique security device.



**NOTE:** If the root logical system is discovered, all other user logical systems inside the device, will also be discovered.

Because an SRX Series logical system device does not support interface NAT, Security Director also does not allow interface NAT configuration of logical system. The logical system cannot participate in group NAT in Security Director. For a device NAT policy, the interface based translation selection and pool with Overflow Pool as interface are not supported in logical systems. The configuration is validated during the publishing of the NAT policy to avoid commit failures in the device.

**Related  
Documentation**

- [Creating NAT Policies on page 409](#)
- [Publishing NAT Policies on page 433](#)
- [Managing NAT Policies on page 436](#)
- [Managing NAT Pools on page 459](#)
- [Global Address Book Overview on page 406](#)

---

## Global Address Book Overview

In Junos OS Release 11.2 and later releases, the address book is moved from the zone level to the device global level. This permits objects to be used across many zones and avoids inefficient use of resources. This change also permits nested groups to be configured within the address book, removing redundancy from repeating address objects.

The Security Director application manages its address book at the global level, assigning objects to devices that are required to create policies. If the device is capable of using a global address book, Security Director pushes address objects used in the policies to the device global address book. Nested address group capability is used in the publish and update feature of Security Director depending on the device capability.

## Differences Between Global and Zone-Based Address Books

The global address book is supported in Junos OS Release 11.2 and later releases.

- An address book is not configured within a specific zone; therefore, one address book can be associated with multiple zones.
- If a global address book is defined, you cannot create zone-based address books.
- By default, there is an address book called *global* associated with all zones.
- A zone can be attached to only one address book in addition to the global address book, which contains all zones by default.
- Address name overlaps are possible between the global address book and zone address book. For example, Security Director will attempt to match an address in the zone-based address book first, and, if the address is not found, the global address book is checked. You must ensure that the correct address objects are used in the policy.
- NAT rules can use address objects only from the global address book. They cannot use addresses from user-defined address books.



NOTE: Beginning in Junos OS Release 12.1, zone-based address books are no longer supported. Devices running Junos OS Release 12.1 or later must use the global address book.



NOTE: Beginning in Junos OS Release 11.2, NAT rules can use address objects from the global address book. However, Security Director will still continue to define the NAT address in the rule itself rather than referring to the global address book.

**Related  
Documentation**

- [NAT Overview on page 403](#)
- [Creating NAT Policies on page 409](#)
- [Managing NAT Policies on page 436](#)



## CHAPTER 36

# Creating and Managing NAT Policies

- Creating NAT Policies on page 409
- Unlocking Locked Policies on page 423
- Ordering the Rules in a NAT Policy on page 424
- Adding Rules to a NAT Policy on page 427
- Publishing NAT Policies on page 433
- Managing NAT Policies on page 436

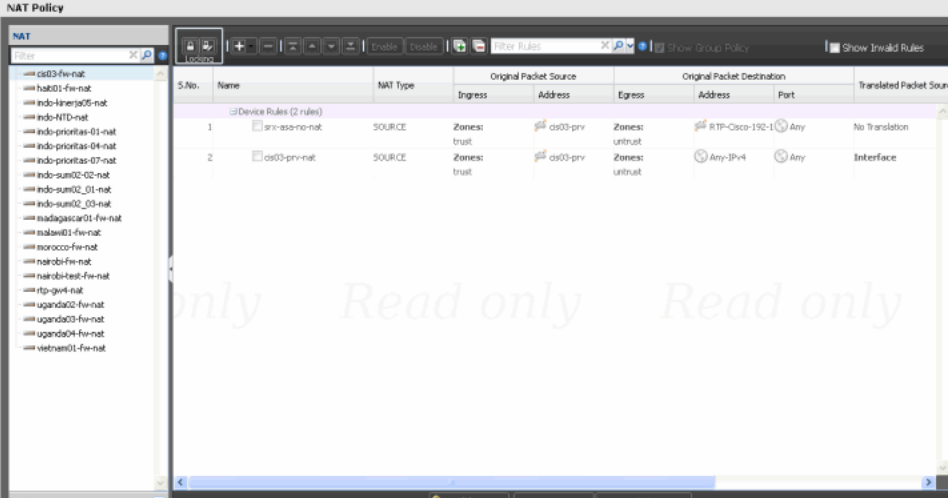
## Creating NAT Policies

To create a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears, as shown in [Figure 189 on page 409](#). NAT Policy Tabular view is a table with two panes. The left pane displays all the NAT policies in the system, which includes device, group, and global NAT policies.

Figure 189: NAT Tabular View



S.No.	Name	NAT Type	Ingress	Address	Egress	Address	Port	Translated Packet Source
1	any-ssm-no-nat	SOURCE	Zone:	os03-priv	Zone:	RTP-Cisco-192-1	Any	No Translation
2	os03-priv-nat	SOURCE	Zone:	os03-priv	Zone:	Any-IP-v4	Any	Interface

2. Click **Create NAT Policy** from the left pane.

The Create NAT Policy page appears. You can create a group policy or a device policy on this page.

3. To create a group policy:
  - a. Enter the name of the group policy in the Name field.
  - b. Enter a description for the group policy rules in the Description field. Security Director sends the comments entered in this field to the device.
  - c. Click the Show Assigned Devices check box to make devices on which policies have been configured available for selection.
  - d. Select the devices on which the group policy will be published in the Select Devices pane. Select the devices from the Available column and click the right arrow to move these devices to the Selected column.

You can also search for the devices by entering the device name, device IP address, or device tag in the Search field in the Select Devices section. Once the searched devices are displayed, you can move them to the Selected column as shown in [Figure 190 on page 410](#).

**Figure 190: Create NAT Policy Page**

**Create NAT Policy**

Type: ☒ Group ☐ Device

Name:

Description:

☐ Enable Auto ARP Configuration

☐ Show only devices without policy assigned

Available		Selected	
Filter	Select: All   None	Filter	Select: All   None
10.205.230.1	Global		
10.205.230.10	Global		
10.205.230.100	Global		
10.205.230.101	Global		
10.205.230.102	Global		
10.205.230.103	Global		
10.205.230.104	Global		
10.205.230.105	Global		
10.205.230.106	Global		
10.205.230.107	Global		
10.205.230.108	Global		
Total: 568			

Create Cancel

- e. Click **Create**.

During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is

disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.



**NOTE:**

- One device can hold configuration data related to one NAT policy only. Therefore you cannot share devices for multiple NAT policies.
- All logical systems are now available for selection for a group NAT policy. These logical systems support the Translated Packet Source match type as Interface.

4. To create a device policy:

- Enter the name of the device policy in the Name field.
- Enter a description for the device policy in the Description field.
- Select the device on which the device policy will be published from the Device menu.
- Click **Create**.

During a device assignment for a device policy, only devices from the current domain are listed.

All devices policy enables rules to be enforced globally to all the devices managed by Security Director. All devices policy is part of the Global domain and is visible in all the child domains if the view parent is enabled.

Validate policies by clicking the **Validate** button, available next to the Save and Discard buttons. If any errors are found during the validation, a red warning icon is shown for the respective policies. For NAT policies, incomplete rules and duplicate rule names are validated.

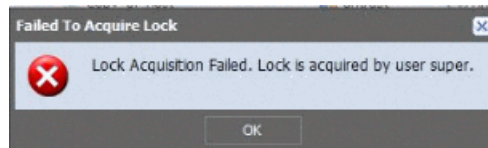
Security Directors permits you to save policies that contain errors. Warnings messages are displayed for policies that contain errors, but you can proceed to save such policies as drafts. You cannot publish policies that are in the draft state. The tooltip for the policy shows the state as draft; because it is a draft, the tooltip does not show the publish option.



**NOTE:** If you do not have permission to the device assigned to a device policy, you cannot view the policy in the respective policy ILP.

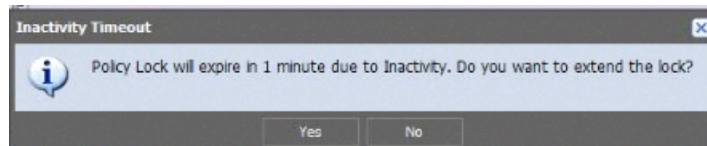
Before you can edit the policy, you must lock it by clicking the lock icon, which is available in the policy tabular view, as shown in [Figure 189 on page 409](#). You can hold more than one policy lock at a given time. You can unlock the policy by clicking the unlock icon next to the lock icon in the policy tabular view. If you attempt to lock a policy that is already locked by another user, the following message appears, as shown in [Figure 191 on page 412](#). The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

**Figure 191: Lock Failure Error Message for the Second User**



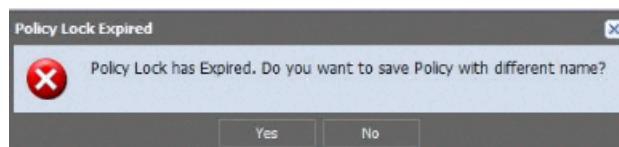
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 192 on page 412](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see [“Unlocking Locked Policies” on page 423](#).

**Figure 192: Inactivity Timeout Error**



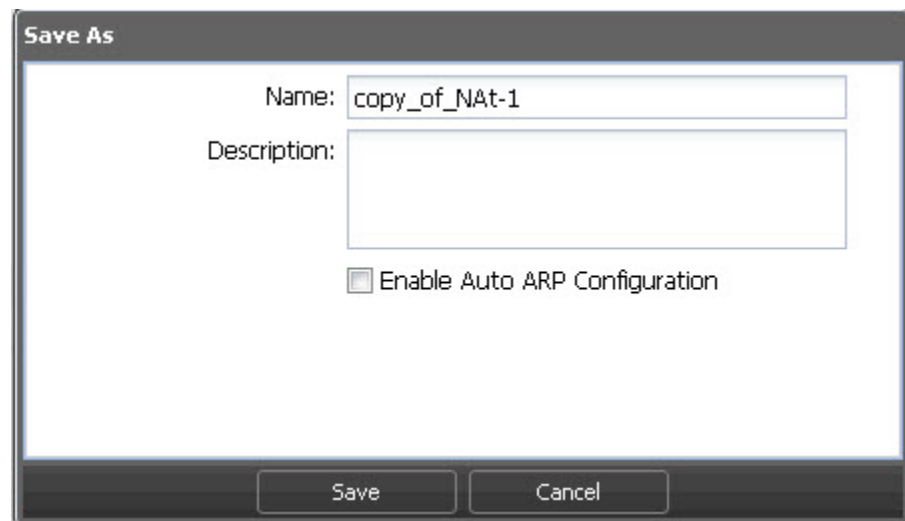
Click **Yes** to extend the locking period. If you click **No**, and if there is activity on the policy within the last minute of the lock's life, the timer will be reset and the lock will not be released. If you ignore the message, when the policy lock timeout interval expires 1 minute later, you are prompted to either save the edited policy with a different name or lose the changes, as shown in [Figure 193 on page 412](#).

**Figure 193: Policy Lock Expired Message**



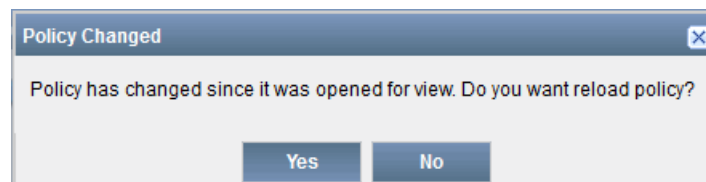
If you click **Yes** to save the edited policy with a different name, the following window appears, as shown in [Figure 194 on page 413](#). If you navigate away from the locked policy, either the policy is unlocked (when there are no changes) or you will get an option to save the edited policy with a different name.

Figure 194: NAT Locked Policy-Save As Window



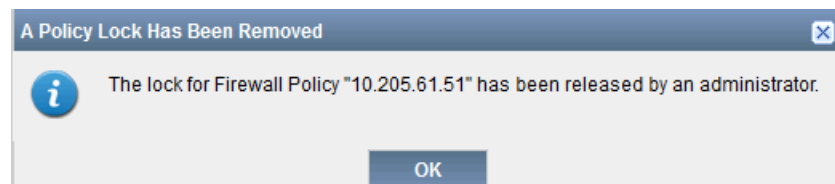
After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 195 on page 413](#).

Figure 195: NAT Policy-Unsaved Changes Message



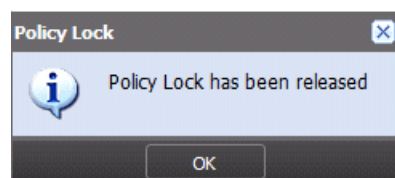
If the Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 196 on page 413](#).

Figure 196: NAT Policy- Policy Unlock by Admin Message



If you do not edit the locked policy and the policy lock timeout expires, the following warning message appears, as shown in [Figure 197 on page 413](#).

Figure 197: NAT Policy Lock Release Message



The policy is locked and released for the following policy operations. Also, these operations are disabled for a policy, if the policy is locked by some other user.

- Modify
- Assign devices
- Rollback
- Delete



**NOTE:**

- You can unlock the policy by logging out of the application or when the policy lock timeout expires. You can unlock your policies even if they are not edited.
- If the browser crashes when the policy is still locked, the policy is unlocked only after the timeout interval expires.
- If there is an object conflict resolution during a migration, import, or rollback, and if you are editing any objects, you will receive a save as option for the edited objects. The behavior is the same when you import addresses from CSV.
- Policy lock is not released under the following scenario:
  - If you save or discard you changes to the locked policy.
  - if you do not make any changes to the locked policy and navigate to another policy.
- It is recommended to configure the session time longer than the lock timeout value.

---

To perform an inline addition of a new NAT pool object in the source NAT pool:

1. Click **Translated Packet Source** and select **Translation Type** as Pool.

Figure 198: Setting Source NAT Pool Page

2. Click the plus sign to create the source NAT pool.

Figure 199: Create Source NAT Pool Page

You can select **No Translation**, **Port/Range**, or **Overload** for the Translation field.

3. Click **Create** to create the source NAT pool or **Cancel** to discard the changes.

To perform inline addition of a new NAT pool object in the destination NAT pool:

1. Click **Translated Packet Destination** and select **Pool** for the Translation Type.

Figure 200: Setting the Destination Pool Page

Translation Type: Pool

Destination Pool: Haiti\_Server\_NAT

Ok Cancel

2. Click the plus sign (+) to create the destination NAT pool.

Figure 201: Create Destination NAT Pool Page

Create Destination NAT Pool

Name:

Description:

Pool Address: Select Address ...

Port:

Create Cancel

3. Click **Create** to create the destination NAT pool or **Cancel** to discard the changes.



**NOTE:** Advanced NAT pool options must be modified from the Object Builder workspace in the NAT pool ILP.

To create address objects or address group for the NAT policy:

1. Click the source address. The following window appears with the available addresses to create the objects.

Figure 202: Create Inline NAT Address Object

Available

Filter

Select: All None

10.159.2.0/25 (10.159.2.0/25)	Global
10.159.3.0/24 (10.159.3.0/24)	Global
10.159.4.0/24 (10.159.4.0/24)	Global
144.201.76.32 (144.201.76.32)	Global
Addr-66.0.192.112/28 (66.0.192.112/28)	Global
Addr-66.184.206.216 (66.184.206.216)	Global
ADDR-DNS-VIP-v6 (2001:4888:2::a0:d:...	Global
ADDR-GROUP-v4 (group)	Global

Total: 209

Host Network Range Other

Ok Cancel

Selected

Select: All None

2. Click on the plus sign (+) to create the new address object or address group for NAT policy.

There are two radio buttons available to create a new address object or address group, as shown in [Figure 203 on page 417](#). By default, the Address radio button is selected.

**Figure 203: Create NAT Address Page**

3. Click **Create** to create the new address object or **Cancel** to discard all changes.

To create address groups for Source and Destination NAT rules of source address:

1. Select the Address Group radio button to create the new address group.

[Figure 204 on page 417](#) shows the page that appears.

**Figure 204: Inline Address Group Creation for NAT Policy**

Available		Selected	
Filter	Select: All   None		Select: All   None
10.159.2.0/25 (10.159.2.0/25)	Global		
10.159.3.0/24 (10.159.3.0/24)	Global		
10.159.4.0/24 (10.159.4.0/24)	Global		
144.201.76.32 (144.201.76....)	Global		
Addr-66.0.192.112/28 (66.0....)	Global		
Addr-66.184.206.216 (66.18....)	Global		
Total: 211			

2. Enter the name of an address group in the Name field.
3. In the Addresses filed, you can select all addresses available in the Available column or select few addresses to create a new address group.
4. Click **Create** to create the address group. This adds the newly created address objects to the selected addresses and returns to the address selector. Click **Cancel** to discard your changes and return to the NAT ILP.



**NOTE:** Follow the same steps to create objects for the Source NAT rule for the destination address. You can create address object inline similar to address group inline.

To add Junos OS protocols to the NAT policy:

1. Click on any column and select the **Protocol** check box. The Protocol column is added in the NAT ILP.

This column is not enabled by default.

2. Click the **Protocol** column for the required policy, and a separate window appears, listing all the protocols.

The supported protocol range is from 0 to 255 in the Junos OS Release 11.4 and later. For a single rule, you can choose up to four protocols.

[Table 34 on page 418](#) shows the protocols that have unique names. The other protocols, which do not have names, are identified with numbers.

**Table 34: Junos OS Protocol Names**

Protocol Name	Description
ah	Authentication Header
egp	Exterior gateway protocol
esp	Encapsulating Security Payload
gre	Generic routing encapsulation
icmp	Internet Control Message Protocol
icmp6	Internet Control Message Protocol version 6
igmp	Internet Group Management Protocol
ipip	IP over IP
ospf	Open Shortest Path First
pim	Protocol Independent Multicast
rsvp	Resource Reservation Protocol
sctp	Stream Control Transmission Protocol
tcp	Transmission Control Protocol
udp	User Datagram Protocol

3. Select the required protocols from the list, and click **OK**.

You can send the protocols to clusters, logical systems, or standalone devices. You can perform a normal or global search of protocols with names or numbers.

You can search for NAT policies in the left pane using NAT policy names and devices used in the NAT policy. You can search the rules in the right pane using NAT rule type, original packet source, original packet destination, translated packet source, translated packet destination, and the description used in the rule.

Tooltip view is available to show the object value information for the objects that you are using within the policies. Mouse over the source address or destination address and objects information is provided in the tool tip. The tooltip contains address group name, value of the address such as IP, and subnet.

Security Director provides advanced search options for NAT policies. Click the down arrow icon next to the search icon and select **Advance Search**, and the following box appears, as shown in [Figure 205 on page 419](#).

**Figure 205: Advanced Search Box for NAT Policies**

The screenshot shows a web-based 'Advance Search' dialog box. It features a title bar with the text 'Advance Search'. Below the title bar, there are several search criteria sections. The first section is 'Rule Name' with a text input field. The second section is 'Type' with a dropdown menu. The third section is 'Original Packet Source' with a sub-section containing 'Ingress' and 'Address' text input fields. The fourth section is 'Original Packet Destination' with a sub-section containing 'Egress', 'Address', and 'Port' text input fields. The fifth section is 'Translated Packet Address' with a text input field. At the bottom of the dialog, there are three buttons: 'Filter', 'Reset', and 'Cancel'.

You can perform advanced searches for the following fields:

- Rule Name
- Type—Type of NAT (source, destination, or static)
- Original Packet Source
  - Ingress—Zone, interface, or routing instance
  - Address
- Original Packet Destination
  - Egress—Zone, interface, or routing instance
  - Address

- Port
- Translated Packet Address
- Description
- Custom column

The following advanced search criteria are available:

- Wildcard search for rule names using an asterisk (\*) is allowed.
- For a rule name search, only the OR operation is allowed, because a policy cannot have multiple rule names.
- For source and destination addresses, both AND and OR operations are allowed.
- For ingress and egress fields, both AND and OR operations are allowed.
- For port, you can only use the OR operation.
- Translated packet address field can only use the OR operation.
- Multiple groups can be grouped using parenthesis. Grouping can be used during filed or keyword searches as well.
- Negate (-) symbol can be used to exclude objects that contain a specific term name.
- The plus (+) operator can be used to specify that the term after the + symbol existing the field value to be filtered along with other searched items.
- Escaping special characters are part of the search syntax. The supported special characters are + - & || ! ( ) { } [ ] ^ " ~ \* ? : \.

[Table 35 on page 420](#) explains certain specific Security Director search behavior.

**Table 35: Specific Security Director Search Behavior**

Search Item	Description
IPv4 addresses	If you provide a valid IPv4 address, range, or network in the search field, Security Director finds all addresses that include these IPv4 address, range, or network.
Destination port in service	If you configured a destination port range of a service, Security Director matches ports within this range but this is valid only during field or keyword search.
Keyword or field	If you require to search specific attributes in an object as opposed to global search, you can use keyword or field search.

[Table 36 on page 420](#) shows example search results for different parameters.

**Table 36: Example: Different Advanced Search Parameters for NAT**

Scenario	Query Parameter	Description
Wildcard search for rule names	RuleName:( Device* )	Rule names starting with <i>Device</i> are filtered.

Table 36: Example: Different Advanced Search Parameters for NAT (*continued*)

Scenario	Query Parameter	Description
Search rule name along with NAT type	RuleName:( <i>rs1</i> ) AND dcNatRuleType:( SOURCE )	Source NAT with rule name <i>rs1</i> are filtered.
Ingress zone with address to egress zone with address	Ingress:( <i>trust</i> ) AND SrcAddress:( <i>add1_1</i> ) AND Egress:( <i>trust</i> ) AND DstAddress:( 2.2.2.2/32 )	Rules with ingress zone <i>trust</i> , address <i>add1_1</i> , and egress zone <i>trust</i> , address 2.2.2.2/32, are filtered.
Ingress zone with address to egress zone with address, along with the port number	dcNatRuleType:( DESTINATION ) AND Ingress:( <i>zone</i> ) AND SrcAddress:( 2.2.2.2/32 ) AND DstAddress:( any-ipv4 ) AND Service:( 1024 )	Destination NAT rule having ingress as <i>zone</i> , source address as 2.2.2.2/32, destination address as <i>any-ipv4</i> , and port number as 1024 are filtered.  You can provide the port number (1024) or the port range (1024 65535).
Search rule name with translated packet source address	RuleName:( <i>r1</i> ) AND dcNatRuleType:( SOURCE ) AND Ingress:( <i>trust</i> ) AND SrcAddress:( <i>add1_1</i> ) AND Egress:( <i>trust</i> ) AND DstAddress:( 2.2.2.2/32 ) AND Service:( 1024 65535 ) AND TranslatedPacketAddress:(src-pool )	Source rules with rule name <i>r1</i> , source address <i>add1_1</i> , egress zone <i>trust</i> , destination address 2.2.2.2/32, port 1024 or 65535, and translated packet address <i>src-pool</i> are filtered.



**NOTE:** You can also search by giving IPv6 addresses in the source field or the destination address field.

To hide the policies in the left pane that do not have any defined rules:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Empty Device Policies** check box to hide the device exception policies that do not have any rules, as shown in [Figure 206 on page 422](#).

Figure 206: Policy View Settings



3. Policies with no defined rules are hidden in the left pane.

To hide the policies in the left pane that do not have any devices assigned:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Policies With No Devices Assigned** check box to filter device and group policies that are not assigned to any device, as shown in [Figure 206 on page 422](#).
3. Policies without any assigned devices are hidden in the left pane.

#### Related Documentation

- [Adding Rules to a NAT Policy on page 427](#)
- [Ordering the Rules in a NAT Policy on page 424](#)
- [Publishing NAT Policies on page 433](#)
- [Managing NAT Policies on page 436](#)

## Unlocking Locked Policies


All the locked policies can be viewed in a single page. This page is available for a user with Manage Policy Locks tasks assigned. This page shows all the locks only if the user has Unlock task assigned, other wise user will see only his locks. To view the locked policies:

1. Select **Security Director > NAT Policy > Manage Policy Locks**.

The Manage Policy Locks page appears showing only those locks that can be managed by the current user. The page contains the following fields:

- Policy name
- User (IP Address)
- Lock acquired time
- Time for lock expiry

Figure 207: NAT Policy-Manage Policy Locks



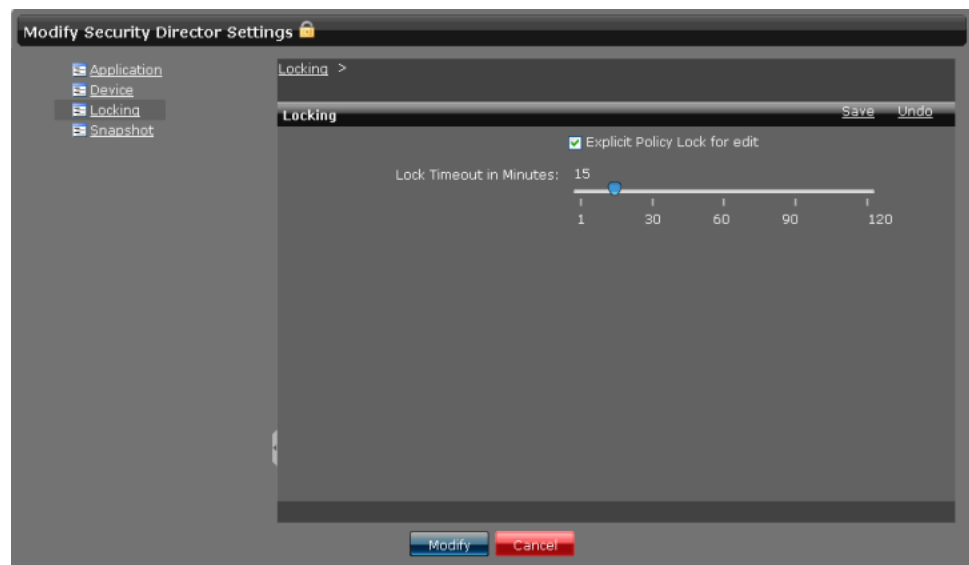
Policy	User	Lock Acquired Time	Lock Expires In
FW_3150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 23 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilo	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	3 Mins 50 Secs

2. Right-click the policy that you want to unlock, and press **Unlock**. You can select policies that are locked by you and unlock them. To unlock your policies, you do not need any administrator privileges. To unlock policies locked by other users, you must have the task LOCK assigned to you.

User with administrator privileges can configure the lock settings. To configure the lock settings:

1. Click on **Application Switcher** option, and go to **Network Application Platform > Administration > Manage Applications**.
2. Right click the Security Director application, and select **Modify Application Settings**. The following page appears, as shown in [Figure 208 on page 424](#).

Figure 208: Modify Security Director Settings



3. Under the Locking option, you can configure the locking timeout value in minutes. The minimum value that you can configure is 2 minutes and the maximum is 120 minutes. By default, the timeout value is configured for 5 minutes.
4. By default, the Explicit Policy Lock for edit option is enabled. You can disable this option, if you do not want to lock the policies before editing. When this option is disabled, policies can be edited by any user. The behavior is the same as for concurrent editing. The first user gets the preference of saving the changes for a policy. The next save on the same version of a policy results in the user being asked to save the policy with a new name.



**NOTE:** Acquiring a policy lock or releasing lock is audit logged. Release locking will show the reason for the release, for example, an explicit release, on save, discard, timeout, or administrator release. Administrator changes of the lock configuration are also audit logged. To see the audit logs, from the Security Director task bar, select Audit Logs.

**Related Documentation**

- [Creating NAT Policies on page 409](#)
- [Managing NAT Policies on page 436](#)

## Ordering the Rules in a NAT Policy

To reorder the rules in a NAT policy:

1. Select **Security Director > NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to reorder.

The rules of the NAT policy are displayed in the right pane.

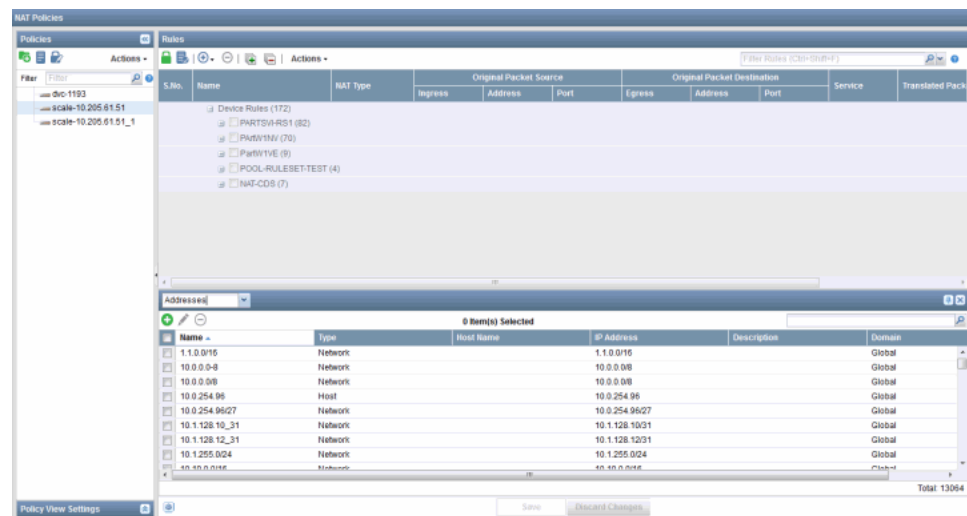
3. Select a rule that you want to reorder and click the appropriate icon on the top of the right pane.

Icon Name	Description
Move Rule Up	Moves the rule one level up in the hierarchy.
Move Rule Down	Moves the rule one level down in the hierarchy.
Move Rule to Top	Moves the rule to the top of the hierarchy.
Move Rule to Bottom	Moves the rule to the bottom of the hierarchy.

The rule is now positioned accordingly. When the NAT policy is provisioned, the rules are provisioned to the devices in the order you have specified.

The address, service, and NAT pools objects can be created, managed, dragged and dropped to the required rules from the NAT policy landing page. The objects are listed in the policy landing page, as shown in [Figure 209 on page 425](#)

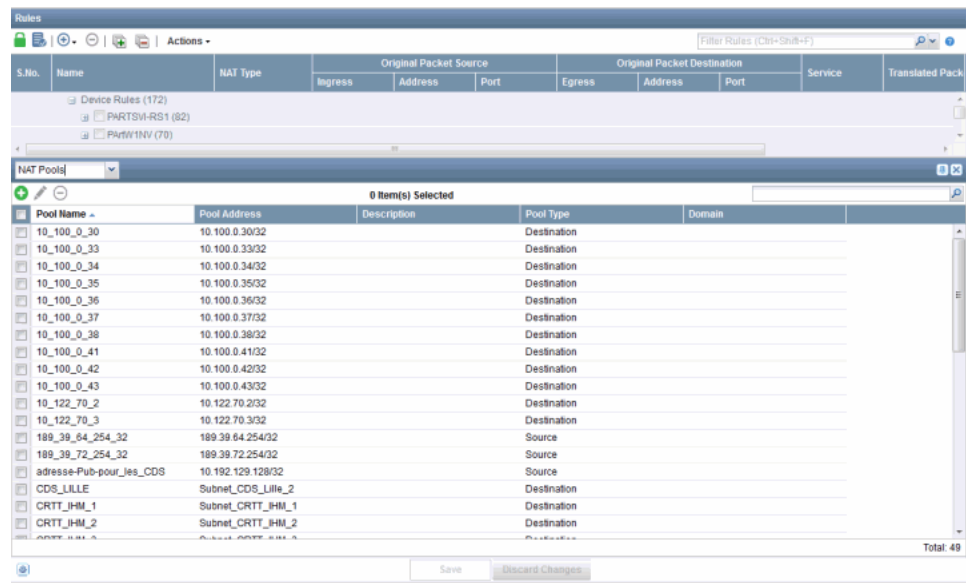
**Figure 209: NAT Policies Landing Page**



You can select address, service, or a NAT pool objects from the drop-down list. To create a new address, service, or a NAT pool object, click the plus sign (+). To know more about creating these objects, see [“Creating Addresses” on page 124](#), [“Creating Services” on page 108](#), and [“Creating NAT Pools” on page 456](#).

You can modify an object by clicking the pencil icon and delete objects by clicking the minus sign (-). You can search for any object by its name and IP address in the search field available in the top right corner, as shown in [Figure 210 on page 426](#)

Figure 210: NAT Policies-Drag and Drop Objects Window



You can drag more than one object and drop on the respective columns in the policy tabular view. Security Director ensure that objects are dropped in the supported columns and it does not permit to drop under any other columns. The drag and drop of objects is supported on the Source Address, Destination Address, and Service columns. You can drag source or destination NAT pool (only a single item) and drop into source or destination NAT rule. Before dropping any object to the policy rules, you must first lock the respective policy. A single address can be dragged and dropped from source address field to destination address field of the same rule or across the rules. A single service also can be dragged and dropped across the rules in NAT policy. Single source or destination NAT pool can be dragged and dropped across rules. However, you cannot drag and drop multiple items across rules. In the NAT policy landing page, you can reorder the rules by dragging and dropping.

You can drag and drop the objects across the rules. If an object already exists for a rule and your drop a new object, the previous object is over written by the new object. The new object is copied to the rule.

#### Related Documentation

- [Creating NAT Policies on page 409](#)
- [Adding Rules to a NAT Policy on page 427](#)
- [Publishing NAT Policies on page 433](#)
- [Managing NAT Policies on page 436](#)

## Adding Rules to a NAT Policy

When a new NAT policy is created, by default the policy displays links to create rules for the policy. If you have created a group NAT policy, you will see a Create Source Rule link in the right pane. If you have any cut or copied rules or rule groups, you will also have Paste Rules to paste the rules or rule groups. If you have created a device NAT policy, you will see Create Source Rule, Create Destination Rule, and Create Static Rule links, and also Paste Rules to paste the rules or rule groups.

Depending on the type of rule you have chosen, some fields in the rule will not be applicable. If you choose a source NAT rule, the Translated Packet Destination field will not be applicable. If you choose a destination NAT rule, the Egress field in the Original Packet Destination column and the Translated Packet Source fields are not applicable. If you choose a static NAT rule, the Address field in the Original Packet Source column, the Egress field in the Original Packet Destination column, Port field in the Original Packet Destination column, and Translated Packet Source fields are not 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.

The Proxy ARP option is available under different fields based on the type of rule you have chosen. With a static NAT rule, the Proxy ARP option is available under the Translated Packet Source field. With the destination NAT rule and static NAT rule, the Proxy ARP option is available under the Address field in the Original Packet Destination column.

The Proxy ARP feature also automatically selects the interface based on the Egress field for source NAT rule and the Ingress field for destination NAT rule and static NAT rule. The auto Proxy ARP is enabled by default. It is only applicable for imported, migrated, and cloned NAT policies.



**NOTE:** Based on the IP version used, Security Director pushes either Proxy ARP or Proxy NDP CLI command to the device. GUI shows only the Proxy ARP check box.

To add rules to a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Click the NAT policy you want to add rules to from the left pane.

The existing rules of the NAT policy are displayed in the right pane.

3. Click the + icon to add rules, and select the type of rule you want to add.

A new rule is added in the last row depending on the type of rule you have added. The newly added rules blink with a different color for few seconds. The behavior is same if you add a new rule before or after a rule, clone a rule, or paste a rule.

The rule is assigned a serial number based on the number of rules already added to the policy. By default, the zones are set to Empty, and the address and port of the packet source and packet destination are set to Any. The Translated Source and Translated Packet Source columns are either set to No Translation or Not Applicable, depending on the rule you are adding.

4. Click the **Name** field in the rule and change the name of the rule.
5. Click the **Ingress** field in the Original Packet Source column and select the appropriate zone or interface or routing instance.

The Zone or Interface or routing instance selector appears.

6. Select the appropriate option from the Source Traffic Matching Type drop-down menu.
7. In the zone or interface or routing instance selector, select the zones or interfaces or routing instance you want to associate the rule to, from the Available column.

On selection of Routing Instance option, you can select one or more of the available virtual routers on the device. For the group NAT policy, the consolidated list of all virtual routers on all devices that the policy is assigned to will be listed.

8. Click the right arrow in the selector.

The selected zones or interfaces or virtual routers are moved to the Selected column.

9. Click **OK**.
10. Click the **Address** field in the Original Packet Source column and select the appropriate addresses.

The Address selector appears.

11. In the address selector, select the addresses you want to associate the rule to, from the Available section. You can select all addresses by clicking **Page** and unselect them all by clicking **None**.
12. Click the right arrow in the selector.

The selected addresses are now moved to the Selected section.

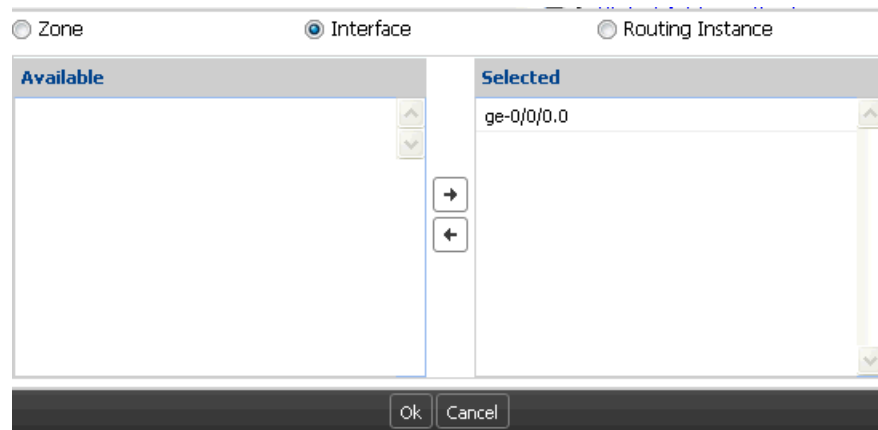
13. Click **OK**.
14. Click the **Port** field in the Original Packet Source column to enter the source port numbers. Source NAT supports a source port for the original packet source. For all rules, the source port is added to the Original Packet Source column. The source Port field is disabled for the destination NAT. The port numbers must be separated by commas, and a maximum of eight entries is allowed, including ports and port ranges.

The Address and Port fields are also available in the Original Packet Source field for Static NAT.

15. Click the **Egress** field in the Original Packet Destination column and select the appropriate zone or interface or routing instance.

The zone or interface or routing instance selector appears.

Figure 211: Destination Traffic Match Type Selector Page



16. Select the appropriate option from the Destination Traffic Matching Type list.

17. In the zone or interface or routing instance selector, select the zones and interfaces or routing instance you want to associate the rule to, from the Available column.

18. Click the right arrow in the selector.

The selected zones or interfaces or routing instance are now moved to the Selected column.

19. Click **OK**.

20. Click the **Address** field in the Original Packet Destination column and select the appropriate addresses.

The Address selector appears.

21. In the address selector, select the addresses you want to associate the rule to, from the Available column. You can select all addresses by clicking **Page** and unselect them all by clicking **None**.

22. Click the right arrow in the selector.

The selected addresses are now moved to the Selected column.

23. Click **OK**.

24. Click the **Port** field in the Original Packet Destination column.

You can enter a single port value or the port range. The devices running Junos OS Release 12.1X47 and later releases support multiple ports and ranges, in the same way as does the Source port.

Click **Select Port Sets** to expand and choose port sets. The maximum number of ports or port ranges that you can configure in a single rule is 8. A validation error is displayed in a tooltip if you select more than 8 ports or port ranges.

The device capability of the port set is validated based on the matching schema version and not on the Junos OS version running on the device.

25. Click the **Service** column to select one or more services for the source and destination type NAT rules. This is supported for the devices running Junos OS Release 12.1X47.

Select the required services from the Available column and move them to the Selected column. You can also create services inline by clicking the plus sign (+).



**NOTE:** NAT rule cannot reference a combination of port, protocol, and service options. If service information is configured, you cannot configure port and protocol. Publishing of services is validated based on the schema.

26. Click the **Translated Packet Source** field.

27. Select the appropriate translation type from the Translation Type drop-down menu.

- a. If you select **Pool** as the option from the Translation Type drop-down menu, you will see that there will be new fields to specify.
- b. Select the appropriate NAT pool from the Source Pool drop-down menu.  
All relevant options from the NAT pool you have chosen are displayed.
- c. Select the **Configure Proxy ARP** check box to enable the proxy ARP feature.
- d. Select the check boxes next to the address ranges you want to include and select the appropriate interface.

28. Click **OK**.

29. Click the **Destination Address** field in the Translated Packet Destination column and select the appropriate addresses.

This option is available only for destination NAT rule.



**NOTE:** For static NAT rule, you can configure Routing Instance from the Translated Packet Destination column.

30. Select the type of translation from the Translation Type drop-down menu.

31. Select the appropriate NAT pool from the Destination Pool drop-down menu.



**NOTE:** If you are creating a static NAT rule, the Translated Address list appears. You can select the appropriate address from the list.

32. Click **OK**.

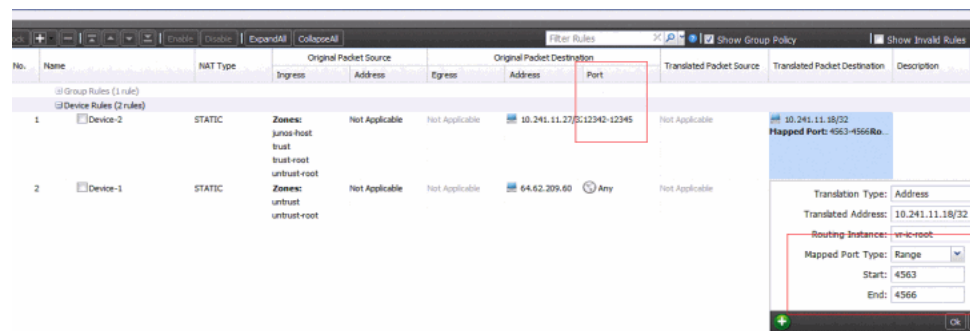
33. Click the Port field in the Original Packet Destination column.

The port selector appears.

34. Select the appropriate port type from the Port Type drop-down menu.

You can configure static NAT destination and mapped ports (single port, range of ports, or no ports) along with destination and translated addresses. This is supported in Junos OS Releases 12.1 R13.5, 12.1X44-D1, and 11.4R5.5. If the destination port is configured, destination and translated addresses must be host addresses. The destination and translated host addresses can be either IPv4, or IPv6 version.

Figure 212: Port Configuration for Static NAT



If the device Junos OS version is previous to the Junos OS Release 12.1R3.5, and there is a schema mismatch in Security Director, a warning message is displayed during the preview of NAT CLI.

35. Click **OK**.

36. Click the **Description** field and enter a description for the rule.

37. Click **Save**.

Security Director automatically generates the rule set names, each consisting of alphabets, numbers, underscore, and hyphen. A rule set name has only 30 characters, with the last 4 characters reserved for the counter value that is used if two rule sets have the same name. Security Director will truncate the rule set name if it goes beyond 26 characters.

A rule set name for source, destination, and static NAT rules is created as follows:

- Source NAT rule—The rule set name is created by taking the first value of the ingress and the first value of the egress, along with the match type (zone, routing instance, or interface). If two rule set names are the same, a counter value is appended to the end of one of the names.

Rule set name format for source NAT rules: <Ingress

Type>\_<firstIngressValue>-<EgressType>\_<firstEgressValue>-<nextCounterValue>

Table 37 on page 431 shows the rule set names for different ingress and egress values.

**Table 37: Example: Rule Set Names for Different Ingress And Egress Values of Source NAT Rules**

Ingress and Egress Value	Rule Set Name
source rule1 from zone trust to zone untrust	Zone_trust-Zone_untrust
source rule2 from zone trust to zone untrust,dmz	Zone_trust-Zone_untrust-1
source rule3 from zone trust to zone untrust,dmz,xyz	Zone_trust-Zone_untrust-2
source rule4 from Routing instance vrouter1, vrouter2 to zone dmz,xyz	RI_vrouter1-Zone_dmz
source rule5 from interface fe-0/0/1.0 to zone dmz,xyz	IF_fe-0010 -Zone_dmz

- Destination NAT and static NAT rules—The rule set name is created by taking the first and second value of the ingress, along with the match type (zone, routing instance, interface). If two rule set names are the same, a counter value is appended to the end of one of the names.

Rule set name format for destination NAT and static NAT rules: <Ingress Type>\_<firstIngressValue>\_<secondIngressValue>—<nextCounterValue>

Table 38 on page 432 shows the rule set names for different ingress values.

**Table 38: Example: Rule Set Names for Destination NAT and Static NAT**

Ingress Value	Rule Set Name
static rule1 from zone trust	Zone_trust
source rule2 from zone trust,untrust	Zone_trust_untrust
source rule3 from zone trust,untrust,dmz	Zone_trust_untrust-1



**NOTE:** During NSM migration and publish, Security Director will create the rule set names.

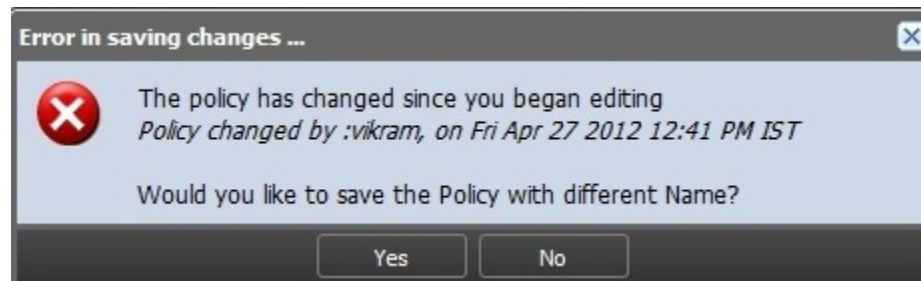


**NOTE:** You should click Save to save any changes you have made to the NAT policy. While in the process of making changes to the NAT policy, If you click on any of the tasks in the task ribbon before saving the NAT policy changes, all changes you have made will be lost. If you click anywhere inside the NAT Policy Tabular view, you will see a confirmation window to save the changes you have made.



**NOTE:** If another user has added new rules to the same policy, modified the existing rules, or deleted existing rules, and that user had already saved the changes before you, you will see the error message as shown in [Figure 213 on page 433](#).

Figure 213: Concurrent NAT Policy Editing Error



The error message provides the user name and time at which changes were made to the policy. Whoever saves the changes first gets the preference to save the new rules added. You will be given an option to save your policy changes with a different name. Click Yes to save the policy with a different name. Only saved rules are published to the policy.

#### Related Documentation

- [Ordering the Rules in a NAT Policy on page 424](#)
- [Publishing NAT Policies on page 433](#)
- [Managing NAT Policies on page 436](#)

## Publishing NAT Policies

To publish a NAT policy:

1. Select **Security Director > NAT Policy > Publish policy**.

The Services page appears with all the NAT policies. It also displays the publish states of the NAT policies.

2. Select the check box next to the NAT policy that you want to publish.

**NOTE:**

- You can search for a specific device on which the policy is published by entering the search criteria in the Search field, in the top-right corner of the Services page. You can search the devices by their name, IP address, and device tags.
- If the NAT policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices, to view all devices on which the policy is published.
- Publish fails if two addresses are having the same name.

3. Select the **Schedule at a later time** check box if you want to schedule and publish the configuration later.

4. Click **Next**.

The Affected Devices page displays the devices on which this NAT policy will be published.

5. If you want to preview the configuration changes that will be pushed to the device, click **View** in the Configuration column corresponding to the device. A Configuration Preview progress bar is shown while the configuration pushed to the device is generated.

The CLI Configuration tab appears by default. You can view the configuration details in CLI format.

**Figure 214: NAT Policy CLI Configuration**

```

Configuration for device
CLI Configuration 100% Configuration

##Global address book configurations##
set security address-book global address 10.220.21.254/32 10.220.21.254/32
set security address-book global address 10.33.33.193/32 10.33.33.193/32
set security address-book global address 10.33.57.5/32 10.33.57.5/32
set security address-book global address 10.80.0.192/32 10.80.0.192/32
set security address-book global address 10.80.0.193/32 10.80.0.193/32
set security address-book global address 163.Srv_FBT_2 223.192.163.2/32
set security address-book global address test123 1.2.3.4/32

##source-nat-rule-set##
set security nat source rule-set Zone_test1-Zone_test2 from zone test1
set security nat source rule-set Zone_test1-Zone_test2 from zone test2
set security nat source rule-set Zone_test1-Zone_test2 to zone test2
set security nat source rule-set Zone_test1-Zone_test2 rule Device-1 match source-address 0.0.0.0/0
set security nat source rule-set Zone_test1-Zone_test2 rule Device-1 match destination-address 0.0.0.0/0
set security nat source rule-set Zone_test1-Zone_test2 rule Device-1 then source-nat off

##source-nat-rule-set##
set security nat source rule-set Zone_test3-Zone_test3 from zone test3
set security nat source rule-set Zone_test3-Zone_test3 from zone test4
set security nat source rule-set Zone_test3-Zone_test3 to zone test3
set security nat source rule-set Zone_test3-Zone_test3 to zone test4
set security nat source rule-set Zone_test3-Zone_test3 rule Device-2 match source-address 0.0.0.0/0
set security nat source rule-set Zone_test3-Zone_test3 rule Device-2 match destination-address 0.0.0.0/0
set security nat source rule-set Zone_test3-Zone_test3 rule Device-2 then source-nat off

##source-nat-rule-set##
set security nat source rule-set IF_Esp00-IF_Esp00 from interface Esp0.0
set security nat source rule-set IF_Esp00-IF_Esp00 from interface st0.2
  
```

6. View the XML format of the configuration by clicking the XML Configuration tab.

7. Click **Back**.

8. Click **Publish** if you want to only publish the configuration.

A new job is created and the job ID appears in the Job Information dialog box.

9. Click **Publish and Update** if you want to publish and update the devices with the configuration.

The NAT policy is now moved into the Published state if the configuration is published to all devices involved in the policy. If the configuration is not published to all devices involved in the NAT policy, the NAT policy is placed in the Partially Published state. If a NAT policy is created but not published, the NAT policy is placed in the Unpublished state. If any modifications are made to NAT policy configuration after it is published, the NAT policy is placed in the Republish Required state. You can view the states of the NAT policy by mousing over them. When an address object in the Global domain referenced by a policy in the D1 domain changes, the state of the policy is changed to Republish Required. This occurs though the changes are in the address object, which is in the other domain, and is not same as the policy domain. This applies to all the objects referenced by all the services.

A new job is created and the job ID appears in the Job Information dialog box.

10. Click the job ID to view more information about the job created. This action directs you to the Job Management workspace.

If you get an error message during the publish or if the NAT policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed.

In the Job Details window, use the available filter box to search for any device by filter name, tag name, or IP address. Filtering works only for currently available devices.

Search with the first character of the tag name to search by tag name. If you search with any middle characters, the search fails.

During the publish and update, the disabled rules and objects are not deleted. Disabled rules are updated as inactive configuration. This is an optional setting. You can choose to push the disabled rules to a device by selecting **Update disabled rules to device** option in Security Director application setting, under Platform. By default, Update disabled rules to device option is disabled. For the pushed disabled rules to work after the upgrade, Security Director must import the policy again and the application firewall signature must be downloaded prior to the import.

If you are having the disabled rules on the device, as shown in the following example:

```
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
destination-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
application any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 then
deny
deactivate security policies from-zone untrust to-zone trust policy Device-Zone-5
```

When you import this rules, Security Director sets the state as disabled. If a particular node in the CLI is deactivated, that node is not imported into the Security Director.

If you import a rule, as shown in the following example, Security Director will not set the application service.

```
set security policies from-zone trust to-zone untrust policy Device-Zone-2
description "Rule With Infranet All Traffic Auth"
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
```

```
source-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
destination-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
application any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
permit application-services idp
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
permit application-services uac-policy captive-portal captiveportal_65573
deactivate security policies from-zone trust to-zone untrust policy Device-Zone-2
then permit application-services
```

Security Director does not support inactive nodes and the inactive rules. If the objects in the rule are not defined, Security Director provides a warning message, at the time of import, listing the objects that are not defined.

**NOTE:**

- You can also publish a NAT policy by right-clicking the NAT policy in the NAT Policy Tabular view and selecting Publish NAT Policy. You are redirected to the Affected Devices page.
  - You cannot publish a group NAT policy, if you do not have permission for all the assigned devices. Also publish is not permitted if one or more devices are labeled by another Junos Space user.
  - The publish fails if you have two addresses in a rule with a same name, one from the Global domain and the other from the child domain.
  - You can publish or update the group policy of the global domain from another domain. In this case, policy is published or updated to only those devices which are part of the another domain. However, if you publish or update the group policy in the global domain, the policy is published or updated to all the devices including the devices from the another domain.
  - If a NAT rule with multiple destination port or service configuration is published to a device running the previous version of Junos OS Release 12.1X47, publish fails with an error message.
  - The maximum allowed services for a NAT rule is 3072. If the services exceed more than 3072, publish fails with an error message.
- 

**Related Documentation**

- [Creating NAT Policies on page 409](#)
- [Adding Rules to a NAT Policy on page 427](#)
- [Ordering the Rules in a NAT Policy on page 424](#)
- [Managing NAT Policies on page 436](#)

---

## Managing NAT Policies

---

- [Modifying NAT Policies on page 437](#)
- [Deleting NAT Policies on page 437](#)

- [Cloning NAT Policies on page 438](#)
- [Exporting a NAT Policy on page 438](#)
- [Configuring NAT Rule Sets on page 438](#)
- [NAT Policy Versioning on page 439](#)
- [Managing NAT Policy Versioning on page 440](#)
- [Deleting Rules in a NAT Policy on page 445](#)
- [Grouping Rules in a NAT Policy on page 445](#)
- [Enabling/Disabling Rules in a NAT Policy on page 445](#)
- [Expanding/Collapsing All Rules in a NAT Policy on page 446](#)
- [Cutting/Copying and Pasting Rules or Rule Groups in a NAT Policy on page 446](#)
- [Assigning Devices to a NAT Policy on page 448](#)
- [Deleting Devices from a NAT Policy on page 448](#)
- [Rule Operations on the Filtered Rules on page 449](#)
- [Showing NAT Policy for a Corresponding Log on page 450](#)
- [Viewing Logs Generated by the NAT Rule on page 452](#)

## Modifying NAT Policies

To modify a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Right-click the NAT policy you want to modify from the left pane and select **Modify Policy**.

The Edit Policy window appears. You can modify the name and description of the NAT policy.

3. Click **Modify**.

Whenever you make any changes to the NAT policy, you will have the option of entering a comment before saving the policy. You can enable or disable this option in Platform > Administration > Applications. To enable this option, right-click **Security Director**, and select the **Modify Security Director Settings** option. Under Applications, select the **Enable save comments for policies** check box. By default, this option is disabled.

In NAT ILP, once you enter the comment, you can save this version with a different name. Click **Save as Draft** from Save drop-down list to save the edited NAT policy with a different name. Entering a comment is not required. All comments you enter are logged.

## Deleting NAT Policies

To delete a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Right-click the NAT policy you want to delete and select **Delete Policy**.

A confirmation window appears.

3. Click **Yes**.



**NOTE:** If you delete a NAT policy, the erase configuration is sent to all devices that were a part of the NAT policy during the next Update operation for the device.

## Cloning NAT Policies

To clone a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Right-click the NAT policy you want to clone and select **Clone Policy**.

The Clone Policy window appears. You can modify the name and description mode of the NAT policy.

3. Click **Clone**.

## Exporting a NAT Policy

To export a NAT policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Right-click the NAT policy you want to export and select **Export Policy**.

The Export Policy window appears.

3. Click **Export**.

## Configuring NAT Rule Sets

To configure a NAT rule set:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

2. Right-click the NAT policy you want to configure the rule set and select **Configure RuleSets**.

The Configure Rule Set window appears.

3. Modify the rule set name in the Rule Set column and click **Save** to save the changes.

## NAT Policy Versioning

You create a policy version by taking a snapshot of the policy. You can create versions for all types of NAT policies, including group and device exceptions. The maximum number of versions maintained for any policy is 60. If the maximum limit is reached, you must delete the unwanted versions before taking a new version snapshot. You can delete the older version of snapshots by clicking the **Auto delete oldest version** option, as shown in [Figure 216 on page 440](#). This option is enabled by default. If this option is disabled, every time the oldest version of snapshots are deleted (after the maximum number of versions is reached), a warning message is displayed on the screen. If you enable this option, the oldest snapshots are deleted automatically, without any warning messages.

Versioning and rollback are independent operations for each policy. For example, if you take a snapshot of a group NAT policy, you must create a separate version of each policy rule.

To create a version of the policy:

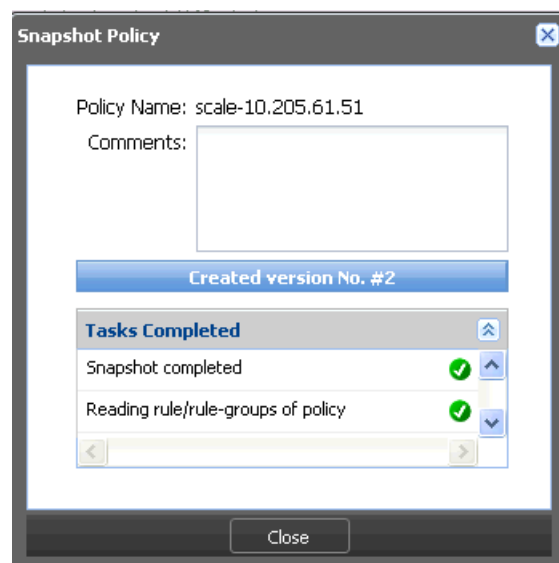
1. Select **Security Director > NAT Policy**.

The Policy Tabular view appears.

2. Right-click the NAT policy you want to take a snapshot of, and select **Snapshot Policy**.

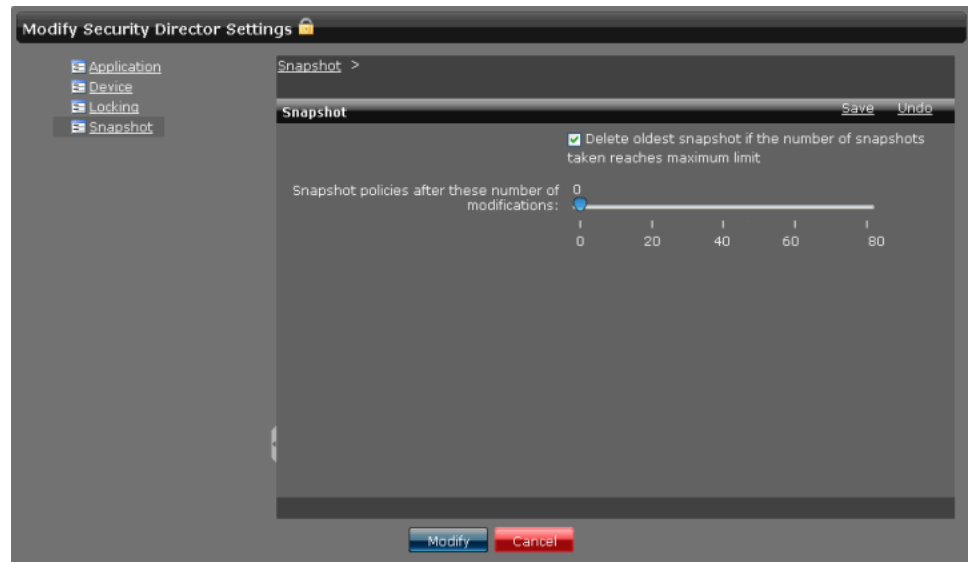
The Policy Name field shows the name of the NAT policy for which the snapshot is taken. Enter your comments in the Comments field, and press **Create to take the snapshot**. The Snapshot Policy Window appears, showing the status of the version as it is created, as shown in [Figure 215 on page 439](#).

**Figure 215: Snapshot Policy**



**NOTE:**

- During policy publish, Security Director takes an automatic snapshot of the policy.
- You can set an option to take the snapshot automatically after you have modified and saved a policy after configured number of times, as shown in [Figure 216 on page 440](#). When the snapshot is taken automatically, Security Director does not make any log entry because it is an internal operation.

**Figure 216: Modify Security Director Settings**

- NAT versioning includes the destination port and services as part of the versioned data you can compare when searching for changes across different versions.

## Managing NAT Policy Versioning

You can view or manage all available versions of a selected policy. You can perform the following tasks on the snapshots:

- Roll back to a specific version.
- View the differences between any two versions (including the current version) of the policy.
- Delete one or more versions from the system.

To roll back the selected version as the current version:

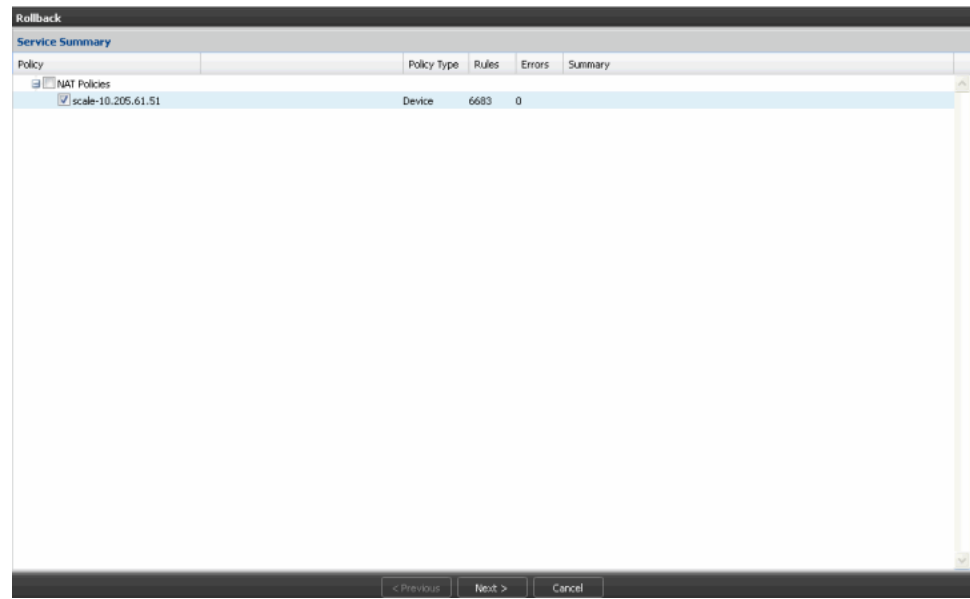
1. Select **Security Director > NAT Policy**.  
The Policy Tabular view appears.
2. Right-click the nat1 policy, and select **Manage Snapshots**.

A window appears showing all the versions of the policy.

3. Select the version that you want to make current and click **Rollback**.

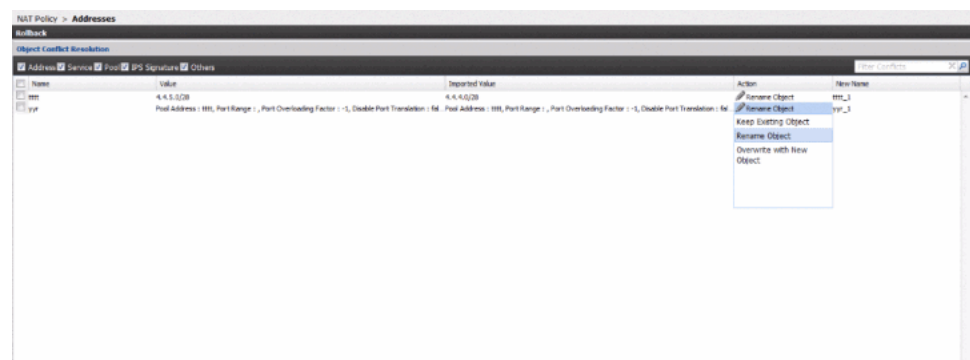
A service summary window appears, as shown in [Figure 217 on page 441](#).

**Figure 217: Rollback Service Summary Report**



The rollback operation replaces all the rules and rule groups of the current version with rules and rule groups from the selected version. For all the shared objects, Object Conflict Resolution (OCR) is performed. If there are any conflicts between the versioned data and the current objects in the system, the OCR window is displayed, as shown in [Figure 218 on page 441](#).

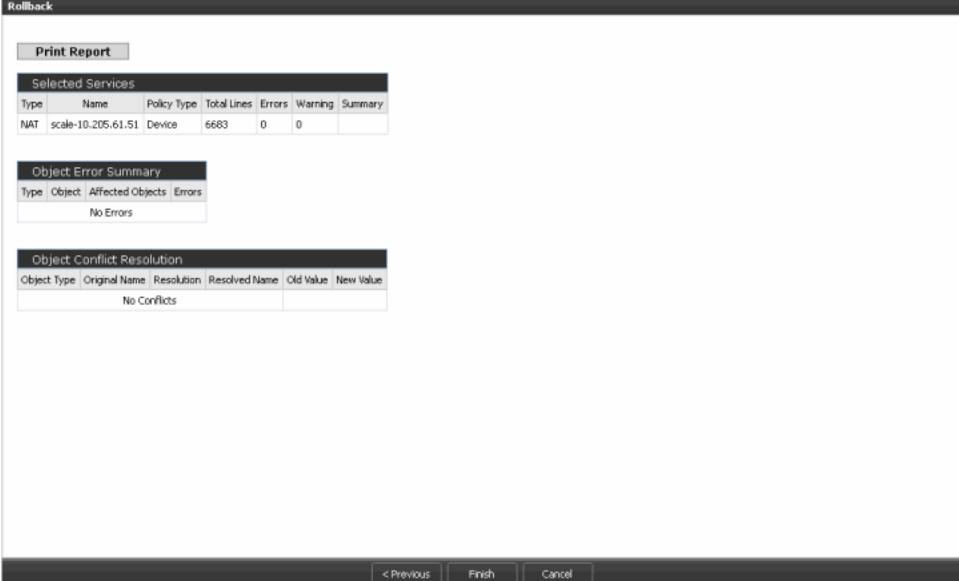
**Figure 218: Object Conflict Resolution Window**



From the OCR window, you can choose to retain the existing object, rename the existing object, or overwrite the existing object with the new object.

4. After finishing all the conflict resolution, click **Next** to view the OCR summary report, as shown in [Figure 219 on page 442](#).

Figure 219: Rollback OCR Summary Report



**Rollback**

**Print Report**

**Selected Services**

Type	Name	Policy Type	Total Lines	Errors	Warning	Summary
NAT	scale-10.205.61.51	Device	6683	0	0	

**Object Error Summary**

Type	Object	Affected Objects	Errors
No Errors			

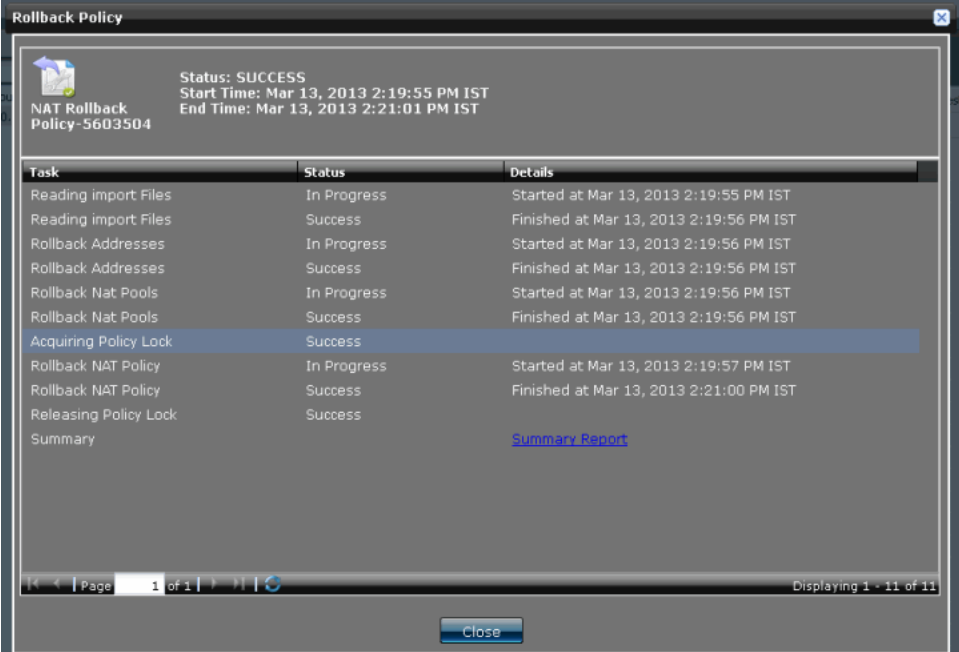
**Object Conflict Resolution**

Object Type	Original Name	Resolution	Resolved Name	Old Value	New Value
No Conflicts					

< Previous Finish Cancel

- Click **Finish** to replace the current policy with the versioned data. A summary of the snapshot policy is provided, as shown in [Figure 220 on page 442](#).

Figure 220: Rollback Policy Summary Report



**Rollback Policy**

**Status: SUCCESS**  
**Start Time: Mar 13, 2013 2:19:55 PM IST**  
**End Time: Mar 13, 2013 2:21:01 PM IST**

**NAT Rollback Policy-5603504**

Task	Status	Details
Reading import Files	In Progress	Started at Mar 13, 2013 2:19:55 PM IST
Reading import Files	Success	Finished at Mar 13, 2013 2:19:56 PM IST
Rollback Addresses	In Progress	Started at Mar 13, 2013 2:19:56 PM IST
Rollback Addresses	Success	Finished at Mar 13, 2013 2:19:56 PM IST
Rollback Nat Pools	In Progress	Started at Mar 13, 2013 2:19:56 PM IST
Rollback Nat Pools	Success	Finished at Mar 13, 2013 2:19:56 PM IST
Acquiring Policy Lock	Success	
Rollback NAT Policy	In Progress	Started at Mar 13, 2013 2:19:57 PM IST
Rollback NAT Policy	Success	Finished at Mar 13, 2013 2:21:00 PM IST
Releasing Policy Lock	Success	
Summary		<a href="#">Summary Report</a>

Page 1 of 1 | Displaying 1 - 11 of 11

Close

To compare two different versions of a policy:

1. Select **Security Director > NAT Policy**.

The Policy Tabular view appears.

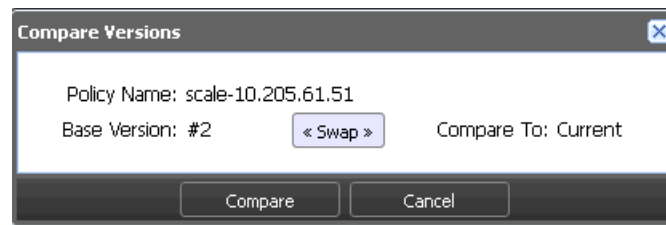
2. Right-click the NAT policy, and select **Manage Snapshots**.

The Manage Versions window appears, showing all policy versions.

3. Select the versions to be compared, and click **Compare**. You can select only two versions at a time to compare.

You can swap the version that you want to make the base version and compare it with the other version by clicking **Swap**, as shown in [Figure 221 on page 443](#).

**Figure 221: Compare Versions with Swap Option**



4. Click **Compare** to view the results.

A Compare Versions window appears, showing the differences between the selected versions, as shown in [Figure 222 on page 443](#).

**Figure 222: Versions Comparing Summary Report**

**Policy Property Changes**

Property	scale-10.205.61.51#1	scale-10.205.61.51#Current
PublishedState	Not Published	Re-publishing Required

**NAT Rule Changes**

Rule Name	NAT Type	Original Packet Source			Original Packet Destination			Translated Packet Source	Translated Packet Destination	Description	Protocol
		Ingress	Address	Egress	Address	Port					

The modified column is highlighted in blue as a hyper link. If you click the modified column, it takes you to the Rule Column Change section to the specific column. Click **NextDiff** to view the each diff. The each diff is highlighted in yellow.

The Compare Versions window has the following sections:

- **Policy Property Changes**—Shows policy changes for the modified rules.
- **Rule Changes**—Displays rules that are added, modified, or deleted.
- **Column Changes**—Shows the differences between the column contents for modified rules.

The Port column is compared based on the effective value of the column content. For example, in version 1 of the policy, the port is configured with the inline values 10, 20, and 30. In version 2 of the policy, the port column is configured to use the port set. Therefore, the policy diff does not show that the Port column is changed. Although the string representations of the column values are different, the effective port values are the same and are therefore considered not to have changed.

To delete versions:

1. Select **Security Director > NAT Policy**.

The Policy Tabular view appears.

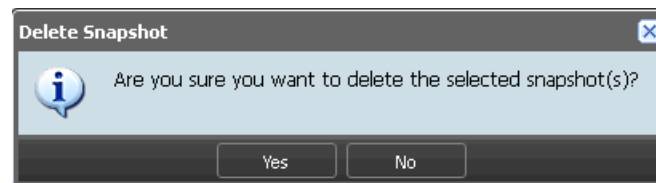
2. Right-click the NAT policy, and select **Manage Snapshots**.

A window appears, showing all policy versions.

3. You can delete multiple versions at one time. When you perform a rollback operation, you are given the option to delete older versions. Select the version that you want to delete, and click **Delete**.

You will receive a Confirm Delete Operation message before you can delete the version, as shown in [Figure 223 on page 444](#).

**Figure 223: Snapshot Delete Confirm Window**



4. Click **Yes** to delete the version, or click **No** to abort the operation.



**NOTE:** If you delete a policy, all versioned data for that policy is deleted.

## Deleting Rules in a NAT Policy

To delete rules in a NAT policy:

1. Select **Security Director > NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to delete.  
The rules of the NAT policy appears in the right pane.
3. Select the check boxes next to the rules that you want to delete.
4. Click the **Delete Rule** icon on the top of the right pane.

## Grouping Rules in a NAT Policy

To group rules in a NAT policy:

1. Select **Security Director > NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to group.  
The rules of the NAT policy are displayed in the right pane.
3. Select the check boxes next to the rules you want to group.
4. Right-click the rules and select **Rule Group > Create Rule Group**.  
The Create Rule Group window appears.
5. Enter a name for the rule group in the Name field.
6. Enter a description for the rule group in the Description field.
7. Click **Create**.



**NOTE:** When the rule group is created, you can add a rule into the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

## Enabling/Disabling Rules in a NAT Policy

To enable or disable rules in a NAT policy:

1. Select **Security Director > NAT Policy**.  
The NAT Policy Tabular view appears.
2. Select the NAT policy whose rules you want to enable or disable.  
The rules of the NAT policy appears in the right pane.

3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.



**NOTE:** You can enable or disable a rule group. When a rule group is disabled, all rules in the rule group are also disabled. The rule group row in the Tabular view is greyed out but the rules are not greyed out. However, the rules in the rule group are not published to the device during the publish operation, if they are disabled.

## Expanding/Collapsing All Rules in a NAT Policy

To expand or collapse all rules in a firewall policy:

1. Select **Security Director > NAT Policy**.

The NAT Policy Tabular view appears.

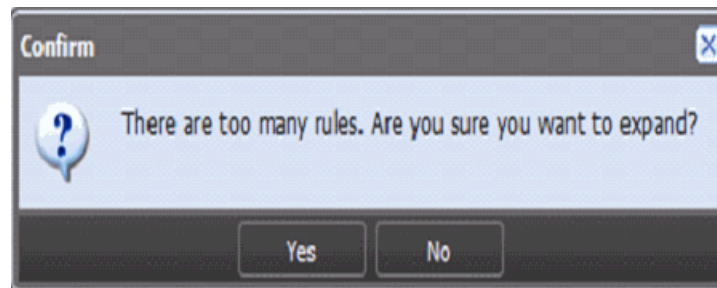
2. Select the NAT policy whose rules you want to expand.

By default, NAT policy rules in collapsed state are displayed in the right pane.

3. Click the **ExpandAll** icon, and all rules corresponding to that particular NAT policy are expanded.

If a NAT policy contains more than 1000 rules, a warning message is displayed before expanding, as shown in [Figure 224 on page 446](#).

**Figure 224: Expand All Warning Message for More Than 1,000 Rules**



4. Click the **CollapseAll** icon to collapse all rules.

## Cutting/Copying and Pasting Rules or Rule Groups in a NAT Policy

To cut or copy and paste rules or rule groups in a NAT policy:

1. On the right pane, select the device rule or rule group that you want to cut or copy. Right-click the selected device rule or rule group, and select **Cut** or **Copy**. If Cut is selected, related rule or rule group is removed from the right pane view.

You can copy the rules without locking a policy. However, you must lock the policy for the cut operation. You can select the combination of rules or rule groups for cutting

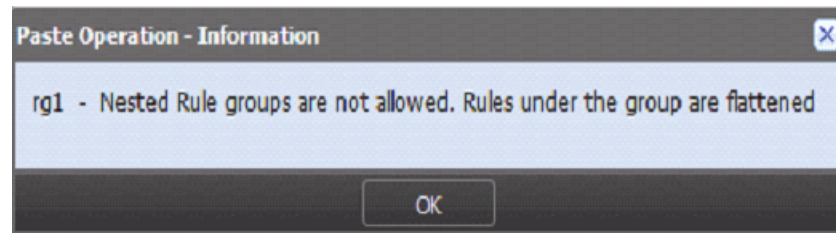
or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

2. On the left pane, select the NAT policy in which you want to paste the rule or rule group. On the right pane, right-click the rule or rule group that you want to paste. You can paste the rule or rule group before or after the selected rule or rule group by choosing the **Paste Before** or **Paste After** option, respectively.

If you are cutting and pasting rules across different policies, you must first save the cut operation in the current policy before moving to another policy for pasting. Otherwise, an error message is displayed, giving you the option either save or discard the changes.

Security Director does not support nested rule grouping. If you paste a rule group in another custom rule group, an error message is displayed, giving you the option to proceed by flattening the copied rule group, as shown in [Figure 225 on page 447](#).

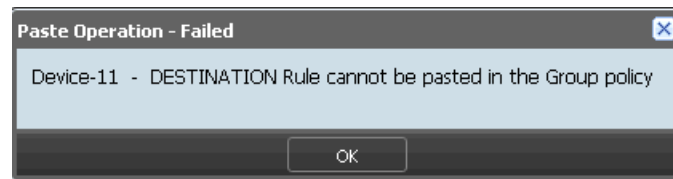
**Figure 225: Nested Rule Group Operation Warning Message**



Rule paste fails under the following conditions:

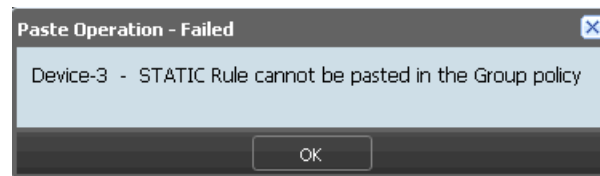
- If you copy the destination NAT rule and paste the rule in the group policy, the error shown in [Figure 226 on page 447](#) appears.

**Figure 226: Destination NAT Rule Paste Error**



- If you copy the static NAT rule and paste the rule in the group policy, the error shown in [Figure 227 on page 447](#) appears.

**Figure 227: Static NAT Rule Paste Error**



- If you copy a source rule of translation type Pool to the group rule, the error shown in [Figure 228 on page 448](#) appears.

**Figure 228: Group Policy Paste Error**

## Assigning Devices to a NAT Policy

To assign devices to a group NAT policy:

1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the NAT policy to which you want to assign devices and select **Assign Devices**.

The Assign Devices to Service window appears.

3. Select the devices that need to be added to the NAT policy in the Select Devices pane. Select the devices from the Available column and click the right arrow to move these devices to the Selected column. There is option to search for any devices in the Selected column of the Assign Devices window.

4. Click **Modify**.



---

### NOTE:

- If you do not have permission to certain devices, they will not be visible while assigning devices to a new or existing NAT policy.
  - You cannot view the device or exception policies at the left pane, for the assigned devices, that are labeled by the other Junos Space users.
- 

## Deleting Devices from a NAT Policy

To delete devices from a group NAT policy:

1. Select **Security Director > NAT Policies**.

The Policy Tabular view appears.

2. Right-click the NAT policy from which you want to delete devices and select **Assign Devices**.

The Assign Devices to Service window appears.

3. Select the devices that need to be deleted from the NAT policy in the Select Devices pane. Select the devices from the Selected column and click the left arrow to move these devices to the Available column.

4. Click **Modify**.



**NOTE:** Deleting a device from a group NAT policy creates a device NAT policy. This policy carries all the device-exception rules of the device from the group NAT policy.

## Rule Operations on the Filtered Rules

You can perform various rule operations on the filtered list of rules. For example, consider a policy having seven rules such as *a, b, c, d, e, f*, and *g* in an order inside a rule group. After filtering, if only second and sixth rules are filtered, that is only rules *b* and *f*, [Table 39 on page 449](#) explains the various rule operations on the filtered rules.

**Table 39: Various Rule Operation on the Filtered Rules**

Rule Operation	Description
Add rule before	<p>To add a new rule before an existing rule, select the existing rule in the filtered list and add the new rule above it.</p> <p>For example, if you perform this operation by selecting the sixth rule that is <i>f</i>, the seventh rule must be added before the sixth rule, in the filtered list. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Add rule after	<p>To add a new rule after an existing rule, select the existing rule in the filtered list and add the new rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the seventh rule must be added after the second rule. This rule is added at the third place in the full list.</p>
Paste before	<p>To paste a copied rule before an existing rule, select the existing rule in the filtered list and paste the copied rule above it.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the copied rule must be added after the sixth rule. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Paste after	<p>To paste a copied rule after an existing rule, select the existing rule in the filtered list and paste the copied rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the copied rule must be added after the second rule. The new rule is added at the third place in the full list.</p>
Clone	<p>To clone a selected rule, select the existing rule you want to clone in the filtered list. The cloned rule will be added above the selected rule.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the cloned rule must be added after the sixth rule, at the seventh place. The rule <i>g</i> must be moved down to the eighth place in the full list. This can be checked by clearing the filter from the search box.</p>

Table 39: Various Rule Operation on the Filtered Rules (*continued*)

Rule Operation	Description
Move rule to top	<p>To move a rule to the top of a list, select the rule you want to move in the filtered list and move rule to the top. If you move a rule from a filtered list to the top of that list, the selected rule is also moved to the top of the full list.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved to the top in the rule group, at first place in the original list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule to bottom	<p>To move a rule to the bottom of the list, select the rule you want to move in the filtered list and move rule to the bottom. If you move a rule from a filtered list to the bottom of that list, the selected rule is also moved to the bottom of the full list.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved to the bottom in the rule group, at the seventh place in the full list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the last rule in the full list.</p>
Move rule up	<p>To move a rule up one position in the list, select the rule you want to move in the filtered list and move rule up one position.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved before the second rule <i>b</i> in the filtered list. This rule is moved to the second place in the rule group in the full list.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule down	<p>To move a rule down one position in the list, select the rule you want to move in the filtered list and move rule down one position.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved after the sixth rule <i>f</i> in the filtered list. This rule is moved to the sixth rule in the rule group in the full list.</p> <p>This option is disabled for the last rule in the full list.</p>

## Showing NAT Policy for a Corresponding Log

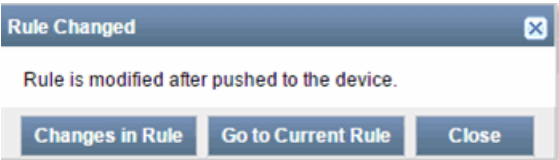
When a log is generated for a source, destination, or static NAT rule in the Event Viewer workspace, you can view the corresponding NAT policy. Based on the logs, you have an option to view either the source NAT rule or the destination NAT rule, or both. If you select a static NAT rule to view the log, both the source and the destination NAT rule logs are shown.

To view the source NAT policy for a corresponding log:

1. Under the Event Viewer workspace, if a log is generated by a source NAT rule, the corresponding rule name is populated in the NAT Src Rule column. Right-click the required log, and select **Show Source NAT Policy**.

If there are no changes in the rules, you are directly redirected to the corresponding NAT rule with filters applied on both left and right pane of the NAT Policies landing page. If there is a change in the current rule and the rule that generated the log, a pop-up window is displayed, as shown in [Figure 229 on page 451](#).

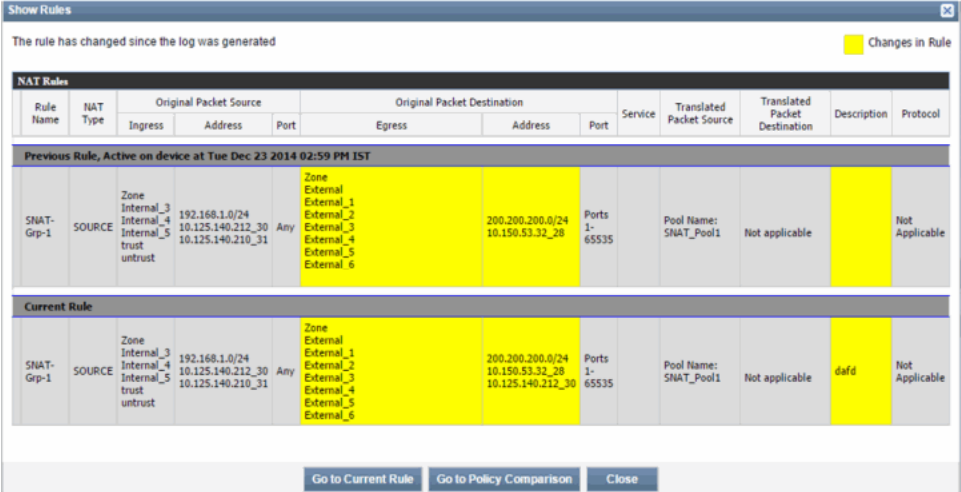
Figure 229: Jumping to the Current NAT Rule



If there is a name conflict between a source NAT rule and static NAT rule, a pop-up message prompts you to choose either the source NAT or static NAT rule.

- 2. Click **Changes in Rule** to view the diff between the current rule and the version of the rule that generated the log. The current version of the rule is compared with the version that existed at the time of log generation, as shown in [Figure 230 on page 451](#).

Figure 230: Changes in Rule View Window



Click **Go to Policy Comparison** to compare the rules within the current NAT policy, as shown in [Figure 231 on page 452](#).

Figure 231: Policy Comparison

Compare Versions: Router2 > #0 : Current												
Previous Diff			Next Diff			Top			Show Unchanged Rules			
Rule Name	NAT Type	Original Packet Source			Original Packet Destination			Service	Translated Packet Source	Translated Packet Destination	Description	Protocol
Zone_Internal_3-Zone_Ext-1												
NAT-Gap-1	SOURCE	Zone Internal_3	192.168.1.0/24	Any	Zone External_1	200.200.200.0/24	Ports 1-65535		Pool Name: NAT_Pool1	Not applicable	default	Not Applicable
Zone_trust-Zone_ext-trust		Zone Internal_4	10.125.140.212_30	Any	Zone External_2	10.155.53.32_30						
source-nat-rule-0_155	SOURCE	Zone trust	10.1.255.41	Any	Zone ext-trust	10.10.0.0/16	Any		Pool Name: pool1	Not applicable	Rule created for scale	Not Applicable

Rule Columns Changes			
Rule	Column	Zone	Zone
NAT-Gap-1	Egress	External_1	External_1
		External_2	External_2
		External_3	External_3
		External_4	External_4
		External_5	External_5
		External_6	External_6
NAT-Gap-1	Destination Address	200.200.200.0/24	200.200.200.0/24
		10.155.53.32_30	10.155.53.32_30
NAT-Gap-1	Description		default
source-nat-rule-0_155	Source Address	10.1.255.41	10.1.255.41
		10.125.140.212_30	10.125.140.212_30

OR

Click **Go to Current Rule** to view the current policy rule. In the left-pane search window, the policy name search string is shown; In the right-pane search window, the current rule name filter string is shown.

To view the destination NAT policy for a corresponding log:

- Under the Event Viewer workspace, if a log is generated by the Destination NAT rule, the corresponding rule name is populated in the NAT Dst Rule column. Right-click the required log, and select **Show Destination NAT Policy**

In the NAT policy workspace, a pop-up window is displayed, as shown in [Figure 229 on page 451](#).

If there is a name conflict between the destination NAT rule and static NAT rule, a pop-up message is shown to choose either the destination NAT or static NAT rule.

- The rest of the procedure is the same as for viewing the source NAT policy.

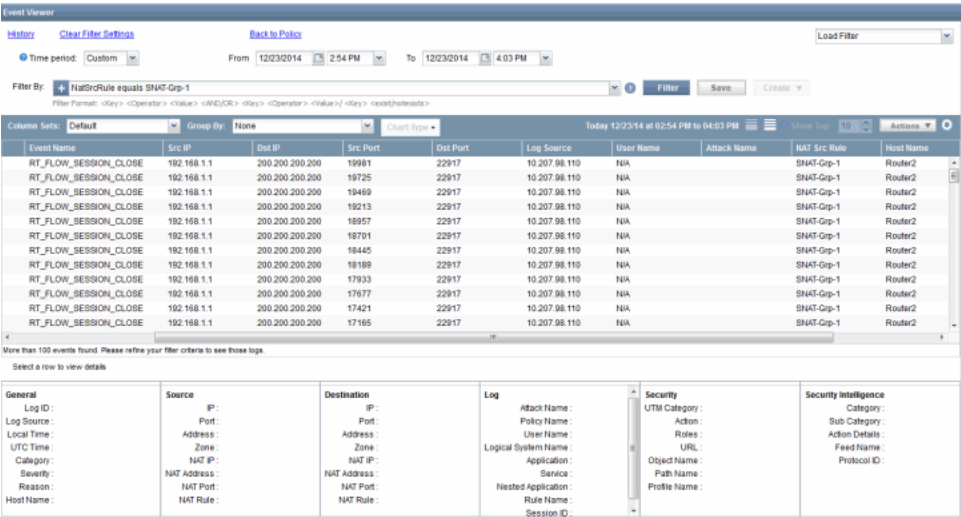
For a log that is generated by double NAT (both source NAT and destination NAT), rule names are populated for both source and destination rules. When you right-click, you will have both Show Source NAT Policy and Show Destination NAT Policy options. You can select either of these options to view the policy.

## Viewing Logs Generated by the NAT Rule

To view the logs generated by any NAT rule:

- Select **Security Director > NAT Policies**.  
The Policy Tabular view appears.
- On the right pane, right-click the rule for which you want to view the log, and select **Show Events Generated by Rule**.
- In the Event Viewer workspace, the corresponding log generated by the rule appears, as shown in [Figure 232 on page 453](#).

Figure 232: Log Displayed in the Event Viewer



You are automatically redirected to the Event Viewer workspace to view the log. The Custom time period is applied. The last updated time and the current time is used for filtering the logs. For a source NAT rule, the corresponding log is shown under the NAT Src Rule column. For a destination NAT rule, the log is shown under the NAT Dst Rule column. If you select a static NAT rule, both source and destination NAT rule logs are shown.



**NOTE:** After upgrading Security Director to Release 14.1R2, to view the corresponding NAT rule for a log, you must publish and update the policy.

Related Documentation

- [Creating NAT Policies on page 409](#)
- [Adding Rules to a NAT Policy on page 427](#)
- [Ordering the Rules in a NAT Policy on page 424](#)
- [Publishing NAT Policies on page 433](#)



## CHAPTER 37

# Creating and Managing NAT Pools

- [Creating NAT Pools on page 456](#)
- [Managing NAT Pools on page 459](#)

## Creating NAT Pools

A Network Address Translation (NAT) pool is a continuous range of IP addresses that you can use to create a NAT policy. NAT policies perform address translation by translating internal IP addresses to the addresses in these pools.

To create a NAT pool:

1. Select **Security Director > NAT Policies > NAT Pools**. In the NAT pools page, click plus sign (+) to create a new NAT pool.

The Create NAT Pool page appears, as shown in [Figure 233 on page 456](#).

**Figure 233: Create NAT Pool Page**

2. Enter the name of the NAT pool in the Name field.
3. Enter a description for the NAT pool in the Description field.
4. Select the type of NAT pool from the Pool Type menu.
5. Select the appropriate address from the Pool Address menu.
6. Expand the Routing Instance pane by clicking on the down arrow.
7. Select the device from the Device list. The Routing Instance field lists the available routing instances for the selected devices.

8. Select the desired routing instance for the selected device from the routing instances listed.
9. Expand the Advanced pane by clicking the down arrow.
10. Enter an appropriate value in the Host Address Base field.
11. Select the appropriate option from the Translation menu.

If the Translation type is No Translation:

- You can now create a source NAT pool with a single IP and no port translation.
- Two new parameters, Address Pooling and Address Sharing, are available. You can choose Address Pooling for all types of translations, but you can enable address sharing only when you select No Translation. If you select Host Address Base, the Address Pooling or Address Sharing options are not shown.
- Select the appropriate option from the Overflow Pool Type menu. If you select Pool in the Overflow Pool Type menu, select the appropriate NAT pool from the Overflow Pool selector.

If the Translation type is Port/Range:

- Select the required address pool the Address Pooling menu.
- Select the port from the Port menu.

If the Translation type is Overload:

- Select the required address pool the Address Pooling menu.
- Select an appropriate value from the Port Overloading Factor selector.

12. Click **Create**.

To create an address or address group:

1. Click the plus sign (+) next to the Pool Address drop-down menu to create a new address or new address object. [Figure 234 on page 458](#) shows the page that appears.

**Figure 234: Inline Address Group Creation for NAT Pool**

**Create NAT Pool**

**Create Address Object**

Object Type: ☐ Address ☒ Address Group

Name:

Description:

Addresses:

Available		Selected	
Filter	Select: <a href="#">All</a> <a href="#">None</a>		Select: <a href="#">All</a> <a href="#">None</a>
10.159.2.0/25 (10.159.2.0/25)	Global		
10.159.3.0/24 (10.159.3.0/24)	Global		
10.159.4.0/24 (10.159.4.0/24)	Global		
Addr-66.0.192.112/28 (66.0....)	Global		
Addr-66.184.206.216 (66.18...	Global		
ADDR-DNS-VIP-v6 (2001:48...	Global		
Total: 30			
<input type="checkbox"/> Host	<input type="checkbox"/> Network	<input type="checkbox"/> Wildcard	<input type="checkbox"/> Range <input type="checkbox"/> Other

**Create** **Cancel**

2. Select the Object Type radio buttons to create either a new NAT pool address or a new address group.
3. In the Name field, enter the name of an address group.
4. In the Addresses field, you can select all addresses available in the Available column or select few addresses to create a new address group.
5. Click **Create** to create the address group. This adds the newly created address objects to the selected addresses and returns to the address selector. Click **Cancel** to discard your changes and return to the Create NAT Pool window.



**NOTE:** You can create address object inline similar to address group inline.

**Related Documentation**

- [NAT Overview on page 403](#)
- [Managing NAT Pools on page 459](#)

- [Creating NAT Policies on page 409](#)
- [Managing NAT Policies on page 436](#)

## Managing NAT Pools

---

You can delete, modify, and clone NAT pools listed in the NAT Pool page.

To open the NAT Pool page:

- Select **Security Director > NAT Policies > NAT Pool**.

The NAT Pool page appears.

You can right-click the NAT pool to manage it.

You can perform the following tasks on the NAT Pool page:

- [Deleting NAT Pools on page 459](#)
- [Modifying NAT Pools on page 459](#)
- [Cloning NAT Pools on page 460](#)
- [Show Duplicate NAT Pools on page 460](#)
- [Find NAT Pool Usage on page 462](#)
- [Replace Addresses on page 463](#)
- [Show Unused NAT Pools on page 464](#)
- [Delete All Unused NAT Pools on page 465](#)

## Deleting NAT Pools

To delete a NAT pool:

1. Select **Security Director > NAT Policies > NAT Pools**.  
The Manage NAT Pool page appears.
2. Select the NAT pool that you want to delete, right-click, and select **Delete NAT Pools**.  
The Delete pop-up window appears displaying all the NAT pools that you can delete.
3. Click **Delete**.



**NOTE:** You cannot delete a NAT pool that is associated with a NAT policy.

## Modifying NAT Pools

To modify a NAT pool:

1. Select **Security Director > NAT Policies > NAT Pools**.  
The NAT Pool page appears.
2. Select the NAT pool that you want to modify, right-click, and select **Modify NAT Pool**.

The Modify NAT Pool page appears.

3. On the Modify NAT Pool page, you can edit the description and IP range of the NAT pool. You cannot modify the NAT pool name.
4. Click **Modify**.

You will receive a warning message when you try to modify a NAT pool used in a NAT policy. When you modify a pool associated with a published policy, you must republish the policy so that the changes are reflected in the policy.

## Cloning NAT Pools

To clone a NAT pool:

1. Select **Security Director > NAT Policies > NAT Pools**.  
The NAT Pools page appears.
2. Select the NAT pool you want to clone, right-click, and select **Clone NAT Pool**.  
The Clone NAT Pool window appears.
3. Make appropriate changes and save the NAT pool.



**NOTE:** You can also clone the NAT pool by right-clicking the NAT pool and selecting the Clone NAT Pool option.

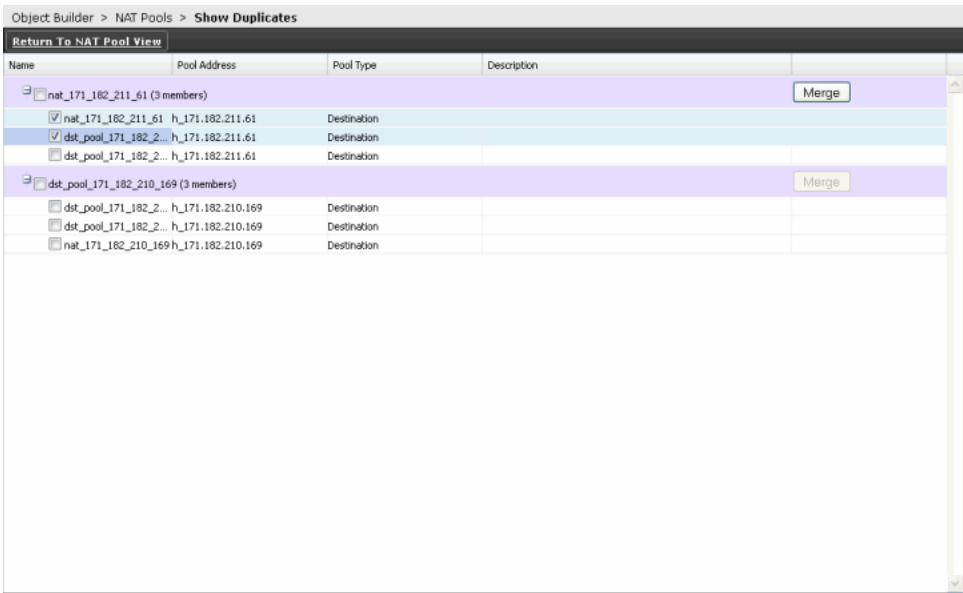
## Show Duplicate NAT Pools

To find duplicate address objects:

1. Select **Security Director > NAT Policies > NAT Pools**.  
The NAT Pools page appears.
2. Select the NAT pool for which you want to find the duplicate objects. Right-click the NAT pool or use the Action drawer, and click **Show Duplicates**.

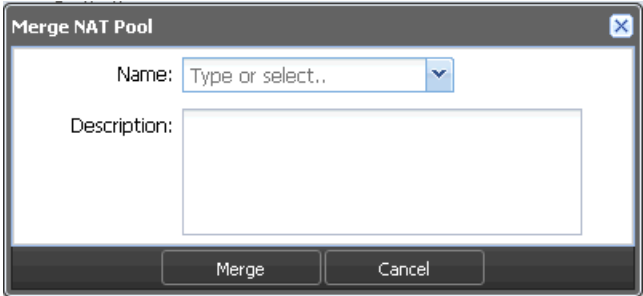
A window appears showing all the groups with duplicate objects, as shown in [Figure 235 on page 461](#).

Figure 235: Show Duplicates of NAT Pool



3. If you want to merge duplicate objects in a group, select the objects and click **Merge**.  
A merge window appears, as shown in [Figure 236 on page 461](#). In the Name field, provide a new object name or select existing object names from the list.

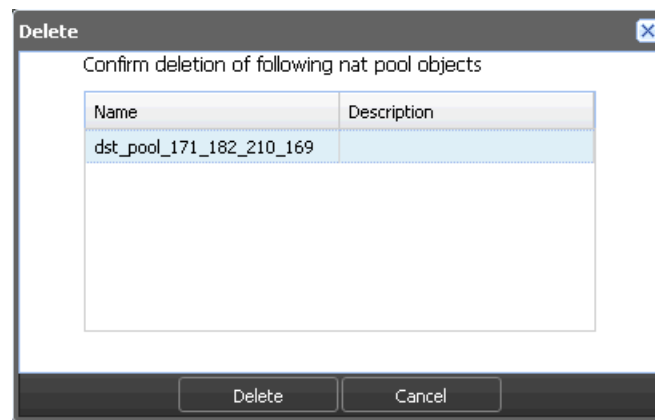
Figure 236: Merge NAT Pool



**NOTE:** You can merge all the objects in a group by clicking the **Merge** button after you select all the objects by clicking the group name.

4. If you want to delete objects in a group, select an object or objects, right-click, and then select **Delete**. A confirmation window appears before the selected objects are deleted, as shown in [Figure 237 on page 462](#).

Figure 237: Delete Duplicate NAT Pool Objects



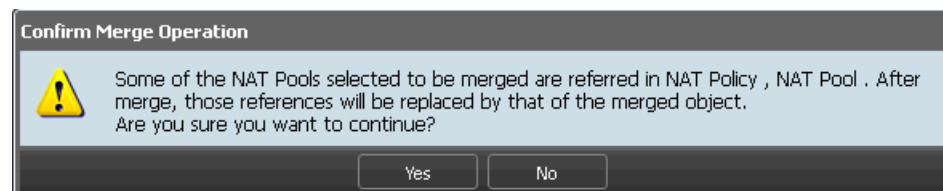
Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

5. If you want to find the usage of the duplicate objects in other groups, select an object, right-click, and then select **Find Usage**.

The usage window appears showing the usage of the selected object in any service ( NAT policy ) or security objects (NAT pool or address groups), as shown in

[Figure 238 on page 462](#).

Figure 238: Confirm Merge Operation



Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Find NAT Pool Usage

To find address usage:

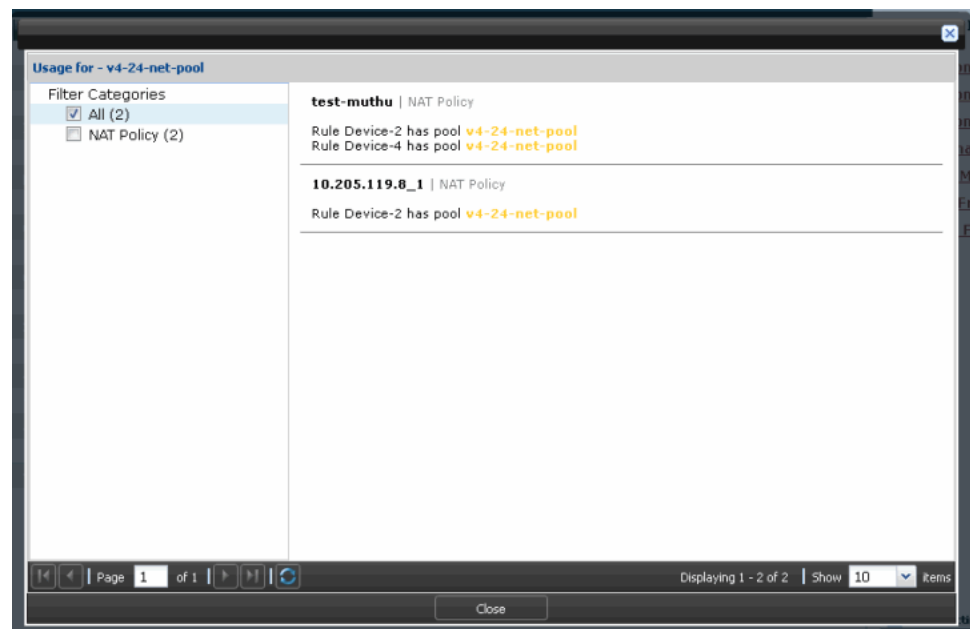
1. Select **Security Director > NAT Policies > NAT Pools**.

The NAT pool page appears.

2. Select the NAT pool for which you want to find the usage. Right-click the address or use the Action drawer, and click **Find Usage**.

A window appears, showing all the locations where this NAT pool object is used, as shown in [Figure 239 on page 463](#).

Figure 239: NAT Pool Usage Window



Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Replace Addresses

You can select one or more NAT pools to replace with another NAT pool of the same pool type. To replace one or more NAT pools:

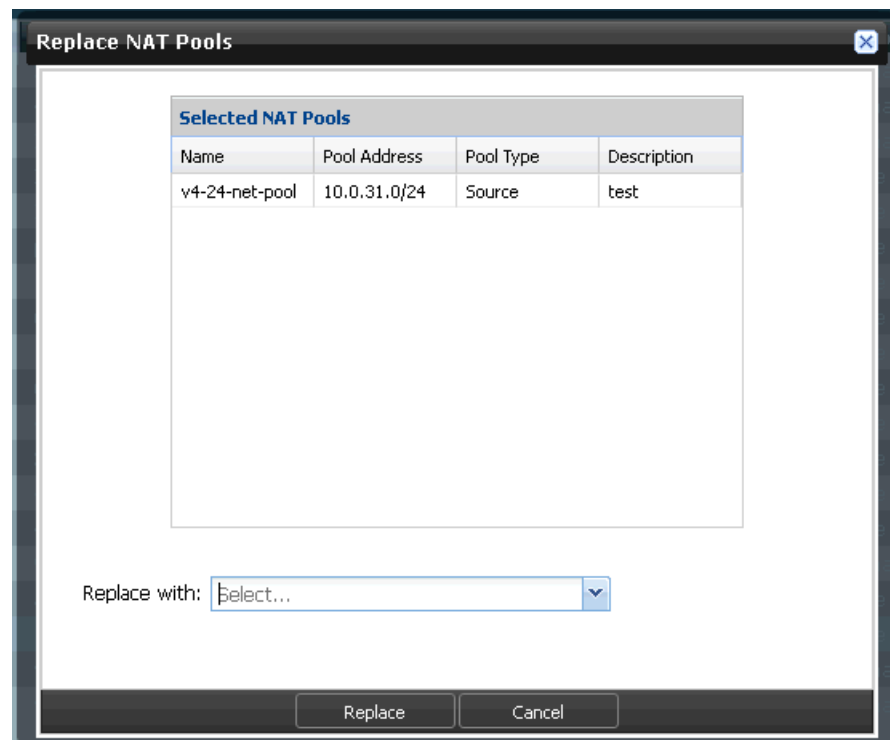
1. Select **Security Director > NAT Policies > NAT Pools**.

The NAT pool page appears.

2. Select the NAT pool that you want to replace. Right-click the NAT pool or use the Action drawer, and click **Replace NAT Pools**. You can replace a single NAT pool or multiple NAT pools.

A window appears, showing the NAT pool(s) you have selected to be replaced, along with a drop-down list of the NAT pools that are available to replace the NAT pool you have selected. See [Figure 240 on page 464](#).

Figure 240: Replace NAT Pools



3. In the Replace NAT Pools window, select the NAT pool to be replaced with the other NAT pool, and click **Replace**. If the selected NAT pools are used in any other references, you will receive the following warning message before the pools are replaced. Click **Yes** to continue the replacement operation.

If the operation is successful, you will receive a summary showing the NAT pools that were replaced.

## Show Unused NAT Pools

1. Select **Security Director > NAT Policies > NAT Pools**.

The NAT pool page appears.

2. Right-click any NAT pool or use the Actions drawer, and select **Show Unused**.

A list of all unused NAT pool objects that are not referenced in any policy appear on the page.

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 7](#)

## Delete All Unused NAT Pools

You can find the unused NAT pool objects and delete them. You can clear all the unwanted objects that are not used anywhere.

To delete the unused NAT pools:

1. Select the unused NAT pool object that you want to delete, and right-click the object or use the Actions drawer, and select **Delete All Unused NAT Pools**.

A warning message appears, confirming the delete operation.

2. Click **Yes** to delete all unused NAT pool objects or **No** to cancel the delete operation.

### Related Documentation

- [NAT Overview on page 403](#)
- [Creating NAT Pools on page 456](#)
- [Creating NAT Policies on page 409](#)
- [Managing NAT Policies on page 436](#)



## Creating and Managing Port Sets

- [Creating a Port Set on page 467](#)
- [Managing Port Sets on page 468](#)

### Creating a Port Set

---

You can group a set of ports or port ranges, and reference these port sets, using NAT rules, as source and destination ports.

To create a port set:

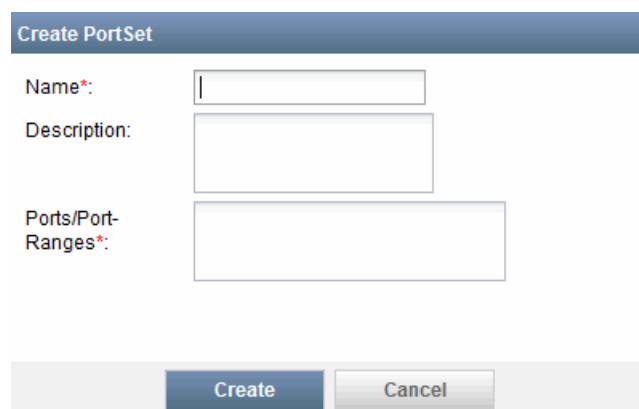
1. Select **Security Director > NAT Policies > Port Sets**.

The Port Sets page appears, listing the existing port sets.

2. To create a new port set, click the plus sign (+).

The Create PortSet page appears, as shown in [Figure 241 on page 467](#).

**Figure 241: Create PortSet**



The screenshot shows a web form titled "Create PortSet". It has three input fields: "Name\*" (with a red asterisk indicating it is mandatory), "Description", and "Ports/Port-Ranges\*" (also with a red asterisk). Below the fields are two buttons: "Create" and "Cancel".

3. In the Name field, enter the name of the new port set. This is a mandatory field.
4. In the Description field, enter a description of the port set.

5. In the Ports/Port-Ranges field, enter the port range. Enter multiple ports with comma separated. The maximum number of port or port range that you can enter for a single port is 8.

6. Click **Create**.

A new port set is created.

**Related  
Documentation**

- [Managing Port Sets on page 468](#)

---

## Managing Port Sets

You can modify, delete, clone, show unused, and find usage for port sets.

To open the Port Sets page:

- Select **Security Director > NAT Policies > Port Sets**.

The Port Sets page appears, listing the port sets.

- Right-click the port set to manage it, or select the required options from Actions.

You can perform the following management tasks on the Port Sets page:

- [Modifying a Port Set on page 468](#)
- [Deleting a Port Set on page 469](#)
- [Cloning a Port Set on page 469](#)
- [Showing Duplicate Port Sets on page 469](#)
- [Finding a Port Set Usage on page 469](#)
- [Showing Unused Port Sets on page 470](#)
- [Deleting All Unused Port Sets on page 470](#)
- [Assigning Domains to Port Sets on page 470](#)

### Modifying a Port Set

To modify a port set:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Right-click the port set and select **Modify PortSet**, or click the pencil icon.

The Modify PortSet page appears.

3. You can modify the name, description, and ports or port ranges.

4. Click **Modify**.

The required values are modified and saved.

## Deleting a Port Set

To delete a port set:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Right-click the port set that you want to delete, and select **Delete PortSets**.

You can also click the minus sign (-) to delete the port set.

3. A confirmation message appears before deletion. Click **Delete**.

The required port set is deleted.

## Cloning a Port Set

To clone a port set:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Select the port set you want to clone, right-click, and select **Clone PortSet**.

You are redirected to the Clone PortSet page.

3. Modify the required field value, and click **Clone**.

## Showing Duplicate Port Sets

To view the duplicate port sets:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Select the port set within which you want to find the duplicate objects. Right-click the port set, and click **Show Duplicates**.

A window appears, showing all the sets that include the duplicate objects.

## Finding a Port Set Usage

To find usage for a port set:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Select the port set for which you want to find the usage. Right-click the port set, and then click **Find Usage**.

A window appears, showing all the locations where this object is used.

## Showing Unused Port Sets

To view all the unused port sets:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. You can either right-click any port set or use the Actions, and select **Show Unused**.

A list of all unused port sets that are not referenced in any policy appears on the page.

## Deleting All Unused Port Sets

You can find all the unused port sets and delete them. You can clear all the unwanted objects that are not used anywhere.

To delete all unused port sets:

1. Select the unused port sets that you want to delete and right-click, or, from Actions, select **Delete All Unused**.

A confirmation message appears before deletion.

2. Click **Yes** to delete all unused port sets, or **No** to cancel the delete operation.

## Assigning Domains to Port Sets

To assign or modify the domain for a port set:

1. Select **NAT Policies > Port Sets**.

The Port Sets page appears.

2. Select the port set for which you want to assign a domain and right-click, or, from Actions, select **Assign PortSet to Domain**.

The Assign To Domain window appears.

3. Select the required domain to assign, and click **Assign**.

A domain is assigned to the port set.

**Related Documentation**

- [Creating a Port Set on page 467](#)

## PART 12

# Using IDP Signature Database Downloads

- [Downloading and Installing Signature Database on page 473](#)



# Downloading and Installing Signature Database

- Downloading the Signature Database on page 473
- Installing the Signature Database on page 475

## Downloading the Signature Database

To download the signature database:

1. Select **Security Director > Download**.

You can see the last log date in the last two weeks as shown in [Figure 242 on page 473](#).

**Figure 242: Signature Download Logs**

Logs in 2 weeks (May 23, 2014 - Jun 6, 2014)					
User Name	User IP	Task	Timestamp	Result	Description
super	localhost	Clean up after parsing IPS/Application Signatures	Jun 6, 2014 3:24:43 PM IST	Success	Clean up successful after parsing signature version 2384
super	localhost	Parse IPS/Application Signatures	Jun 6, 2014 3:24:18 PM IST	Success	Signature version 2384 parsed successfully.
super	localhost	Download	Jun 6, 2014	Success	Signature version

Page 1 of 1

Displaying 1 - 14 of 14

2. Select **Signature Database** from the Downloads workspace.

The Signature Database page appears, as shown in [Figure 243 on page 474](#). You can see the active databases that were downloaded earlier. At any time, Security Director will have only one active signature database.

Figure 243: Signature Database Page

Signature Database					
Active Database on Space					
Database Version	Publish date	Update Job	Installed Device Count	Detectors	Action
2384	2014-06-04 20:10:58	<a href="#">266344</a>	0	<a href="#">5.1.110140207...</a>	<a href="#">Install</a>
Latest list for IPS signatures					
Database Version	Publish date	Update Summary	Detectors	Action	
2382	2014-06-02 20:35:03	<a href="#">3 new signatures</a> <a href="#">4 updated signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2380	2014-05-29 16:34:58	<a href="#">1 new signatures</a> <a href="#">2 updated signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2379	2014-05-27 23:36:53	<a href="#">14 new signatures</a> <a href="#">7 updated signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2376	2014-05-21 18:00:11	<a href="#">6 new signatures</a> <a href="#">10 updated signatures</a> <a href="#">2 renamed signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2375	2014-05-19 18:00:04	<a href="#">6 new signatures</a> <a href="#">2 updated signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2374	2014-05-14 21:00:06	<a href="#">1 new signatures</a> <a href="#">9 updated signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	
2373	2014-05-13 16:08:44	<a href="#">13 new signatures</a>	<a href="#">12.6.140140207...</a>	<a href="#">Delta Download</a> <a href="#">Full Download</a>	

The following download options are available for the signature download:

- Delta Download—Downloads only the updates from the previous downloaded version.
- Full Download—Downloads the complete signature database; the download might take a longer time.

### 3. Select **Download Configuration**.

The Download Configuration page appears, as shown in [Figure 244 on page 474](#).

Figure 244: Download Configuration Page

Download Configuration
Download URL: <input type="text" value="https://services.netscreen.com"/>
<b>Use Proxy Server</b>
Enable Proxy: <input type="checkbox"/>
Host Name: <input type="text"/>
Host Port: <input type="text"/>
User Name: <input type="text"/>
User Password: <input type="password"/>
<input type="checkbox"/> <input type="button" value="Schedule at a later time"/>
<input type="checkbox"/> <input type="button" value="Repeat"/>
<div> <input type="button" value="Download"/> <input type="button" value="Cancel"/> </div>

4. Enter the URL from where you want to download the IPS and AppFw signature database in the Download URL field.
5. Click the **Enable Proxy** check box.
6. Enter the hostname in the Proxy Host Name field.
7. Enter the host's port number in the Proxy Host Port field.
8. Enter the username in the Proxy User Name field.
9. Enter the password in the Proxy User Password field.
10. Select the **Schedule at a later time** check box or down arrow to view the scheduling options.
11. Enter a date in the Date and time field. You can also choose a date from the date picker by clicking the date picker icon.
12. Select the time from the drop-down menu.
13. Select the Repeat check box to enable the schedule to recur in a given time interval.
14. Enter a numerical value in the first field in this section.
15. Select the appropriate length of time from the drop-down menu below the first field.
16. Select the **End Time** check box to view the options available to set the end time for recurring downloads.
17. Enter a date in the Date and time field. You can also choose a date from the date picker by clicking the date picker icon.
18. Select the time from the drop-down menu.
19. Click **Download**.

All the downloaded signatures are created in the System domain in read-only mode. The configuration that are downloaded are also saved in the System domain.

Security Director downloads both the AppID1.0 and the ngAppID2.0 application, and groups them with Security Director. These two applications and this group are downloaded and parsed from different ZIP folders. The offline packages are also imported and parsed similarly to the online packages. You can perform the offline download from <https://signatures.juniper.net/space/2/latest/latest-space-update.zip>.

#### Related Documentation

- [Installing the Signature Database on page 475](#)

## Installing the Signature Database

To install the signature database:

1. Select **Security Director > Downloads**.  
You can see the last login date in the last two weeks.
2. Select Signature Database from the Downloads workspace.

The Signature Database page appears. You can see the active database that was downloaded earlier.

3. Select **Install Configuration**.

The Install Configuration page appears, as shown in [Figure 245 on page 476](#).

**Figure 245: Install Configuration Page**

Device name	Device IP	Platform	OS Version	IPS License	APP License	Detector Vers...	Connection St...
HE_SRX-61-41	10.205.61.41	SRX3400	12.1X47-D10	Yes(2360)	Yes(2360)	12.6.140140207	Up
SRX2	10.207.98.110	FIREFLY-PERIMETER	12.1X47-D2	No(-)	No(-)	12.6.130121210	Up
Node-177 (Cluster)	10.205.50.177	SRX3400	12.1I20140508_srx_12q1_x47.1-647656	Yes(2379)	Yes(2379)	12.6.140140207	Up

Page 1 of 1 | Probe Devices | Displaying 1 - 3 of 3 | Show 25 items

☒ Enable Incremental Update

☐ Schedule at a later time

☐ Repeat

Install Cancel

Firefly Perimeter devices support IDP from Junos OS Release 12.1X47 onwards, and does not need license to use the IDP feature. The Signature Installation page lists the Firefly Perimeter devices though there is no license for IDP.

- Click the down arrow next to Signature Summary to view the version of the database and platforms that support this database.
- When you select a device for signature update, you can perform an incremental update or a full update of the signature database. Incremental update is the default. If the diff files for each incremental version are not available, a full update is performed regardless of which option you select. If diff files for incremental versions are available in Security Director and you select an incremental signature update, an incremental signature update is performed for both branch SRX Series devices and high-end SRX Series devices. For high-end SRX Series devices, a full update of the signature database is always performed.

If you do not want to perform an incremental update, clear the **Enable Incremental Update** check box, and a full signature update will be performed. For each new version download of the signature database, Junos Space will store the diff files for the previous 10 versions.

6. Click the check box next to the devices on which you want to install the database.
7. Select the **Schedule at a later time** check box or click the down arrow to view the scheduling options.
8. Enter a date in the Date and time field. You can also choose a date from the date picker by clicking the date picker icon.
9. Select the time from the drop-down menu.
10. Click the down arrow next to the Repeat section to enable the schedule to recur in a given time interval. You can also click the check box next to Repeat section to enable the schedule to recur in a given time interval.
11. Enter a numerical value in the first field in this pane.
12. Select the appropriate length of time from the drop-down menu below the first field.
13. Click the down arrow next to the End Time section to view the options available to set the end time for recurring installations. You can also click the check box next to End Time section to view the options available to set the end time for recurring installations.
14. Enter a date in the Date and time field. You can also choose a date from the date picker by clicking the date picker icon.
15. Select the time from the drop-down menu.
16. Click **Install**.

The configuration installing and device probing list devices only from the current domain, and probes devices only from the current domain.

Security Director sends the full signature database update if any one of the following scenarios is true:

- You install an older version of the signature files.
- The corresponding diff files do not exist.
- A signature file is added using the offline update.

You can perform an offline update of the signature database files by downloading the latest signature version from

<https://services.netscreen.com/space/latest/latest-space-update.zip> and storing it locally. Select **Upload From FileSystem** to upload the signature to Junos Space. Once the upload is completed, you can install the latest signature file version on to the device.



**NOTE:** Only the primary SRX Series device node is discovered by Security Director. If a job is created to install an IPS signature on the primary SRX Series node, the IPS signature is automatically installed on the SRX Series secondary node also.

Based on the device schema version (Junos OS Release 12.1x47 or older), Security Director installs the App-Sig-Package to the device, as shown in the [Table 40 on page 478](#):

Table 40: App-Sig-Package Details

Device Junos Version	App-Sig-Package
12.1x47	ngAppID2.0
Versions previous to 12.1X47	AppID1.0

**Related Documentation**    • [Downloading the Signature Database on page 473](#)

## PART 13

# Using IPS Management

- [Creating and Managing IPS Signatures and Signature Sets on page 481](#)
- [Creating and Managing IPS Policies on page 493](#)



## CHAPTER 40

# Creating and Managing IPS Signatures and Signature Sets

- [IPS Management Overview on page 481](#)
- [Creating IPS Signatures on page 482](#)
- [Managing IPS Signatures on page 484](#)
- [Creating a Policy Template on page 487](#)
- [Adding Rules to a Policy Template on page 488](#)
- [Managing Policy Templates on page 489](#)

### IPS Management Overview

---

You can use the IPS Management workspace to download and install the AppSecure signature database to security devices. You can automate the download and install process by scheduling the download and install tasks and configure these tasks to recur at specific time intervals. This ensures that your signature database is up-to-date.

You can view the predefined IPS policy templates and create customized IPS policy-sets in this workspace. You can also enable IPS configuration in a firewall policy and provision IPS related configuration with firewall policy.

During a device assignment for a group policy, only devices from the current and child domains (with view parent enabled) are listed. Devices in the child domain with view parent disabled are not listed. Not all the group policies of the Global domain are visible in the child domain. Group policies of the Global domain (including All device policy) are not visible to the child domain, if the view parent of that child domain is disabled. Only the group policies of the Global domain, which has devices from the child domain assigned to it, are visible in the child domain. If there is a group policy in global domain with devices from both D1 and the Global domains assigned to it, only this group policy of the Global domain is visible in the D1 domain along with only the D1 domain devices. No other devices, that is the Device-Exception policy, of the Global domain is visible in the D1 domain.

You cannot edit a group policy of the Global domain from the child domain. This is true for All Devices policy as well. Modifying the policy, deletion of the policy, managing a snapshot, snapshot policy and acquiring the policy lock is also not allowed. Similarly, you cannot perform these actions on the Device-Exception policy of the D1 domain from

the Global domain. You can prioritize group policies from the current domain. Group policies from the other domains are not listed.

During a device assignment for a device policy, only devices from the current domain are listed. If you move a device from one domain to another and the move is valid, the device-exception policy is also moved from the current domain to the target domain. This is possible if the view parent mode is enabled in the target domain. If the view parent is not enabled in the target domain, the move is not valid.

- Related Documentation**
- [Downloading the Signature Database on page 473](#)
  - [Installing the Signature Database on page 475](#)

## Creating IPS Signatures

To create an IPS signature:

1. Select **Security Director > IPS Management**.

The IPS Policies page appears with all IPS policies.

2. Click **IPS Signature**.

All IPS signatures that are downloaded appears in the View All IPS Signatures page, as shown in [Figure 246 on page 482](#). This page displays the version of the signature database. The left pane displays the different categories of signature and the right pane displays the signatures.

**Figure 246: View All IPS Signatures Page**

Name	Severity	Category	Object Type	Recommended	Pre-defined/Custom
Additional Web Services - Critical	Critical	SSL_FTR,WORM,GOP...	Dynamic Group	No	Pre-defined
Additional Web Services - Info	Info	SSL_FTR,WORM,GOP...	Dynamic Group	No	Pre-defined
Additional Web Services - Major	Major	SSL_FTR,WORM,GOP...	Dynamic Group	No	Pre-defined
Additional Web Services - Minor	Minor	SSL_FTR,WORM,GOP...	Dynamic Group	No	Pre-defined
Additional Web Services - Warning	Warning	SSL_FTR,WORM,GOP...	Dynamic Group	No	Pre-defined
All Attacks			Static Group	No	Pre-defined
Anomaly			Static Group	No	Pre-defined
Anomaly - All			Dynamic Group	No	Pre-defined
Anomaly - Critical	Critical		Dynamic Group	No	Pre-defined
Anomaly - Info	Info		Dynamic Group	No	Pre-defined
Anomaly - Major	Major		Dynamic Group	No	Pre-defined
Anomaly - Minor	Minor		Dynamic Group	No	Pre-defined
Anomaly - Warning	Warning		Dynamic Group	No	Pre-defined
APP		APP	Static Group	No	Pre-defined
APP - All		APP	Dynamic Group	No	Pre-defined
APP - Critical	Critical	APP	Dynamic Group	No	Pre-defined
APP - Info	Info	APP	Dynamic Group	No	Pre-defined
APP - Major	Major	APP	Dynamic Group	No	Pre-defined
APP - Minor	Minor	APP	Dynamic Group	No	Pre-defined
APP - Warning	Warning	APP	Dynamic Group	No	Pre-defined

3. Click **Create IPS Signature**.

The Create IPS Signature page appears, as shown in [Figure 247 on page 483](#).

Figure 247: Create IPS Signature Page

The screenshot shows the 'Create IPS Signature' page. At the top, there's a breadcrumb trail: 'IPS Policy > IPS Signature > Create IPS Signature'. Below this, the 'Create IPS Signature' form is displayed. It has two tabs: 'Signature Details' (selected) and 'Supported Detectors'. The 'Signature Details' tab contains the following fields and controls:

- Name:** A text input field.
- Category:** A text input field.
- Action:** A dropdown menu with 'None' selected.
- Keywords:** A text input field.
- Severity:** A dropdown menu with 'Info' selected.
- Description:** A large text area.
- Signature Details Section:**
  - Binding:** A dropdown menu with 'IP' selected.
  - Time Scope:** A dropdown menu.
  - Match Assurance:** A dropdown menu.
  - Protocol:** A text input field.
  - Time Count:** A text input field.
  - Performance Impact:** A dropdown menu.
  - Add Signature:** A button.
  - m01:** A label for the signature set.
  - Context:** A dropdown menu with 'stream' selected.
  - Direction:** A dropdown menu with 'Client to Server' selected.
  - Pattern:** A text input field.
  - Regex:** A text input field.
  - Negated:** A checkbox.

4. Enter the name of the signature in the Name field.
5. Enter the category of the signature in the Category field.
6. Enter a keyword in the Keywords field.
7. Select the appropriate severity of the signature from the Severity drop-down menu.
8. Select the appropriate action for the signature from the Action drop-down menu.
9. Enter the description for this signature in the Description field.
10. Select the **Signature Details** tab from the Pattern Set page. Enter the following:
  - a. Select the appropriate option from the Attack Object Binding drop-down menu.
  - b. Select the appropriate option from the Time Scope drop-down menu.
  - c. Select the appropriate option from the Match Assurance drop-down menu.
  - d. Enter the name of the protocol in the Protocol field.
  - e. Enter the value of the time count in the Time Count field.
  - f. Select the **Performance Impact** check box if you want to do so.
  - g. Click the **Add Signature** button.
  - h. Select the appropriate option from the Context drop-down menu.
  - i. Select the appropriate direction from the Direction dropdown menu.
  - j. Enter appropriate information in the Pattern field.
  - k. Enter appropriate information in the Regex field.
  - l. Select the **Negated** check box if you want to do so.
  - m. Select the **Shellcode** check box if you want to do so.

- n. Click the **Add Anomaly** button.
  - o. Select the appropriate anomaly from the Anomaly drop-down menu.
11. Click the **Supported Detectors** button to view the descriptors that are supported with this signature.
  12. Click **Save**.

**Related  
Documentation**

- [Managing IPS Signatures on page 484](#)

---

## Managing IPS Signatures

You can filter, modify, or delete IPS signatures listed in the View All IPS Signatures page.

To open the View All IPS Signatures page:

- Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page appears.

You can either right-click or use the Actions drawer to manage IPS signatures.

You can perform the following tasks in the View All IPS Signatures page:

- [Filtering IPS Signatures on page 484](#)
- [Modifying IPS Signatures on page 485](#)
- [Deleting IPS Signatures on page 485](#)
- [Cloning IPS Signatures on page 485](#)
- [Creating Static Signature Groups on page 486](#)
- [Creating Dynamic Signature Groups on page 486](#)
- [Creating IPS Signature Sets on page 487](#)

## Filtering IPS Signatures

To filter IPS signatures:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures. The right pane displays the signatures and the left pane displays the different filters that can be used to filter the signatures. The different parameters that can be used to filter the signatures include, Severity, Category, Object Type, Direction, Action, Match Assurance, Recommended, and Signature Set. Every parameter has different subparameters.

2. Click the check box next to the subparameters within a parameter.

The IPS signatures will now be filtered by the filters you have applied.

## Modifying IPS Signatures

To modify IPS signatures:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures.

2. Select the check box next to the IPS signature you want to modify.



**NOTE:** You cannot modify a predefined IPS signature. You can only modify the custom IPS signatures you have added.

3. Click **Modify IPS Signature** in the Actions drawer.

You are redirected to the Modify IPS Signature page. You can make necessary changes to the application signature here.

4. Click **Save**.

## Deleting IPS Signatures

To delete IPS signatures:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures.

2. Select the check box next to the IPS signatures you want to delete.



**NOTE:** You cannot delete the predefined IPS signatures. You can only delete the custom IPS signatures you have added.

3. Click **Delete Selected** in the Actions drawer.

A confirmation window appears.

4. Click **Yes**.

## Cloning IPS Signatures

To clone IPS signatures:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures that are downloaded.

2. Select the check box next to the IPS signature you want to clone.

3. Click **Clone IPS Signature** in the Actions drawer.

You are redirected to the Create IPS Signature page. You can clone the IPS signature here.

## Creating Static Signature Groups

To create a static signature group:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures.

2. Select the check box next to the IPS signatures you want to include in the IPS signature static group.
3. Select the signature, right-click and select **Create Static Group**.

The Create IPS Signature Static Group page appears.

4. Enter the name of the static signature group in the Name field.
5. Select the Recommended check box if you want to do so.
6. Click the **Add** icon to add IPS signatures to the static group.

The IPS Signature Selector window appears.

7. Select the appropriate IPS signatures and click Update.

## Creating Dynamic Signature Groups

To create a dynamic signature group:

1. Select **Security Director > IPS Management > IPS Signature**.

The View All IPS Signatures page displays all IPS signatures.

2. Select the signature, right-click and select **Create Dynamic Group**.

The Create IPS Signature Dynamic Group page appears.

3. Enter the name of the dynamic signature group in the Name field.
4. Select the check box next to the appropriate option in the Recommended pane.
5. Select the check boxes next to the appropriate actions in the Actions pane.
6. Select the appropriate directions from the drop-down menus in the Direction pane.
7. Select the appropriate check box in the Pre-defined/Custom pane.
8. Select the appropriate check boxes in the Match Assurance pane.
9. Select the appropriate check boxes in the Performance Impact pane.
10. Click the **Advanced** tab.
11. In the Category pane, select the appropriate signatures from the Available column and click the right arrow to push them to the Selected column.
12. In the Service pane, select the appropriate signatures from the Available column and click the right arrow to push them to the Selected column.
13. Select the appropriate check boxes in the Severity pane.
14. Click **Create**.



**NOTE:** In Security Director Release 13.1, all Security Director filters in dynamic group are removed. During upgrade from Security Director Release 12.2 to Release 13.1, if the dynamic group in Release 12.2 contains Security Director related filters, Security Director internally converts to static group during the migration.

## Creating IPS Signature Sets

To create an IPS signature set:

1. Select **Security Director > IPS Management > IPS Signature**.  
The View All IPS Signatures page displays all IPS signatures.
2. Select the appropriate IPS signatures and then click **Create IPS Signature-Set**.

### Related Documentation

- [Creating IPS Signatures on page 482](#)

## Creating a Policy Template

To create a policy template:

1. Select **Security Director > IPS Management**.  
You see the IPS Policies Tabular view.
2. Click **Policy Templates**.  
You see the Policy Templates Tabular view with two panes and the first signature set is selected by default. The left pane displays all the policy templates in the system. The policy templates from the current domain and the predefined policy templates are listed. The right pane displays all the rules in a specific policy templates.  
All the policy templates under the Predefined node are predefined policy templates. All the policy templates under the Custom node are user-defined policy templates.
3. Click **Create Policy Template**.  
The Create Policy Template page appears.
4. Enter the name of the policy template in the Name field.
5. Enter the description for the policy template in the Description field.
6. Click **Create**.

Validate policy templates by clicking the **Validate** button, available next to the Save and Discard buttons. If any errors are found during the validation, a red warning icon is shown for the respective policy template.

### Related Documentation

- [Adding Rules to a Policy Template on page 488](#)
- [Managing Policy Templates on page 489](#)

## Adding Rules to a Policy Template

---

To add rules to a policy template:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates Tabular view appears.

2. Click the policy template you want to add rules to from the left pane.

The existing rules of the policy template are displayed in the right pane.

3. Click the **+** icon to add rules, and select the type of the rule you want to add. The newly added rule blinks different color for a few seconds.

A new rule is added in the last row.

4. Click the **IPS Signature** column in the rule.

The IPS Signature Selector window appears. You can select and add IPS signatures from this window.

5. Click **Update** in the IPS Signature Selector window when you select the IPS signatures for the rule.

6. Click the **Action** column in the rule and select the appropriate action for the rule.

7. Click the **Notification** column in the rule.

A drop-down menu with all notification options appears. To add appropriate notification options:

- a. Click the **Enable** check box next to the Attack Logging field if you want to log the attacks.
- b. Click the **Enable** check box next to the Attack Flag field if you want to flag attacks.
- c. Select the appropriate option from the IP Action drop-down menu.
- d. Select the appropriate option from the IP Target drop-down menu.
- e. Enter the value of the timeout interval in the Timeout field.
- f. Click the **Enable** check box next to the Log IP Action field if you want to maintain a log of the IP actions performed.
- g. Select the appropriate severity from the Severity drop-down menu.
- h. Click the **Enable** check box next to Terminal field.
- i. Click **Update**.



**NOTE:** You can also modify the IP action and the additional sections in the Notification drop-down menu by clicking the IP Action and Additional columns in the rule.

---

8. Click the **Description** column and enter a description for the rule.
9. Click **Save**.

- Related Documentation**
- [Creating a Policy Template on page 487](#)
  - [Managing Policy Templates on page 489](#)

---

## Managing Policy Templates

- [Deleting Policy Templates on page 489](#)
- [Cloning Policy Templates on page 489](#)
- [Enable or Disable Rules in a Policy Templates on page 490](#)
- [Grouping Rules in a Policy Templates on page 490](#)
- [Expanding/Collapsing All Rules in a Policy Template on page 491](#)
- [Cutting/Copying And Pasting Rules or Rule Groups in a Policy Template on page 491](#)
- [Adding Rules to a Policy Template on page 492](#)

### Deleting Policy Templates

To delete policy templates:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates page displays all policy templates. The left pane displays the predefined and custom policy templates. The right pane displays the signatures in the respective policy templates.

2. Right-click the policy template you want to delete and select **Delete Policy Template**.

A confirmation window appears.



**NOTE:** You cannot delete a predefined policy template. You can only delete a custom policy template.

3. Click **Yes**.

### Cloning Policy Templates

To clone policy templates:

1. Select **Security Director > IPS Management > Policy Template**.

The Policy Templates page displays all policy templates. The left pane displays the predefined and custom policy templates. The right pane displays the signatures in the respective policy template.

2. Right-click the policy template you want to clone and select **Clone Policy Templates**.

You are redirected to the Clone Policy Templates page. You can modify the name and description on this page.

3. Click **Clone**.

## Enable or Disable Rules in a Policy Templates

To enable or disable rules in a policy template:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates page displays all policy templates. The left pane displays the predefines and custom policy templates.

2. Select the policy template for which you want to enable or disable the rule in the left pane.

All rules of the this policy template appear in the right pane.

3. Select the rule you want to enable or disable and click the appropriate button.

The disabled rule appears dimmed.

4. Click **Save**.

## Grouping Rules in a Policy Templates

To group rules in a policy template:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates page displays all policy templates. The left pane displays the predefines and custom policy templates.

2. Select the policy template for which you want to group all rules, in the left pane.

All rules of the this policy template appear in the right pane.

3. Select the check boxes next to the rules you want to group.

4. Right-click the rules and select **Rule Group > Create Rule Group**.

The Create Rule Group pop-up window appears.

5. Enter a name for the rule group in the Name field.

6. Enter a description for the rule group in the Description field.

7. Click **Create**.



**NOTE:** When the rule group is created, you can add rules in the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

---

## Expanding/Collapsing All Rules in a Policy Template

To expand or collapse all rules in a policy template:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates page displays all policy templates. The left pane displays the predefines and custom policy templates.

2. Select the policy template for which you want to expand or collapse all rules, in the left pane.

All rules of the this signature-set appear in the right pane.

3. Click the **Expand All RuleGroups** icon, and all rules corresponding to that particular policy template are expanded.
4. Click the **Collapse All RuleGroups** icon to collapse all rules.

## Cutting/Copying And Pasting Rules or Rule Groups in a Policy Template

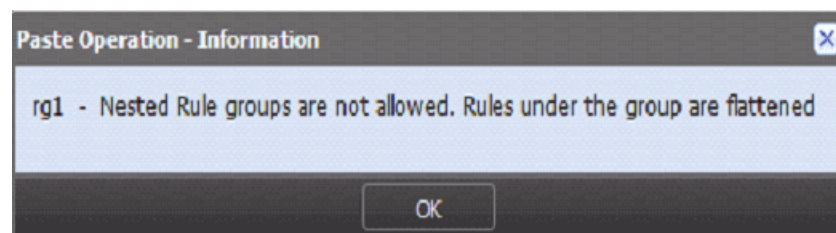
To copy and paste rules in a policy template:

1. In the right pane, select the rule that must be copied. Right-click on the selected rule, and select **Cut** or **Copy**. If Cut is selected, related rule or rule group is removed from the right pane view.
2. In the left pane, select the policy template that you want to paste the rule. In the right pane, right-click on the rule that you want the rule to be pasted. You can paste the rule before the selected rule or after the selected rule by choosing **Paste Before** or **Paste After** options.

If you are cutting and pasting rules across different policy templates, you must first save the cut operation in the current policy template before moving to another policy template for pasting. Otherwise, an error message is displayed, giving you the option either save or discard the changes.

Security Director does not support nested rule grouping. If you paste a rule group in another custom rule group, an error message is displayed, giving you the option to proceed by flattening the copied rule group, as shown in [Figure 248 on page 491](#).

**Figure 248: Nested Rule Group Paste Warning Message**



## Adding Rules to a Policy Template

You can add the rules before or after the IPS rule or exempt rule. To add rules:

1. Select **Security Director > IPS Management > Policy Templates**.

The Policy Templates page displays all policy templates. The left pane displays the predefines and custom policy templates.

2. Select the IPS rule to which you want to add rules, right-click, and select **Add Rules Before** or **Add Rules After**.

You will get an option to add rules before the IPS rule or Exempt rule, or after the IPS rule or Exempt rule.

- Related Documentation**
- [Creating a Policy Template on page 487](#)
  - [Adding Rules to a Policy Template on page 488](#)

## CHAPTER 41

# Creating and Managing IPS Policies

- [Creating IPS Policies on page 494](#)
- [Managing Policy Locks on page 503](#)
- [Ordering the Rules in a IPS Policy on page 504](#)
- [Adding Rules to an IPS Policy on page 507](#)
- [Publishing IPS Policies on page 509](#)
- [Managing IPS Policies on page 513](#)

## Creating IPS Policies

If you want to enable IPS policy creation for a group firewall policy, you need to:

- Enable IPS configuration mode to Advanced for the devices in the group firewall policy.

[Table 41 on page 494](#) shows different IPS configuration modes and their purposes:

**Table 41: IPS Configuration Mode**

IPS Mode	Description
Basic	Turns IPS on or off. If you select this mode, you are given the option to select signature sets. Custom and predefined signature sets are listed. The IPS policy is generated by merging the rules from the signature sets you choose. The IPS policy is read-only.
Advanced	Turns IPS on or off. An empty IPS policy is generated. You can add or delete, disable or enable, or modify an IPS rules and exempt rules.
None	If this mode is selected, you cannot configure IPS on or off settings in a firewall rule. You cannot generate any IPS policies.

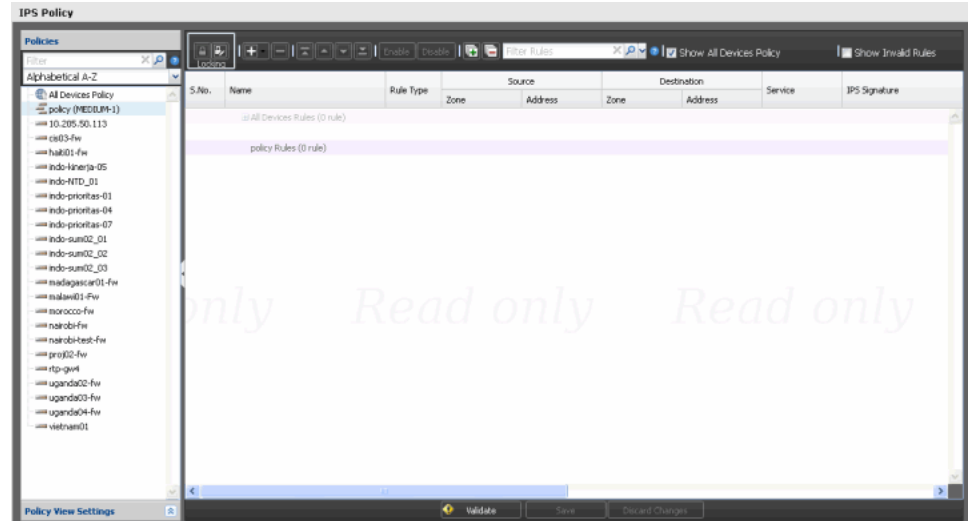
- Set the Action field for the device rule for which you want to enable the firewall policy to Permit.
- Select IPS field to IPS ON or IPS OFF when the firewall policy is configured with IPS mode basic or advanced, and the firewall rule action is set to either permit or tunnel.

To create an IPS rule:

1. Select **Security Director > IPS Management**.

The IPS Policies tabular view appears. The left pane displays the firewall policies and the right pane displays the all devices policy rules and the device rules for which IPS policy can be created as shown in [Figure 249 on page 495](#).

**Figure 249: IPS Policies Tabular View**



2. Select the device policy for which you want to create an IPS rule.

The right pane displays the device policy for which the IPS rules can be created.



**NOTE:** If you do not have permission to the device assigned to a device policy, you cannot view the policy in the respective policy ILP.

3. Select the IPS signature in the IPS signature set that you want to customize for creating an IPS policy and modify the fields appropriately.

You can now add more IPS and exempt rules for this device rule.

4. Click the **Add Rule** icon and select the type of the rule you want to add.

A new rule is added in the last row. If you add an IPS rule, by default, the Source and Destination zones and addresses are inherited from the device rule. The IPS Signature field is set to None. You can now customize the fields in this rule.

For logical systems, you cannot edit source and destination zones, source and destination addresses, and application. Automatically, Security Director sets zone and address fields as Any and application field as default.

5. Click **Save**.

Validate policies by clicking the **Validate** button, available next to the Save and Discard buttons. If any errors are found during the validation, a red warning icon is shown for the respective policies. For IPS policies, incomplete rules and duplicate rule names are validated.

Security Director permits you to save policies that contain errors. Warnings messages are displayed for policies that contain errors, but you can proceed to save such policies as drafts. You cannot publish policies that are in the draft state. The tooltip for the policy shows the state as draft ; because it is a draft, the tooltip does not show the publish option. When you save a policy as a draft, duplicate rule name errors are ignored.

Whenever you make any changes to the IPS policy, you will get an option to enter a comment before saving the policy. You can enable or disable this option in Platform > Administration > Applications. To enable this option, right-click **Security Director**, and select **Modify Security Director Settings** option. Under Applications, select the **Enable save comments for policies** check box. By default, this option is disabled.

Once you enter the comment, in IPS ILP you can save this version with a different name. Click **Save as Draft** from Save drop-down list to save the edited IPS policy with a different name. Entering comments is not mandatory but all entered comments are audit logged.

**NOTE:**

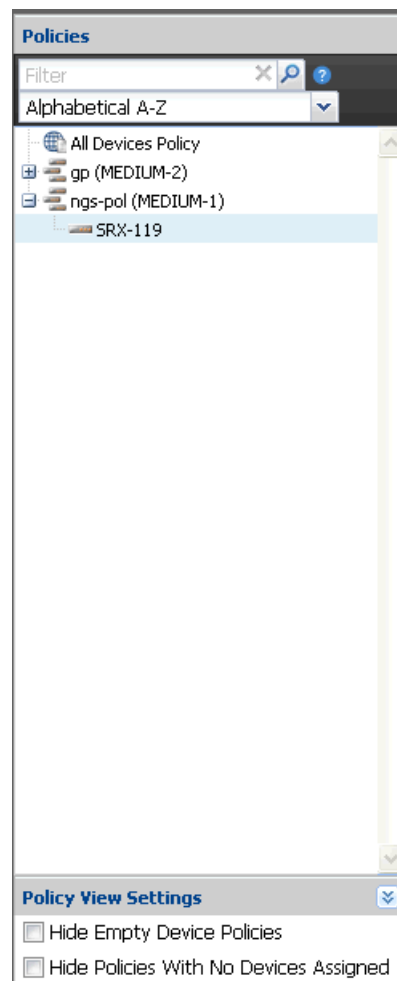
- When the firewall policy is published and updated on the device, the IPS policy configuration is also pushed along with the firewall configuration.
- Security Director deletes custom defined IPS policies only while updating the IPS policy to the device. In case of logical system, if there is a reference to any user defined IPS policy in any of the logical system, those IPS policies are not deleted. But if there an IPS policy which is not referred in any logical system, that policy would be cleaned up during the next update.

---

To hide the policies in the left pane that do not have any defined rules:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Empty Device Policies** check box to hide the device exception policies that do not have any rules, as shown in [Figure 250 on page 497](#).

Figure 250: Policy View Settings



3. Policies with no defined rules are hidden in the left pane.

To hide the policies in the left pane that do not have any devices assigned:

1. At the bottom of the left pane, click the expandable **Policy View Settings** option.
2. Click the **Hide Policies With No Devices Assigned** check box to filter device and group policies that are not assigned to any device, as shown in [Figure 250 on page 497](#).
3. Policies without any assigned devices are hidden in the left pane.

Security Director provides advanced search options for the IPS policies. Click the down arrow icon next to the search icon, select **Advanced Search**, and the following dialog appears, as shown in [Figure 251 on page 498](#).

Figure 251: IPS Advance Search Window

The screenshot shows the 'Advanced Search' window with the following fields:

- Rule Name:
- Rule Type:
- Source:
  - Zone:
  - Address:
- Destination:
  - Zone:
  - Address:
- Service:
- IPS Signature Name:
- Action:
- Description:

Buttons at the bottom: Filter, Reset, Cancel

You can perform advanced searches for the following fields:

- Rule Name
- Source
  - Zone
  - Address
- Destination
  - Zone
  - Address
- Service
- IPS Signature Name
- Action
- Description

The following advanced search criteria are available:

- Wildcard search for rule names using an asterisk (\*) is allowed.
- Security Director supports AND and OR operations between search items. The default behavior is OR.
- For rule name search, only the OR operation is allowed, because a policy cannot have multiple rule names.
- For zone search, only the OR operation is allowed. Wildcard search is supported.

- For service and address fields, OR and AND operations are allowed.
- Multiple groups can be grouped using parenthesis. Grouping can be used during filed or keyword searches as well.
- Negate (-) symbol can be used to exclude objects that contain a specific term name.
- The plus (+) operator can be used to specify that the term after the + symbol existing the field value to be filtered along with other searched items.
- Escaping special characters are part of the search syntax. The supported special characters are + - & & || ! ( ) { } [ ] ^ " ~ \* ? : \.



**NOTE:** Use the AND operator to find rules that match all values for a given set of fields. Use the OR operator to find rules that match any of the values for a given set of fields.

Table 42 on page 499 explains certain specific Security Director search behavior.

**Table 42: Specific Security Director Search Behavior**

Search Item	Description
IPv4 addresses	If you provide a valid IPv4 address, range, or network in the search field, Security Director finds all addresses that include these IPv4 address, range, or network.
Destination port in service	If you configured a destination port range of a service, Security Director matches ports within this range but this is valid only during field or keyword search.
Keyword or field	If you require to search specific attributes in an object as opposed to global search, you can use keyword or field search.

Table 43 on page 499 shows example search results for different parameters.

**Table 43: Examples of Different Advanced Search Parameters**

Scenario	Query Parameter	Description
Wildcard search for rule names in both zone and global rules	RuleName:( All* )	Rule names starting with <i>All</i> are filtered.
Wildcard search for a particular rule name pattern	RuleName:(All-Devices-Zone-Pre*)	Returns All Devices Policy Zone Pre rules
	RuleName:(All-Devices-Global-Pre*)	Returns All Devices Policy Global Pre Rules
	RuleName:(All-Devices-Zone-Post*)	Returns All Devices Policy Zone Post Rules
	RuleName:(All-Devices-Global-Post*)	Returns All Devices Policy Global Post Rules
Source zone to destination zone	SrcZone:( polyzone ) AND DstZone:( untrust )	Rules with source zone <i>polyzone</i> and destination zone <i>untrust</i> are filtered.

Table 43: Examples of Different Advanced Search Parameters (*continued*)

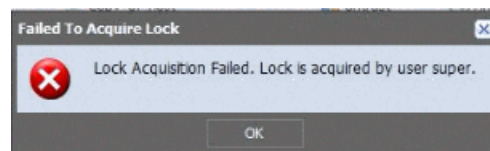
Source zone and source address to destination zone and destination address	SrcZone:( <i>polyzone</i> ) AND SrcAddress:( <i>any</i> ) AND DstZone:( <i>untrust</i> ) AND DstAddress:( <i>polyaddr</i> )	Rules with source zone <i>polyzone</i> , source address <i>any</i> , destination zone <i>untrust</i> , and destination address <i>polyaddr</i> are filtered.
Source zone and source address to destination zone and destination address along with service	SrcZone:( <i>polyzone</i> ) AND SrcAddress:( <i>polyaddr1</i> AND <i>polyaddr2</i> ) AND DstZone:( <i>untrust</i> ) AND DstAddress:( <i>any</i> ) AND Service:( <i>srv1</i> AND <i>srv2</i> )	Rules with source zone <i>polyzone</i> , source addresses <i>polyaddr1</i> and <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with Services <i>srv1</i> and <i>srv2</i> , are filtered.
Source zone and source address to destination zone and destination address along with service port range	SrcZone:( <i>polyzone</i> ) AND SrcAddress:( <i>polyaddr1</i> AND <i>polyaddr2</i> ) AND DstZone:( <i>untrust</i> ) AND DstAddress:( <i>any</i> ) AND Service:( <i>10</i> AND <i>65535</i> )	Rules with source zone <i>polyzone</i> , source addresses <i>polyaddr1</i> and <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with Services having destination port range 10-65535 are filtered.
Rules with action	SrcZone:( <i>polyzone</i> ) AND SrcAddress:( <i>polyaddr1</i> <i>polyaddr2</i> ) AND DstZone:( <i>untrust</i> ) AND DstAddress:( <i>any</i> ) AND Service:( <i>aol</i> <i>apple-ichat</i> ) AND dcRuleAction:( <i>Permit</i> )	Rules with source zone <i>polyzone</i> , source address <i>polyaddr1</i> or <i>polyaddr2</i> , destination zone <i>untrust</i> , and destination address <i>any</i> , with service as either <i>aol</i> or <i>apple-ichat</i> , and action <i>Permit</i> , are filtered.



**NOTE:** You can search by giving IPv6 addresses in the source or the destination address field.

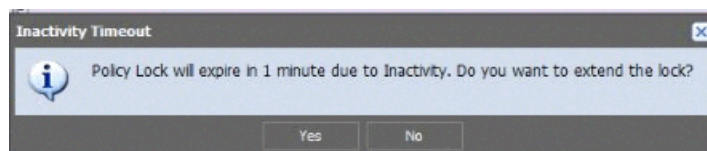
Before you can edit the policy, you must lock it by clicking the lock icon, which is available in the policy view toolbar. You can hold more than one policy lock at a given time. You can unlock the policy by clicking the unlock icon next to the lock icon in the policy tabular view. If you attempt to lock a policy that is already locked by another user, the following message appears, as shown [Figure 252 on page 500](#). The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

Figure 252: Lock Failure Error Message for the Second User



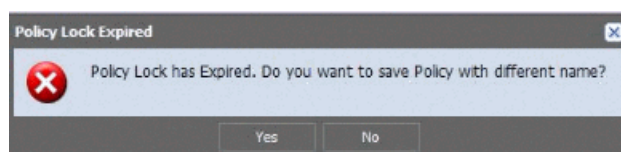
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 253 on page 501](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see [“Managing Policy Locks” on page 503](#).

Figure 253: Inactivity Timeout Error



Click **Yes** to extend the locking period. If you click **No**, and if there is activity on the policy within the last minute of the lock's life, the timer will be reset and the lock will not be released. If you ignore the message, when the policy lock timeout interval expires 1 minute later, you are prompted to either save the edited policy with a different name or lose the changes, as shown in [Figure 254 on page 501](#).

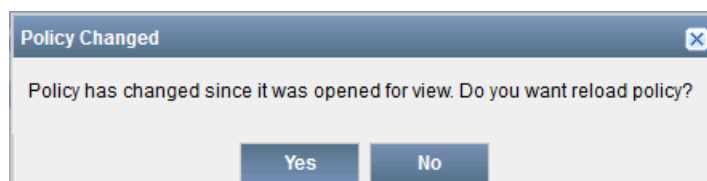
Figure 254: Policy Lock Expired Message



If you click **Yes** to save the edited policy with a different name, the following window appears. If you navigate away from the locked policy, you will get an option to save the edited policy with different name.

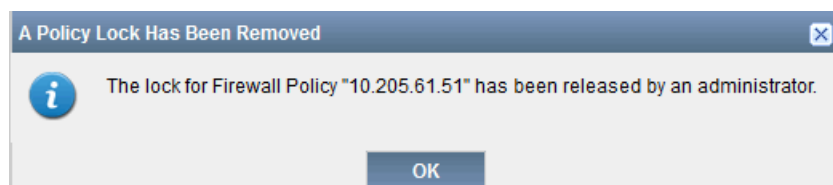
After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 255 on page 501](#).

Figure 255: Unsaved Changes Warning Message

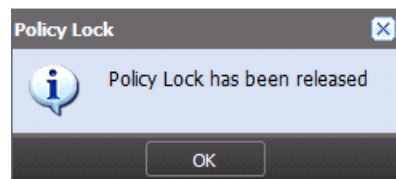


If Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 256 on page 501](#).

Figure 256: Policy Unlock by Admin Message



If you do not edit the locked policy and the policy lock timeout expires, the following warning message appears, as shown in [Figure 257 on page 502](#).

**Figure 257: Policy Lock Release Message**

The policy is locked and released for the following policy operations. Also, these operations are disabled for a policy, if the policy is locked by some other user.

- Modify
- Assign devices
- Rollback
- Delete

**NOTE:**

- You can unlock the policy by logging out of the application or when the policy lock timeout expires. You can unlock your policies even if they are not edited.
- If the browser crashes when the policy is still locked, the policy is unlocked only after timeout interval expires.
- If there is an object conflict resolution during a migration, import, or rollback, and if you are editing any objects, you will receive a save as option for the edited objects. The behavior is the same when you import addresses from CSV.
- Policy lock is not released under the following scenario:
  - If you save or discard you changes to the locked policy.
  - if you do not make any changes to the locked policy and navigate to another policy.
- It is recommended to configure the session time longer than the lock timeout value.
- You can create address objects and address group inline.

**Related Documentation**

- [Publishing IPS Policies on page 509](#)
- [Managing IPS Policies on page 513](#)

## Managing Policy Locks

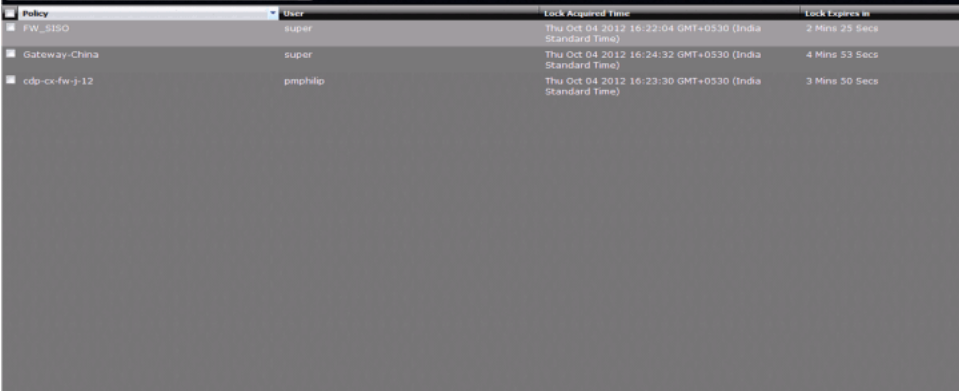
All the locked policies can be viewed in a single page. This page is available for a user having Manage Policy Locks tasks assigned. This page shows all the locks only if the user has Unlock task assigned, other wise user will see only his locks. To view the locked policies:

1. Select **Security Director > IPS Policy > Manage Policy Locks**.

The Manage Policy Locks page appears showing only those locks that can be managed by the current user. The page contains the following fields:

- Policy name
- User (IP Address)
- Lock acquired time
- Time for lock expiry

Figure 258: IPS Policy-Manage Policy Locks



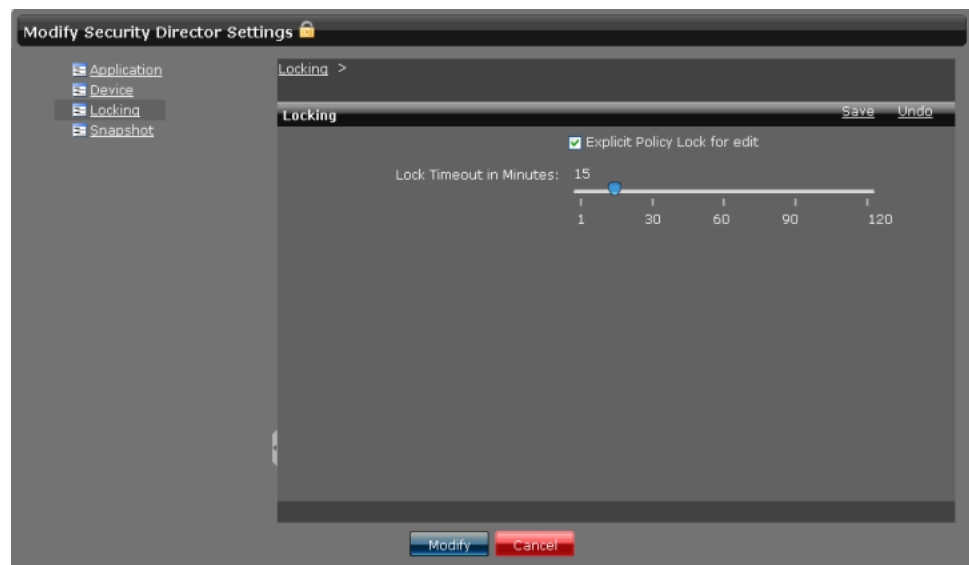
Policy	User	Lock Acquired Time	Lock Expires In
FW_3150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 25 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilo	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	3 Mins 50 Secs

2. Right-click the policy that you want to unlock, and press Unlock. You can select policies that are locked by you and unlock them. To unlock your policies, you do not need any administrator privileges. To unlock policies locked by other users, you must have the task LOCK assigned to you.

User with administrator privileges can configure the lock settings. To configure the lock settings:

1. Click **Application Switcher**, and go to **Network Application Platform > Administration > Manage Applications**.
2. Right-click the **Security Director** application, and select **Modify Application Settings**. The following page appears, as shown in [Figure 259 on page 504](#).

Figure 259: Modify Security Director Settings



3. Under the Locking option, you can configure the locking timeout value in minutes. The minimum value that you can configure is 2 minutes and the maximum 120 minutes. By default, the timeout value is configured for 5 minutes.
4. By default, the Explicit Policy Lock for edit option is enabled. You can disable this option, if you do not want to lock the policies before editing. When this option is disabled, policies can be edited by any user. The first user gets the preference of saving the changes for a policy. The next save on the same version of a policy results in the user being asked to save policy with new name.



**NOTE:** Acquiring a policy lock or releasing a lock is audit logged. Release locking will show the reason for the release, for example, an explicit release, on save, discard, timeout, or administrator release. Administrator changes of the lock configuration are also audit logged. To see the audit logs, from the Security Director task bar, select Audit Logs.

#### Related Documentation

- [Creating IPS Policies on page 494](#)
- [Publishing IPS Policies on page 509](#)
- [Managing IPS Policies on page 513](#)

## Ordering the Rules in a IPS Policy

To reorder the rules in a IPS policy:

1. Select **Security Director > IPS Policy**.

The Policy Tabular view appears.

2. Select the IPS policy whose rules you want to reorder.

The rules of the IPS policy are displayed in the right pane.

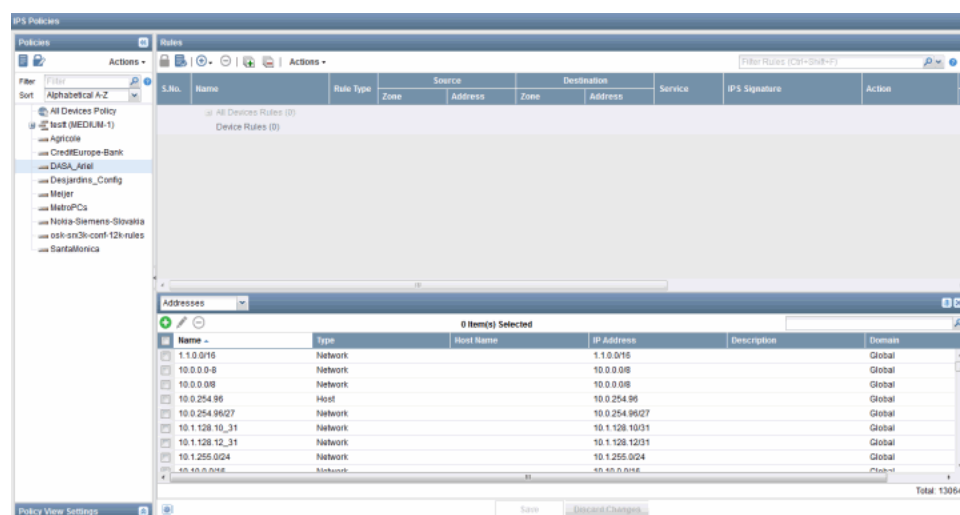
3. Select a rule that you want to reorder and click the appropriate icon on the top of the right pane.

Icon Name	Description
Move Rule Up	Moves the rule one level up in the hierarchy.
Move Rule Down	Moves the rule one level down in the hierarchy.
Move Rule to Top	Moves the rule to the top of the hierarchy.
Move Rule to Bottom	Moves the rule to the bottom of the hierarchy.

The rule is now positioned accordingly. When the IPS policy is provisioned, the rules are provisioned to the devices in the order you have specified.

The address and service objects can be created, managed, dragged and dropped to the required rules from the IPS policy landing page. The objects are listed in the policy landing page, as shown in [Figure 260 on page 505](#).

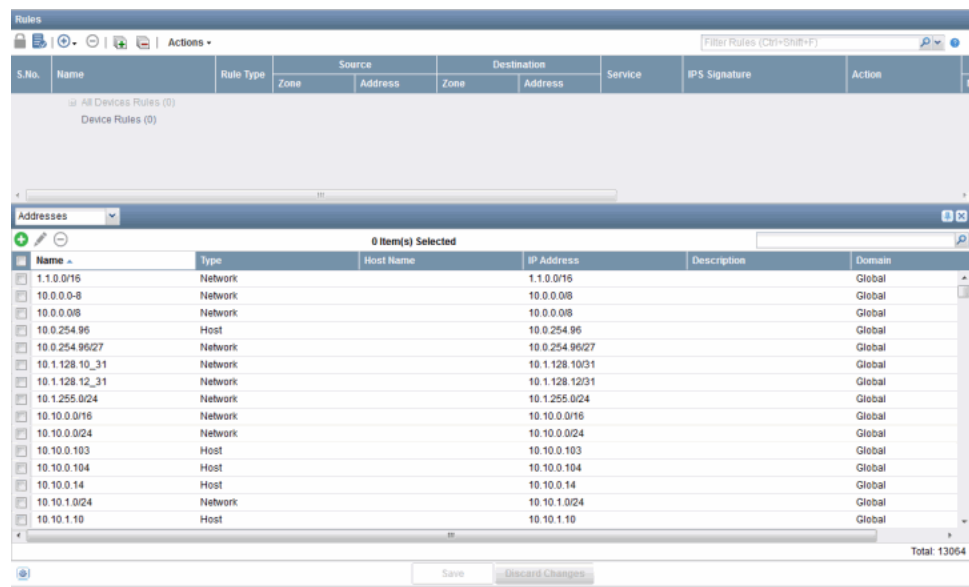
**Figure 260: IPS Policies Landing Page**



You can select address or service objects from the drop-down list. To create a new address or service object, click the plus sign (+). To know more about creating address and services objects, see [“Creating Addresses” on page 124](#) and [“Creating Services” on page 108](#).

You can modify an object by clicking the pencil icon and delete objects by clicking the minus sign (-). You can search for any object by its name and IP address in the search field available in the top right corner, as shown in [Figure 261 on page 506](#).

Figure 261: IPS Policies- Drag and Drop Objects Window



You can drag more than one object and drop on the respective columns in the policy tabular view. Security Director ensure that objects are dropped in the supported columns and it does not permit to drop under any other columns. The drag and drop of objects is supported on the Source Address, Destination Address, and Service columns. You can drag a single service from drag panel and drop it into IPS Policy rule service field. However, multiple service drag and drop is restricted. Before dropping any object to the policy rules, you must first lock the respective policy. You can drag and drop a single address from source address field to destination address field of same rule or across rules. Also, you can drag and drop a single service across rules. However, you cannot drag and drop multiple items across rules. In the IPS policy landing page, you can reorder the rules by dragging and dropping.

You can drag and drop the objects across the rules. If an object already exists for a rule and you drop a new object, the previous object is over written by the new object. The new object is copied to the rule.

#### Related Documentation

- [Creating IPS Policies on page 494](#)
- [Adding Rules to an IPS Policy on page 507](#)
- [Publishing IPS Policies on page 509](#)
- [Managing IPS Policies on page 513](#)

---

## Adding Rules to an IPS Policy

---

To add rules to an IPS policy:

1. Select **Security Director > IPS Policy**.

The IPS Policy tabular view appears.

2. From the left pane, click the IPS policy to which you want to add rules.

The right pane displays the existing rules of the IPS policy.

3. Click the **+** icon to add a rule and select the type of the rule you want to add (IPS or Exempt rule). The newly added rules blink a different color for a few seconds. A new rule is added to the bottom row.

4. Click the **Name** field in the rule and change the name of the rule.

5. Click the **Source Zone** field in the rule and select the appropriate zone from the list of zones.

6. Click the **Source Address** field in the rule.

The address selector appears.

7. From the Available column, select the addresses you want to associate the rule to. You can select all addresses by clicking **Page** and clear them all by clicking **None**.

8. Click the right arrow in the address selector. There are two options available such as Include Selected and Exclude Selected. If you select **Include Selected**, all the addresses selected are sent to the device. If you select the **Exclude Selected**, except the selected addresses, all other configurations are moved to the device.

The selected addresses are now moved to the Selected column.

9. Click **OK**.

10. Click the **Destination Zone** field in the rule and select the appropriate zone from the list of zones.

11. Click the **Destination Address** field in the rule.

The address selector appears.

12. Select the addresses you want to associate the rule to, from the Available column. You can select all addresses by clicking **Page** and unselect them all by clicking **None**.

13. Click the right arrow in the address selector.

The selected addresses are now moved to the Selected column.

14. Click **OK**.

15. Click the **Service** field in the rule.

The service selector appears.

16. Select the services you want to associate the rule to, from the Available column.

17. Click the right arrow in the service selector.

The selected services are now moved to the Selected column.

18. Click **OK**.

19. Click the **IPS Signature** column in the rule.

The IPS Signature Selector window appears. You can select and add IPS signatures from this window.

20. Click **Update** in the IPS Signature Selector window when you select the IPS signatures for the rule.

21. Click **Action** column in the rule and select the appropriate action for the rule.

22. Click **Notification** column in the rule.

A drop-down menu with all notification options appears. To add appropriate notification options:

- a. Click the check box next to the Attack Logging field if you want to log the attacks.
- b. Click the check box next to the Alert Flag field if you want to flag attacks.
- c. Click the check box next to the Log Packets if you want to log the packets.
- d. Click **OK**.

23. Click **IP Action** column in the rule.

A drop-down menu with all IP action option appears.

- a. Select the appropriate option from the IP Action drop-down menu.
- b. Select the appropriate option from the IP Target drop-down menu.
- c. Enter the value of the timeout interval in the Timeout Value field.
- d. Click **Log Taken** and **Log Creation** fields, if you want to maintain a log of the IP actions performed.
- e. Click **OK**.

24. Click **Additional** column in the rule.

- a. Select the appropriate severity from the Severity drop-down menu.
- b. Click the check box next to the Terminal field.
- c. Click **OK**.

25. Click the **Description** column and enter a description for the rule.

26. Click **Save**.

**NOTE:**

- For exempt rules, Action and IPS Options (Notification, IP Action, and Additional) are not available.
- If you have any cut or copied rules or rule groups, you will have Paste Rules links to paste the rules or rule groups. The pasting options are available only for the predefined rule groups.

**Related Documentation**

- [Creating IPS Policies on page 494](#)
- [Ordering the Rules in a IPS Policy on page 504](#)
- [Publishing IPS Policies on page 509](#)
- [Managing IPS Policies on page 513](#)

## Publishing IPS Policies

To publish an IPS policy:

1. Select **Security Director > IPS Management > Publish IPS Policy**.

The Services page appears with all the IPS policies. It also displays the publish states of the IPS policies.

2. Select the check box next to the IPS policy that you want to publish.
3. Select the **Schedule at a later time** check box if you want to schedule and publish the configuration later, as shown in [Figure 262 on page 509](#).

**Figure 262: IPS Policy Publish Page**

IPS Policy > Publish IPS Policy

Select: All | None Type to Search Service

Name	Publish State	Description
<input checked="" type="checkbox"/> All Devices Policy	Published	Predefined Policy for all devices
<input type="checkbox"/> GP-1	Published	

☒ Schedule at a later time

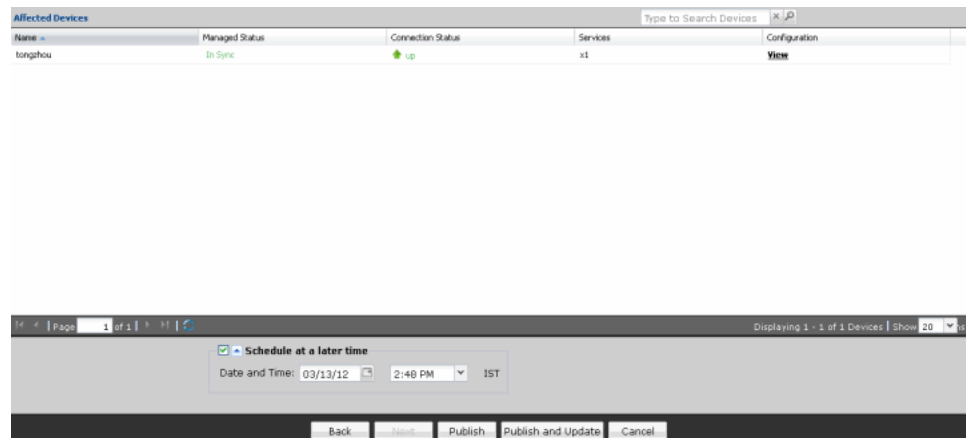
Date and Time: 11/02/12 12:39 PM UTC+05:30

Back Next Publish Publish and Update Cancel

4. Click **Next**.

The Affected Devices page displays the devices on which this IPS policy will be published, as shown in [Figure 263 on page 510](#).

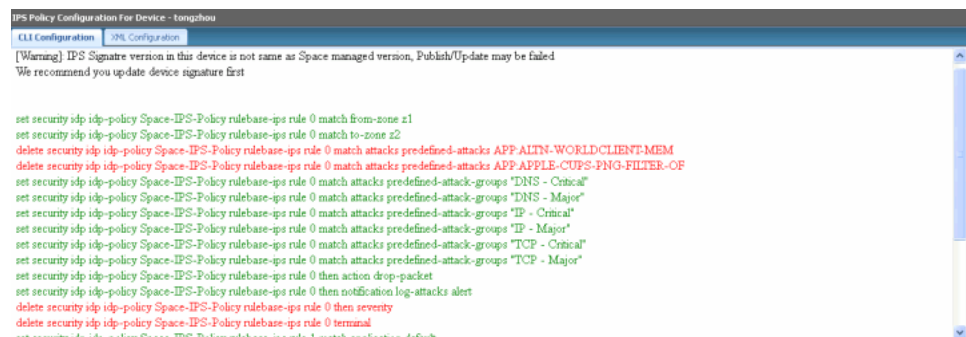
**Figure 263: Policy Publish-Affected Devices Page**



5. If you want to preview the configuration changes that will be pushed to the device, click **View** in the Configuration column that corresponds to the device. The Configuration Preview progress bar is shown while the configuration to be pushed to the device is generated.

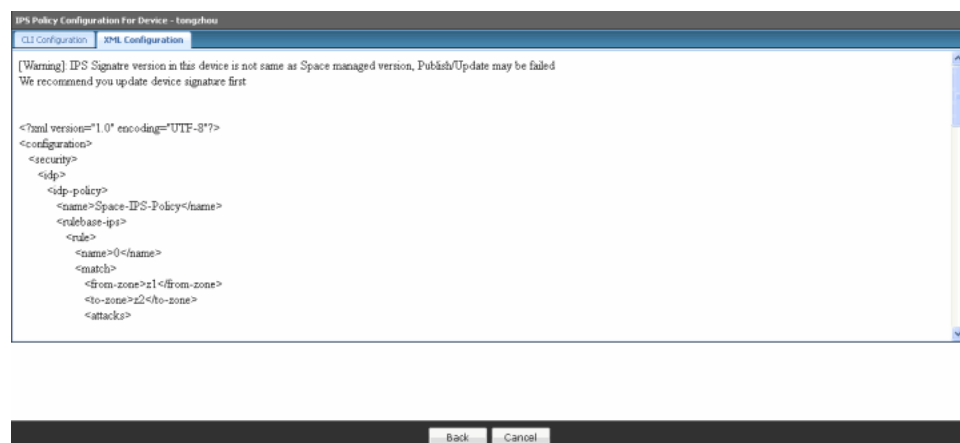
The CLI Configuration tab appears by default. You can view the configuration details in CLI format, as shown in [Figure 264 on page 510](#).

**Figure 264: Policy Publish-CLI Configuration**



6. View the XML format of the configuration by clicking the **XML Configuration** tab, as shown in [Figure 265 on page 511](#).

Figure 265: Policy Publish-XML Configuration



7. Click **Back**.

8. Click **Publish** if you want only to publish the configuration.

A new job is created and the job ID appears in the Job Information dialog box.

9. Click **Publish and Update** if you want both to publish and to update the devices with the configuration.

The IPS policy is now moved into the Published state if the configuration is published to all devices involved in the IPS policy. If the configuration is not published to all devices involved in the IPS policy, the IPS policy is placed in the Partially Published state. If an IPS policy is created but not published, the IPS policy is placed in the Unpublished state. If any modifications are made to IPS policy configuration after it is published, the IPS policy is placed in the Republish Required state. You can view the states of the policies by mousing over them. When an address object in the Global domain referenced by a policy in the D1 domain changes, the state of the policy is changed to Republish Required. This occurs though the changes are in the address object, which is in the other domain, and is not same as the policy domain. This applies to all the objects referenced by all the services.

A new job is created and the job ID appears in the Job Information dialog box.

10. Click the job ID to view more information about the job created. This action redirects you to the Job Management workspace. In the Job Management workspace, the commit check status and the compile status are both checked at the device end. The state is changed to either success or failure, depending on the compile status of the configuration. There is a timeout window of 15 minutes for the compile status. If the compilation takes longer than 15 minutes, the job fails with a warning message.

If you get an error message during the publish, or if the IPS policy publish fails, go to the Job Management workspace and view the relevant job ID to see why the publish failed. Also, during the compile, detailed job view captures the compile progress.

In the Job Details window, use the available filter box to search for any device by filter name, tag name, or IP address. Filtering works only for currently available devices. Search with the first character of the tag name to search by tag name. If you search with any middle characters, the search fails.

During the publish and update, the disabled rules and objects are not deleted. Disabled rules are updated as inactive configuration. This is an optional setting. You can choose to push the disabled rules to a device by selecting **Update disabled rules to device** option in Security Director application setting, under Platform. By default, Update disabled rules to device option is disabled. For the pushed disabled rules to work after the upgrade, Security Director must import the policy again and the application firewall signature must be downloaded prior to the import.

If you are having the disabled rules on the device, as shown in the following example:

```
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
  destination-address any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 match
  application any
set security policies from-zone untrust to-zone trust policy Device-Zone-5 then
  deny
deactivate security policies from-zone untrust to-zone trust policy Device-Zone-5
```

When you import this rules, Security Director sets the state as disabled. If a particular node in the CLI is deactivated, that node is not imported into the Security Director.

If you import a rule, as shown in the following example, Security Director will not set the application service.

```
set security policies from-zone trust to-zone untrust policy Device-Zone-2
description "Rule With Infranet All Traffic Auth"
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
  source-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
  destination-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 match
  application any
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
  permit application-services idp
set security policies from-zone trust to-zone untrust policy Device-Zone-2 then
  permit application-services uac-policy captive-portal captiveportal_65573
deactivate security policies from-zone trust to-zone untrust policy Device-Zone-2
  then permit application-services
```

Security Director does not support inactive nodes and the inactive rules. If the objects in the rule are not defined, Security Director provides a warning message, at the time of import, listing the objects that are not defined.

**NOTE:**

- You can also publish an IPS policy by right-clicking the IPS policy in the IPS Policy tabular view and selecting Publish Policy. You are redirected to the Affected Devices page.
- You can search for a specific device on which the policy is published by entering the search criteria in the Search field, in the top-right corner of the Services page. You can search the devices by their name, IP address, and device tags.
- If the IPS policy is to be published on a large number of devices, the devices are displayed across multiple pages. You can use the pagination and display options available on the lower ribbon, just below the list of devices, to view all devices on which the policy is published.
- When you configure Packet Capture on a device that does not have the sensor setting, Security Director shows a warning message in the IPS publish window.
- If a device does not have a license or has an expired license, a warning message appears during the publish and update of the IPS policy. However, the CLI is still generated.
- The publish fails if you have two addresses in a rule with a same name, one from the Global domain and the other from the child domain.
- You can publish or update the group policy of the global domain from another domain. In this case, policy is published or updated to only those devices which are part of the another domain. However, if you publish or update the group policy in the global domain, the policy is published or updated to all the devices including the devices from the another domain.

- Related Documentation**
- [Creating IPS Policies on page 494](#)
  - [Managing IPS Policies on page 513](#)

## Managing IPS Policies

You can delete, enable, and disable rules in an IPS policy, in advanced mode.

To open the IPS Policies page:

- Select **Security Director > IPS Policy**.

The IPS Policy Tabular view appears.

You can perform the following tasks in the IPS Policies space. These tasks are only permitted when firewall policy is set to IPS Advanced mode.

1. [Deleting IPS Policy Rules on page 514](#)
2. [Enabling or Disabling Rules in an IPS Policy on page 514](#)

3. [Cloning a Rule in an IPS Policy on page 514](#)
4. [Grouping Rules in an IPS Policy on page 515](#)
5. [Expanding/Collapsing All Rules in an IPS Policy on page 515](#)
6. [Cutting/Copying And Pasting Rules or Rule Groups in an IPS Policy on page 515](#)
7. [Adding Rules to an IPS Policy on page 516](#)
8. [Rule Operations on the Filtered Rules on page 516](#)

## Deleting IPS Policy Rules

To delete rules in an IPS policy:

1. Select **Security Director > IPS Management**.  
The IPS Policy tabular view appears.
2. Select the device policy from which you want to delete IPS policy rules.  
The right pane displays the device rules for which IPS policy is enabled.
3. Select the check box next to the IPS or exempt rule you want to delete.
4. Click the **Delete** icon.
5. Click **Save**.

## Enabling or Disabling Rules in an IPS Policy

To enable or disable rules in an IPS policy:

1. Select **Security Director > IPS Management**.  
The IPS Policy tabular view appears.
2. Select the IPS policy whose rules you want to enable or disable.  
The rules of the firewall policy are displayed in the right pane.
3. Select the check boxes next to the rules that you want to enable or disable.
4. Click the **Enable** or **Disable** icon.
5. Click **Save**.

## Cloning a Rule in an IPS Policy

To clone a rule in an IPS policy:

1. Select **Security Director > IPS Policy**.  
The IPS Policy tabular view appears.
2. Select the IPS policy whose rule you want to clone.  
The rules of the IPS policy appears in the right pane.
3. Select the check box next to the rule that you want to clone.
4. Right-click and select **Clone**.

## Grouping Rules in an IPS Policy

To group rules in an IPS policy:

1. Select **Security Director > IPS Policy**.

The Policy tabular view appears.

2. Select the IPS policy whose IPS rules you want to group.

The rules of the IPS policy are displayed in the right pane.

3. Select the check boxes next to the rules you want to group.

4. Right-click the rules and select **Rule Group > Create Rule Group**.

The Create Rule Group pop-up window appears.

5. Enter a name for the rule group in the Name field.

6. Enter a description for the rule group in the Description field.

7. Click **Create**.



**NOTE:** When the rule group is created, you can add rules in the rule group, modify the rule group name, move the rule into another rule group, ungroup rules, and ungroup rule groups using appropriate options.

## Expanding/Collapsing All Rules in an IPS Policy

To expand or collapse all rules in an IPS policy:

1. Select **Security Director > IPS Policy**.

The IPS Policy tabular view appears.

2. Select the IPS policy whose rules you want to expand.

By default, IPS policy rules in collapsed state are displayed in the right pane.

3. Click the **Expand All RuleGroups** icon, and all rules corresponding to that particular policy are expanded.

4. Click the **Collapse All RuleGroups** icon to collapse all rules.

## Cutting/Copying And Pasting Rules or Rule Groups in an IPS Policy

To cut or copy and paste rules or rule groups in an IPS policy:

1. On the right pane, select the device rule or rule group that you want to cut or copy. Right-click the selected device rule or rule group, and select **Cut** or **Copy**. If Cut is selected, related rule or rule group is removed from the right pane view.

You can copy the rules without locking a policy. However, you must lock the policy for the cut operation. You can select the combination of rules or rule groups for cutting

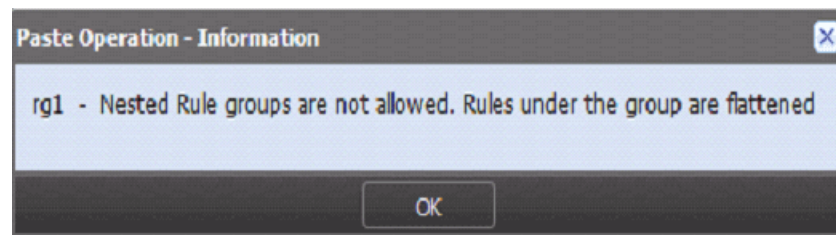
or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

2. On the left pane, select the IPS policy in which you want to paste the rule or rule group. On the right pane, right-click the rule or rule group that you want to paste. You can paste the rule or rule group before or after the selected rule or rule group by choosing the **Paste Before** or **Paste After** option, respectively.

If you are cutting and pasting rules across different policies, you must first save the cut operation in the current policy before moving to another policy for pasting. Otherwise, an error message is displayed, giving you the option either save or discard the changes.

Security Director does not support nested rule grouping. If you paste a rule group in another custom rule group, an error message is displayed, giving you the option to proceed by flattening the copied rule group, as shown in [Figure 266 on page 516](#).

**Figure 266: Nested Rule Groups Paste Operation Warning Message**



## Adding Rules to an IPS Policy

You can add the rules before or after the IPS rule or exempt rule. To add rules:

1. Select **Security Director > IPS Policy**.

The Policy tabular view appears.

2. Select the IPS rule to which you want to add rules, right-click, and select **Add Rules Before** or **Add Rules After**.

You will get an option to add rules before the IPS rule or Exempt rule, or after the IPS rule or Exempt rule.

## Rule Operations on the Filtered Rules

You can perform various rule operations on the filtered list of rules. For example, consider a policy having seven rules such as *a*, *b*, *c*, *d*, *e*, *f*, and *g* in an order inside a rule group. After filtering, if only second and sixth rules are filtered, that is only rules *b* and *f*,

[Table 44 on page 517](#) explains the various rule operations on the filtered rules.

Table 44: Various Rule Operation on the Filtered Rules

Rule Operation	Description
Add rule before	<p>To add a new rule before an existing rule, select the existing rule in the filtered list and add the new rule above it.</p> <p>For example, if you perform this operation by selecting the sixth rule that is <i>f</i>, the seventh rule must be added before the sixth rule, in the filtered list. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Add rule after	<p>To add a new rule after an existing rule, select the existing rule in the filtered list and add the new rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the seventh rule must be added after the second rule. This rule is added at the third place in the full list.</p>
Paste before	<p>To paste a copied rule before an existing rule, select the existing rule in the filtered list and paste the copied rule above it.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the copied rule must be added after the sixth rule. The rule <i>f</i> must be moved down to the seventh place in the full list.</p>
Paste after	<p>To paste a copied rule after an existing rule, select the existing rule in the filtered list and paste the copied rule below it.</p> <p>For example, If you perform this operation by selecting the second rule that is <i>b</i> in the filtered list, the copied rule must be added after the second rule. The new rule is added at the third place in the full list.</p>
Clone	<p>To clone a selected rule, select the existing rule you want to clone in the filtered list. The cloned rule will be added above the selected rule.</p> <p>For example, If you perform this operation by selecting the sixth rule that is <i>f</i> in the filtered list, the cloned rule must be added after the sixth rule, at the seventh place. The rule <i>g</i> must be moved down to the eighth place in the full list. This can be checked by clearing the filter from the search box.</p>
Move rule to top	<p>To move a rule to the top of a list, select the rule you want to move in the filtered list and move rule to the top. If you move a rule from a filtered list to the top of that list, the selected rule is also moved to the top of the full list.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved to the top in the rule group, at first place in the original list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule to bottom	<p>To move a rule to the bottom of the list, select the rule you want to move in the filtered list and move rule to the bottom. If you move a rule from a filtered list to the bottom of that list, the selected rule is also moved to the bottom of the full list.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved to the bottom in the rule group, at the seventh place in the full list. This can be checked by clearing the filter from the search box.</p> <p>This option is disabled for the last rule in the full list.</p>

Table 44: Various Rule Operation on the Filtered Rules (*continued*)

Rule Operation	Description
Move rule up	<p>To move a rule up one position in the list, select the rule you want to move in the filtered list and move rule up one position.</p> <p>For example, If you perform this operation by selecting the sixth rule <i>f</i> in the filtered list, the rule <i>f</i> must be moved before the second rule <i>b</i> in the filtered list. This rule is moved to the second place in the rule group in the full list.</p> <p>This option is disabled for the top rule in the full list.</p>
Move rule down	<p>To move a rule down one position in the list, select the rule you want to move in the filtered list and move rule down one position.</p> <p>For example, If you perform this operation by selecting the second rule <i>b</i> in the filtered list, the rule <i>b</i> must be moved after the sixth rule <i>f</i> in the filtered list. This rule is moved to the sixth rule in the rule group in the full list.</p> <p>This option is disabled for the last rule in the full list.</p>

- Related Documentation**
- [Creating IPS Policies on page 494](#)
  - [Ordering the Rules in a IPS Policy on page 504](#)
  - [Adding Rules to an IPS Policy on page 507](#)
  - [Publishing IPS Policies on page 509](#)

## PART 14

# Configuring Network Devices

- [Creating and Managing Security Zones on page 521](#)
- [Creating and Managing Screens on page 527](#)
- [Configuring Security Logs on page 535](#)
- [Creating and Managing Static Routes on page 541](#)
- [Creating and Managing Routing Instances on page 549](#)
- [Managing Physical Interfaces and Syslog on page 555](#)



# Creating and Managing Security Zones

- [Creating a Security Zone for a Device on page 521](#)
- [Managing Security Zones on page 524](#)

## Creating a Security Zone for a Device

---

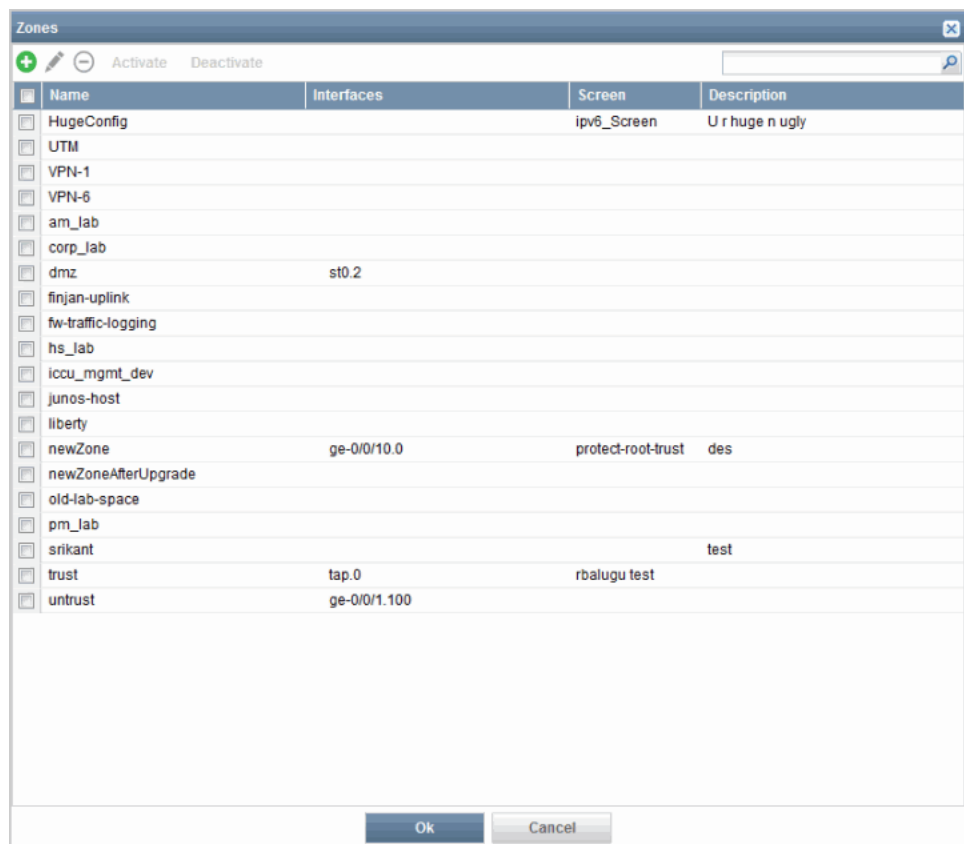
You can create a new security zone or screen for a device in conjunction with the Junos Space Network Application Platform. The Security Director Device Configuration page fetches the DMI configuration value from the Network Application Platform and provides the GUI for making the modifications on the Device Configuration page. Once you finish the modifications, the changes are ported back to the Network Application Platform.

To create a new security zone:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Security section, click **Zones**.

The Zones main page appears, showing the existing zones, as shown in [Figure 267 on page 522](#).

Figure 267: Device Configuration-Zones Main Page



- To add a new zone, click the plus sign (+).

The Create Zone page appears, as shown in [Figure 268 on page 523](#).

Figure 268: Device Configuration-Create Zone Page

**Create Zone**

**General Information**

Name\*: zone-crt

Description:

Application Tracking: ☒

**Interfaces**

Available	Selected
Filter <input type="text"/> <input type="button" value="Search"/> <input type="button" value="Info"/> <b>Select:</b> Page   None fxp0.0 ge-2/0/0.0 ge-9/0/0.0	<b>Select:</b> Page   None ge-11/0/3.0 ge-9/0/3.0

**Traffic Control Options**

Ok Cancel

5. In the Name field, enter the name of the new zone. The asterisk indicates that it is a mandatory field.
6. In the Description field, enter a description for the new zone.
7. By default, the Application Tracking check box is not selected. To maintain the statistics on a device for its application usage, and to provide the application activity update message through the system log, select the **Application Tracking** check box.
8. Under the Interfaces section, in the Available column, select the required interfaces and move them to the Selected column.  
  
You can search for any interface in the Search field of the Available column.
9. Expand the Traffic Control Options section to configure the following parameters:
  - To send an RST for non-SYNC packets that do not match the TCP session, select the **Send TCP reset for non-SYN packet outside existing session** check box.
  - From the Screens drop-down box, select the available screens.
10. Expand the Host Inbound Traffic section to configure the following parameters:
  - Expand the System Services section to select the list of system services. From the Available column, select the required services and move them to the Selected column.

By default, the Permit-List radio button is selected. This permits all the services listed in the Selected column. If you select the Except-List radio button, all other services except the services listed in the Selected column are allowed.

- Expand the Protocols section to select the required protocols. From the Available column, select the required protocols and move them to the Selected column.

By default, the Permit-List radio button is selected. This permits all the protocols listed in the Selected column. If you select the Except-List radio button, all other protocols except the protocols listed in the Selected column are allowed.

11. Expand the Interface Services and Protocols section to configure the allowed system services and protocols.
12. Click **Ok**.

A new zone is created and added to the device.

#### Related Documentation

- [Managing Security Zones on page 524](#)

---

## Managing Security Zones

You can modify, delete, activate, and deactivate the security zones that are listed on the Zones main page.

To manage the zones, right-click the zone or select the required options from the toolbar.

You can perform the following management tasks on the Zones page.

- [Modifying a Security Zone on page 524](#)
- [Deleting a Security Zone on page 525](#)
- [Deactivating a Security Zone on page 526](#)
- [Activating a Security Zone on page 526](#)

### Modifying a Security Zone

To modify a security zone:

1. Select **Security Director > Devices > Device Management**.

The Device Management page appears.

2. Right-click a device and select **Device Configuration > Modify Configuration**.

The View/Edit Configuration page appears.

3. Under Security, click **Zones**.

The Zones main page appears.

4. Select the zone that you want to modify, and click the pencil icon or right-click the zone and select **Edit**.

The Modify Zone page appears, as shown in [Figure 269 on page 525](#).

Figure 269: Modify Zone Page

**Modify Zone -- active-directory-services**

**General Information**

Name\*: active-directory-services

Description:

Application Tracking:

**Interfaces**

Available		Selected
Filter		
fxp0.0		
ge-11/0/3.0		
ge-2/0/0.0		
ge-9/0/0.0	+	
ge-9/0/3.0	-	

**Traffic Control Options**

Ok Cancel

5. On the Modify Zone page, you can modify the required values.
6. To modify the selected zone, click **Ok**.

## Deleting a Security Zone

To delete a security zone:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Security, click **Zones**.  
The Zones main page appears.
4. Select the zone that you want to delete, and click the minus sign (-) or right-click the zone and select **Delete**.  
A confirmation message appears before the zone is deleted. You can select multiple zones for deletion.
5. To confirm the deletion, click **Ok**.

## Deactivating a Security Zone

To deactivate a security zone:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Security, click **Zones**.  
The Zones main page appears.
4. Select the zone that you want to deactivate, right-click it, and select **Deactivate**.  
The deactivated zone is greyed out and not available for any selection.

## Activating a Security Zone

To activate a deactivated zone:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Security, click **Zones**.  
The Zones main page appears.
4. Select the deactivated zone that you want to activate, right-click it, and select **Activate**.  
The zone is activated and available for any selection.

**Related Documentation**

- [Creating a Security Zone for a Device on page 521](#)

# Creating and Managing Screens

- [Creating a Screen for a Device on page 527](#)
- [Managing Screens on page 531](#)

## Creating a Screen for a Device

---

To create a new screen:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Security section, click **Screens**.  
The Screens main page appears, showing the existing screens.
4. To add a new screen, click the plus sign (+).  
The Create Screen page appears, as shown in [Figure 270 on page 528](#).

Figure 270: Device Configuration-Create Screen Page

The screenshot shows a 'Create Screen' dialog box. It has a title bar with the text 'Create Screen' and a close button. The main content area is divided into sections. The first section is 'Basic Information', which contains a 'Name\*' field (marked as mandatory) and a 'Description' field. Below these fields is a checkbox labeled 'Generate alarms without dropping packets'. There are four expandable sections below: 'Denial of Service', 'Anomalies', 'Flood Defense', and 'Reconnaissance'. At the bottom of the dialog are 'Ok' and 'Cancel' buttons.

5. Under the Basic Information section, configure the following parameters:
  - In the Name field, enter the name of the new screen. This is a mandatory field.
  - In the Description field, enter a description for the new screen.
  - To direct the device to generate an alarm when detecting an attack but not to block the attack, select the **Generate alarms without dropping packets** check box.
6. Expand the Denial of Service section to configure the following parameters:
  - To enable the land attack protection option, select the **Land Attack Protection** check box.  

Land attacks occur when an attacker sends spoofed SYN packets containing the IP address of the victim as both the destination and source IP address.
  - To enable the teardrop protection option, select the **Teardrop attack protection** check box.  

Teardrop attacks exploit the reassembly of fragmented IP packets.
  - To enable the ICMP fragment protection option, select the **ICMP fragment protection** check box.

Because ICMP packets contain very short messages, there is no legitimate reason for ICMP packets to be fragmented. If an ICMP packet is so large that it must be fragmented, something is amiss.

- To enable the ping of death attack protection option, select the **Ping of death attack protection** check box.

A ping of death occurs when sent IP packets exceed the maximum legal length (65,535 bytes).

- To enable the large (size > 1024) ICMP packet protection option, select the **Large size ICMP packet protection** check box.
- To enable IP fragment blocking, select the **Block fragment traffic** check box.
- To enable the SYN-ACK-ACK proxy protection screen option, select the **SYN-ACK-ACK- proxy protection** check box.
- To enable the WinNuke attack protection option, select the **WinNuke attack protection** check box.

WinNuke is a DoS attack targeting any computer on the Internet running Windows.

7. Expand the Anomalies section to configure the following parameters:

Under the IP Packet Header section, configure the following parameters:

- To enable the IP with bad option IDs screen option, select the **Bad option** check box.
- To enable IP with security options, select the **Security** check box.

This provides a way for hosts to send security.

- To enable the unknown protocol protection option, select the **Unknown protocol protection** check box.
- To specify the complete route list for a packet to take on its journey from source to destination, select the **Strict source route** check box.
- To enable the IP with source route option, select the **Source route** check box.
- To enable the IP with the timestamp option, select the **Timestamp** check box.

This records the time (in Coordinated Universal Time, or UTC) when each network device receives the packet during its trip from the point of origin to its destination.

- To enable the IP with stream option, select the **Stream** check box.
- This provides a way for the 16-bit SATNET stream identifier to be carried through networks that do not support the stream concept.
- To enable the IP with loose source route option, select the **Loose source route** check box.

This specifies a partial route list for a packet to take on its journey from source to destination.

- To enable the IP with record route option, select the **Record route** check box.

Under the TCP Segment Header section, configure the following parameters:

- To enable the SYN fragment option, select the **SYN Fragment Protection** check box.
- To enable the SYN and FIN flags set option, select the **SYN and FIN Flags Set Protection** check box.
- To enable the FIN flag without ACK and FIN flag set options, select the **FIN Flag without ACK Flag Set Protection** check box.
- To enable the TCP packet without flag set option, select the **TCP Packet without Flag Set Protection** check box.

A normal TCP segment header has at least one flag control set.

8. Expand the Flood Defense section, and configure the following parameters:

- To limit the sessions from the same source IP, enter the number of allowed sessions in the Limit sessions from the same source field.
- To limit the sessions from the same destination IP, enter the number of allowed sessions in the Limit sessions from the same destination field.

Under ICMP/UDP protection, configure the following parameters:

- To enable the ICMP flood protection option, select the **ICMP flood protection** check box.

An ICMP flood typically occurs when ICMP echo requests use all resources in responding, such that valid network traffic can no longer be processed.

- To enable the UDP flood protection option, select the **UDP flood protection** check box.

UDP flooding occurs when an attacker sends IP packets containing UDP datagrams with the purpose of slowing down the resources, such that valid connections can no longer be handled.

Under the SYN flood protection section, configure the following parameter:

- To enable the SYN flood protection option, select the **SYN Flood Protection** check box.

9. Expand the Reconnaissance section, and configure the following parameters:

- To enable IP address spoofing, select the **IP spoofing** check box.

IP spoofing is when a bogus source address is inserted in the packet header to make the packet appear to come from a trusted source.

- To enable IP address sweep, select the **IP sweep** check box.

An IP address sweep is launched with the intent of triggering responses from active hosts.

- To configure the device detect and prevent TCP sweep attack, select the **TCP Sweep** check box.

- To configure the device detect and prevent UDP sweep attack, select the **UDP Sweep** check box.
- To enable port scanning, select the **Port scan** check box.

The purpose of this attack is to scan available services to locate one or more ports that respond, thus identifying a service to target.

10. To create a new screen, click **Ok**.

#### Related Documentation

- [Managing Screens on page 531](#)

---

## Managing Screens

You can modify, delete, activate, and deactivate the screens that are listed on the Screens main page.

To manage screens, right-click the screen or select the required options from the toolbar.

You can perform the following management tasks on the Screens page.

- [Modifying a Screen on page 531](#)
- [Deleting a Screen on page 532](#)
- [Deactivating a Screen on page 533](#)
- [Activating a Screen on page 533](#)

## Modifying a Screen

To modify a screen:

1. Select **Security Director > Devices > Device Management**.

The Device Management page appears.

2. Right-click a device and select **Device Configuration > Modify Configuration**.

The View/Edit Configuration page appears.

3. Under Security, click **Screens**.

The Screens main page appears.

4. Select the screen that you want to modify, and click the pencil icon or right-click the screen and select **Edit**.

The Modify Screen page appears as shown in [Figure 271 on page 532](#).

Figure 271: Modify Screen Page

**Modify Screen -- scr-test**

**Basic Information**

Name\*: scr-test

Description:

Generate alarms without dropping packets: ☒

**Denial of Service**

☐ Land Attack Protection

☐ Teardrop attack protection

☐ ICMP fragment protection

☐ Ping of death attack protection

☐ Large size ICMP packet protection

☐ Block fragment traffic

☐ SYN-ACK-ACK proxy protection

☐ WinNuke attack protection:

**Anomalies**

☐ IP Packet Header

☐ Bad option

☐ Security

☐ Unknown protocol

Ok Cancel

The Modify Screen page appears.

5. On the Modify Screen page, you can modify the required values.
6. To modify the selected screen, click **Ok**.

## Deleting a Screen

To delete a screen:

1. Select **Security Director > Devices > Device Management**.

The Device Management page appears.

2. Right-click a device and select **Device Configuration > Modify Configuration**.

The View/Edit Configuration page appears.

3. Under Security, click **Screen**.

The Screens main page appears.

4. Select the screen that you want to delete, and click the minus sign (-) or right-click the screen and select **Delete**.

A confirmation message appears before the screen is deleted. You can select multiple screens for deletion.

5. To confirm the deletion, click **Ok**.

## Deactivating a Screen

To deactivate a screen:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device, and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Security, click **Screens**.  
The Screens main page appears.
4. Select the screen that you want to deactivate, right-click it, and select **Deactivate**.  
The deactivated screen is greyed out and not available for any selection.

## Activating a Screen

To activate a deactivated screen:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device, and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Security, click **Screens**.  
The Screens main page appears.
4. Select the deactivated screen that you want to activate, right-click it, and select **Activate**.  
The screen is activated and available for any selection.

### Related Documentation

- [Creating a Screen for a Device on page 527](#)



# Configuring Security Logs

- Creating Security Logs on page 535

## Creating Security Logs

To configure security logging:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Security section, click **Security Logging**.

The Create Security Logging page appears, as shown in [Figure 272 on page 535](#).

**Figure 272: Device Configuration-Create Security Logging Page**

The screenshot shows the 'Create Security Logging' dialog box. It has a title bar and a close button. The content is organized into sections with expandable/collapsible headers. The 'General Settings' section is expanded, showing various configuration options. The 'Stream' section shows a table for defining log streams. The 'File' section shows options for file-based logging. The 'Cache' section is currently collapsed. The bottom of the dialog has 'Ok' and 'Cancel' buttons.

4. Under the General Settings section, configure the following parameters:

- From the Mode list, select the mode of logging as stream or event.
- To specify a source IP address or the IP address used when exporting security logs, enter the IP address in the Source Address field.
- From the Format list, select the logging format as syslog, sd-syslog, or binary.
- To limit the rate per second at which data plane logs are generated, enter the rate value in the Rate-Cap field.
- To disable security logging for a device, select the **Disable Logging** check box.
- To use Coordinated Universal Time (UTC) for security log timestamps, select the **UTC-Timestamp** check box.
- To limit the rate per second at which logs are streamed, enter the event rate in the Event-rate field.

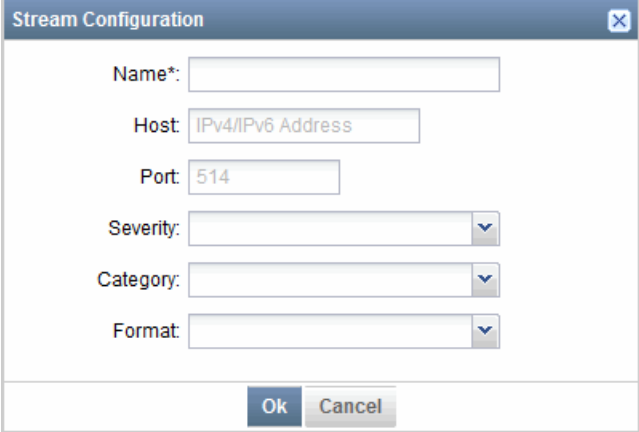
5. Under the Stream section, configure the following parameters:

To create a new stream configuration:

- Click the plus sign (+).

The Stream Configuration page appears, as shown in [Figure 273 on page 536](#).

**Figure 273: Security Logging-Stream Configuration Page**

A screenshot of the 'Stream Configuration' dialog box. The dialog has a title bar with a close button. Inside, there are several input fields: 'Name\*' (empty), 'Host' (with placeholder text 'IPv4/IPv6 Address'), 'Port' (with value '514'), 'Severity' (a dropdown menu), 'Category' (a dropdown menu), and 'Format' (a dropdown menu). At the bottom, there are 'Ok' and 'Cancel' buttons.

Stream Configuration

Name\*:

Host:

Port:

Severity:

Category:

Format:

Ok Cancel

- In the Stream Name field, enter the name of the new stream configuration.
- In the Host field, enter the IPv4 or IPv6 address.
- In the Port field, enter the port number.
- In the Severity list, select one of the following available required severity types:
  - Emergency
  - Alert
  - Critical
  - Error
  - Warning

- Notice
  - Info
  - Debug
- In the Category list, select the type of category as all or content-security.
  - In the Format list, select the type of format as syslog, sd-syslog, welf, or binary.
  - To create a new stream, click **Ok**.

You can modify or delete the existing streams. To modify or edit a stream, select the stream and click the pencil icon. To delete a stream, select the stream and click the minus sign (-).

6. Expand the File section and configure the following parameters:
  - In the File Name field, enter a filename for the log data file.
  - In the File Path field, enter the path where the log file is saved.
  - In the File Size field, enter the maximum size of the log file in megabytes.
  - In the Max No. Of files field, enter the maximum number of log files to create for each session.
7. Expand the Cache section, and configure the following parameters:
  - In the Limit field, enter the maximum number of log entries to store in the cache memory. The default value is 10,000 entries.
8. To restrict the device from logging certain configurations, you can create different exclude configurations.

To create a new exclude configuration:

- Under the Exclude section, click the plus sign (+).

The Exclude Configuration page appears, as shown in [Figure 274 on page 538](#).

**Figure 274: Security Logging-Exclude Configuration Page**

- In the Name field, enter the name of a new exclude configuration.
- Under the Destination section, in the IP Address field, enter the destination IP address in IPv4 or IPv6 address format. The audit log does not include security alarms from the specified destination IP address.

In the Port field, enter the destination IP address port.

- Under the Source section, in the IP Address field, enter the source IP address in IPv4 or IPv6 address format. The audit log does not include security alarms from the specified source IP address.

In the Port field, enter the source IP address port.

- Under the Other Filters section, configure the following parameters:
  - In the Event Id field, enter the event ID of the security event. The audit log does not include security alarms for this event ID.
  - To restrict the logging of failed events, select the **Failure** check box.
  - In the Interface field, enter the name of the interface. The audit log does not include security alarms from the specified interface.
  - In the Policy Name field, enter the policy name.

- In the Process field, specify the name of the process that is generating the events.
  - In the Protocol field, enter the protocol name.
  - To restrict the logging of successful events, select the **Success** check box.
  - In the User Name field, enter the name of the authenticated user. All security events that are enabled by this user are not generated in the audit log.
  - To create a new exclude configuration, click **Ok**.
9. To create a new security log, click **Ok**.



**NOTE:** Security logging is not supported for the logical systems devices.

---

**Related  
Documentation**

- [Modifying a Syslog on page 560](#)



# Creating and Managing Static Routes

- [Creating a Static Route for a Device on page 541](#)
- [Managing Static Routes on page 545](#)

## Creating a Static Route for a Device

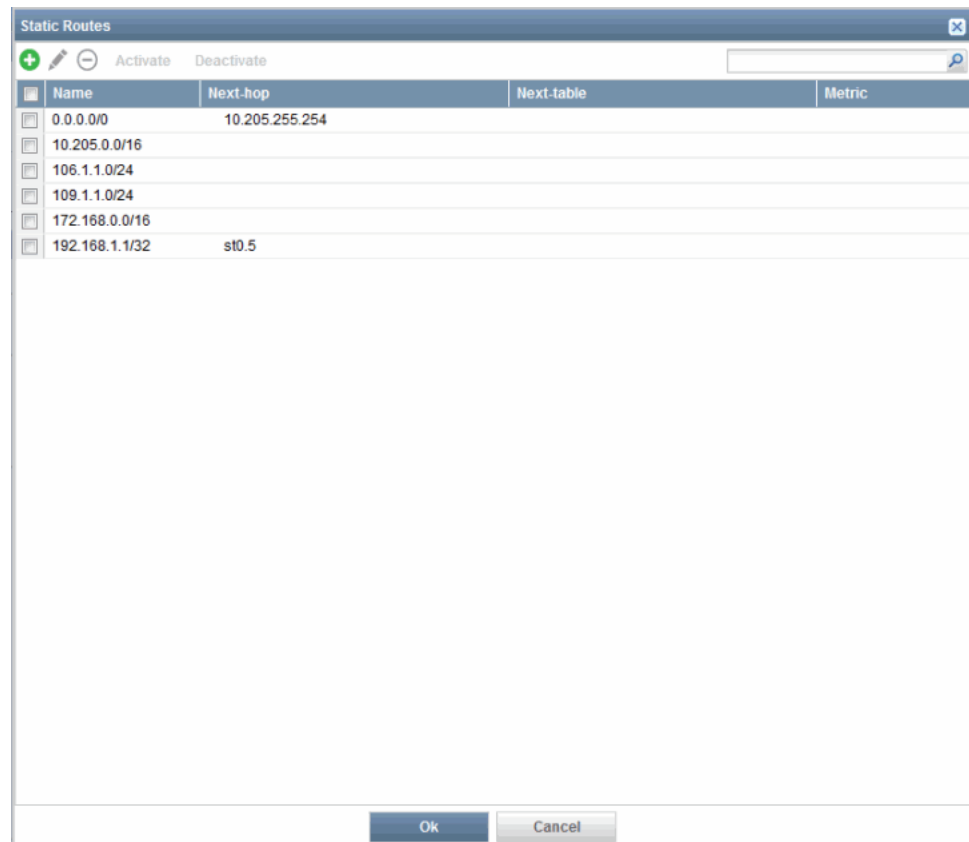
---

To create a new static route:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Routing section, click **Static Routes**.

The Static Routes main page appears, showing the existing static routes, as shown in [Figure 275 on page 542](#).

Figure 275: Device Configuration-Static Routes Main Page



4. To create a new static route, click the plus sign (+).

The Create Static Route page appears, as shown in [Figure 276 on page 543](#).

Figure 276: Static Routes—Create Static Route Page

The screenshot shows the 'Create Static Route' dialog box. The 'Basic Information' section has the 'IPv4' radio button selected. The 'Prefix' field contains the text 'IPv4 Address'. The 'Suffix' field is empty. The 'Next Hop' section has a list box with one entry, 'IP Address/Interface', and plus/minus icons to the left. Below this are sections for 'Qualified Next Hop', 'Next Table', and 'Advanced Options', each with a minus icon to its left. At the bottom right are 'Ok' and 'Cancel' buttons.

5. In the Prefix field, enter the IPv4 address.
6. In the Suffix field, enter the route suffix.
7. Under the Next Hop section, configure the IP address and interface for a next hop to a destination.
  - To configure the next hop, click the plus sign (+).  
The Next Hop page appears.
  - In the IP Address field, enter the IPv4 address.
  - From the Interface list, select the required interface.
  - To configure the next hop, click **Ok**.  
You can configure multiple next hops for a single prefix.
8. Under the Qualified Next Hop section, configure the following parameters:
  - To configure the qualified next hop, click the plus sign (+).  
The Qualified Next Hop page appears.
  - In the IP Address field, enter the IPv4 address.
  - From the Interface list, select the required interface.

- In the Metric field, enter the metric of the qualified next hop.
- In the Preference field, enter the preference of the qualified next hop.
- To configure the qualified next hop, click **Ok**.

Qualified next hops allow you to associate one or more properties with a particular next-hop address.

9. Under the Next Table section, from the Next Table list, select a routing table as a next hop to another table.
10. Under the Advanced Options section, configure the following parameters:
  - In the Preference field, enter the route preference.
  - In the Metric field, enter the metric associated with the forwarding next hop.
  - To drop the packets to the destination without sending back an ICMP message, select the **Discard** check box.
  - Select any one of the following options after Resolve Choices:
    - resolve—To allow resolution of indirectly connected next hops.
    - no-resolve—To not allow resolution of indirectly connected next hops.
    - None—No action.
  - Select any one of the following options after Readvertise Choices:
    - readvertise—To mark the route as eligible to be readvertised.
    - no-readvertise—To not mark the route as eligible to be readvertised.
    - None—No action.
  - Select any one of the following options after Retain Choices:
    - retain—To always keep the route in the forwarding table.
    - no-retain—To not keep the route in the forwarding table.
    - None—No action.
  - Select any one of the following options after Install Choices:
    - install—To add a route into the forwarding table.
    - no-install—To not to add a route to the forwarding table.
    - None—No action.
11. To create a new static route for a device, click **Ok**.

**Related  
Documentation**

- [Managing Static Routes on page 545](#)

## Managing Static Routes

---

You can modify, delete, activate, and deactivate the static routes that are listed on the Static Routes main page.

To manage a static route, right-click the static route or select the required options from the toolbar.

You can perform the following management tasks on the Static Routes page:

- [Modifying a Static Route on page 545](#)
- [Deleting a Static Route on page 546](#)
- [Deactivating a Static Route on page 547](#)
- [Activating a Static Route on page 547](#)

### Modifying a Static Route

To modify a static route:

1. Select **Security Director > Devices > Device Management**.

The Device Management page appears.

2. Right-click a device and select **Device Configuration > Modify Configuration**.

The View/Edit Configuration page appears.

3. Under the Security section, click **Static Routes**.

The Static Routes main page appears.

4. Select the static route that you want to modify, and click the pencil icon or right-click and select **Edit**.

The Modify Static Route page appears, as shown in [Figure 277 on page 546](#).

Figure 277: Modify Static Route Page

**Modify Static Route -- 11.11.11.1/32**

**Basic Information**

☒ IPv4 ☐ IPv6

Prefix: 11.11.11.1

Suffix\*: 32

**Next Hop**

IP Address/Interface
st0.6

**Qualified Next Hop**

IP Address/Interface	Preference	Metric
----------------------	------------	--------

**Next Table**

Next Table: Type or select

**Advanced Options**

Preference:

Metric:

Discard: ☐

Resolve Choices: ☐ resolve ☐ no-resolve ☒ None

Retain Choices: ☐ retain ☐ no-retain ☒ None

Install Choices: ☐ install ☐ no-install ☒ None

Ok Cancel

5. On the Modify Static Route page, you can modify the required values. However, you cannot modify the basic information such as IP address, prefix, and suffix.
6. To modify the selected static route, click **Ok**.

## Deleting a Static Route

To delete a static route:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Routing section, click **Static Routes**.  
The Static Routes main page appears.
4. Select the static route that you want to delete, and click the minus sign (-) or right-click the static route and select **Delete**.

A confirmation message appears before the static route is deleted. You can select multiple static routes for deletion.

5. To confirm the deletion, click **Ok**.

## Deactivating a Static Route

To deactivate a static route:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Routing section, click **Static Routes**.  
The Static Routes main page appears.
4. Select the static route that you want to deactivate, right-click it, and select **Deactivate**.  
The deactivated static route is greyed out and not available for any selection.

## Activating a Static Route

To activate a deactivated static route:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Routing, click **Static Routes**.  
The Static Routes main page appears.
4. Select the deactivated static route that you want to activate, right-click it and select **Activate**.  
The static route is activated and available for any selection.

**Related Documentation** • [Creating a Static Route for a Device on page 541](#)



# Creating and Managing Routing Instances

- [Creating a Routing Instance for a Device on page 549](#)
- [Managing Routing Instances on page 552](#)

## Creating a Routing Instance for a Device

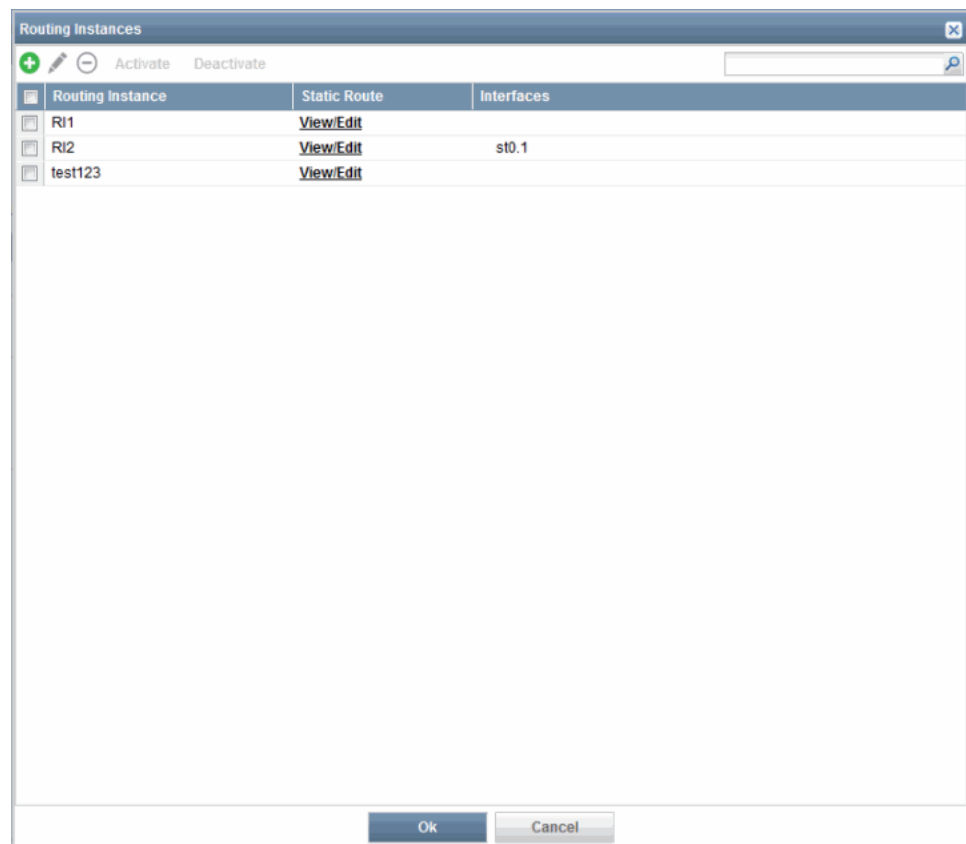
---

To create a new routing instance for a device:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Routing section, click **Routing Instances**.

The Routing Instances main page appears showing the existing screens, as shown in [Figure 278 on page 550](#).

Figure 278: Device Configuration-Routing Instances Main Page



4. To create a new routing instance, click the plus sign (+).

The Create Routing Instance page appears, as shown in [Figure 279 on page 551](#).

Figure 279: Create Routing Instance Page

**Create Routing Instance**

**General Settings**

Name\*:

Description:

**Interfaces**

Available		Selected
Filter <input type="text"/>	Select: Page   None	Select: Page   None
ge-0/0/0.0	+ -	
ge-0/0/1.0		
ge-0/0/2.0		

Ok Cancel

5. In the Name field, enter the name of the routing instance.
6. In the Description field, enter a description for the routing instance.
7. Under the Interfaces section, select the required interfaces from the Available column and copy them to the Selected column.
8. Click **Ok**.

A new routing instance is created.

You can view, edit, or create static routes for each routing instance from the Routing Instance page.

To create a static route for a routing instance:

1. On the Routing Instances page, click **View/Edit** for the required routing instance.  
The Static Routes page for that routing instance appears.
2. To create a new static route for that routing instance, click the plus sign (+).

The Create Static Route page appears. For more information on creating a new static route, see [“Creating a Static Route for a Device” on page 541](#).

You can also manage the static routes created for a routing instance. For more information on managing a static route, see [“Managing Static Routes” on page 545](#).

3. To come back to the Routing Instances page from the Static Routes page, click **Back**.



**NOTE:** You must first save the newly created routing instance before adding a static route to the routing instance.

**Related  
Documentation**

- [Managing Routing Instances on page 552](#)

---

## Managing Routing Instances

You can modify, delete, activate, and deactivate the routing instances that are listed on the Routing Instances main page.

To manage a routing instance, right-click the routing instance or select the required options from the toolbar.

You can perform the following management tasks on the Routing Instances.

- [Modifying a Routing Instance on page 552](#)
- [Deleting a Routing Instance on page 553](#)
- [Deactivating a Routing Instance on page 554](#)
- [Activating a Routing Instance on page 554](#)

### Modifying a Routing Instance

To modify a routing instance:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Routing, click **Routing Instances**.  
The Routing Instances main page appears.
4. Select the routing instance that you want to modify, and click the pencil icon or right-click and select **Edit**.

The Modify Routing Instance page appears, as shown in [Figure 280 on page 553](#).

Figure 280: Modify Routing Instance Page

**Modify Routing Instance -- RI-33**

**General Settings**

Name\*: RI-33

Description:

**Interfaces**

Available	Selected
ge-0/0/0.0	
ge-0/0/1.0	
ge-0/0/10.0	
ge-0/0/11.0	
ge-0/0/12.0	
ge-0/0/13.0	
ge-0/0/14.0	
ge-0/0/15.0	
ge-0/0/2.0	
ge-0/0/3.0	
ge-0/0/4.0	
ge-0/0/5.0	

Ok Cancel

5. On the Modify Routing Instance page, you can modify the required values.
6. To modify the selected routing instance, click **Ok**.

## Deleting a Routing Instance

To delete a routing instance:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Routing, click **Routing Instances**.  
The Routing Instances main page appears.
4. Select the routing instance that you want to delete, and click the minus sign (-) or right-click the instance and select **Delete**.  
A confirmation message appears before the routing instance is deleted.
5. To confirm the deletion, click **Ok**.

## Deactivating a Routing Instance

To deactivate a routing instance:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Routing, click **Static Routes**.  
The Static Routes main page appears.
4. Select the static route that you want to deactivate, right-click it, and select **Deactivate**.  
The deactivated routing instance is greyed out and not available for any selection.

## Activating a Routing Instance

To activate a deactivated routing instance:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under Routing, click **Routing Instances**.  
The Routing Instances main page appears.
4. Select the deactivated routing instance that you want to activate, right-click it, and select **Activate**.  
The routing instance is activated and available for any selection.

**Related Documentation**

- [Creating a Routing Instance for a Device on page 549](#)

# Managing Physical Interfaces and Syslog

- [Managing Physical Interfaces on page 555](#)
- [Modifying a Syslog on page 560](#)

## Managing Physical Interfaces

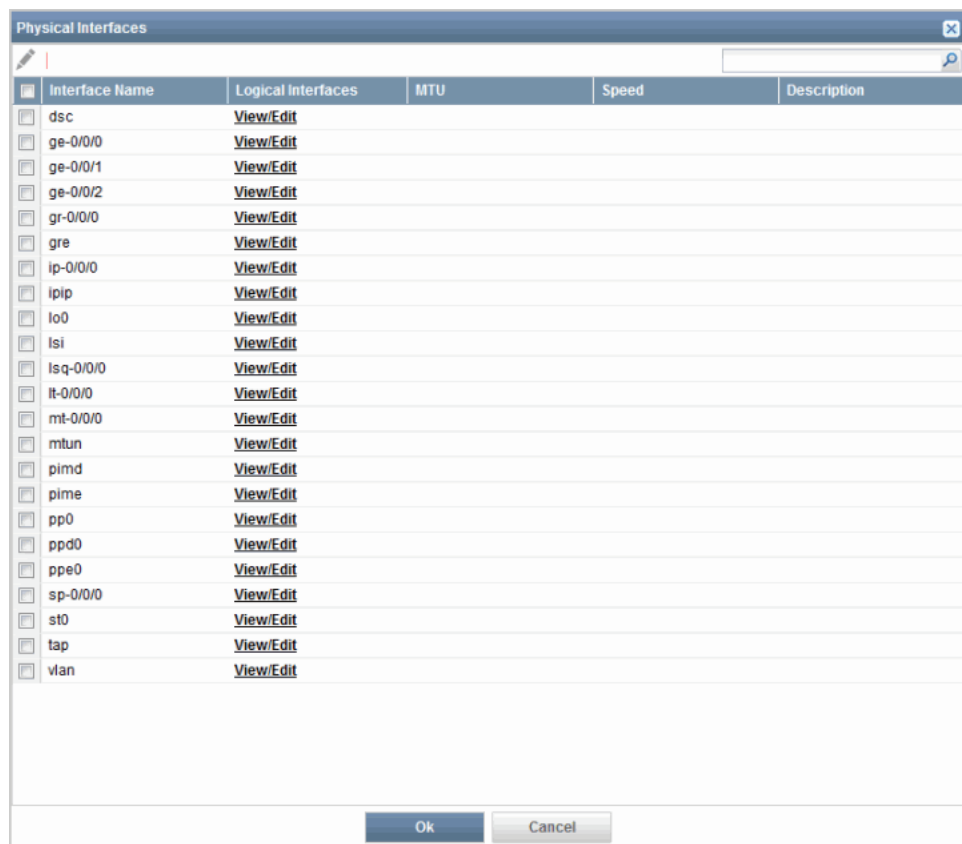
---

To modify the selected physical interface:

1. Select **Security Director > Devices > Device Management**.  
The Device Management page appears.
2. Right-click a device and select **Device Configuration > Modify Configuration**.  
The View/Edit Configuration page appears.
3. Under the Routing section, click **Physical Interfaces**.

The Physical Interfaces main page appears, showing the existing physical interfaces, as shown in [Figure 281 on page 556](#).

Figure 281: Device Configuration-Physical Interfaces Main Page



4. Select the required interface and click the pencil icon, or right-click it and select **Edit**.  
The Modify Physical Interface page appears, as shown in [Figure 282 on page 557](#).

Figure 282: Modify Physical Interface Page

Modify Physical Interface -- ge-0/0/1

**Basic Information**

Description:

MTU:  bytes

Speed:

**Advanced Options**

Enable vlan-Tagging: ☐

Ok Cancel

5. In the Description field, enter a description of the interface.
6. In the MTU field, enter the maximum transmit packet size in bytes.
7. From the Speed list, select the required link speed.
8. To enable the 802.1q VLAN tagging support option, select the **Enable-vlan-Tagging** check box.
9. To complete the modification, click **Ok**.

You can view, edit, or create a logical interface for each of the interfaces listed on the Physical Interfaces page.

To view, edit, or create a logical interface:

1. On the Physical Interfaces page, in the Logical Interfaces column, click **View/Edit** for the required interface.  
  
The Logical Interfaces page for that particular interface appears, listing the existing logical interfaces.
2. To create a new logical interface, click the plus sign (+).  
  
The Create Logical Interface page appears, as shown in [Figure 283 on page 558](#).

Figure 283: Create Logical Interface Page

The screenshot shows a window titled "Create Logical Interface of fxp2". It contains three expandable sections:

- Basic Information:** Includes fields for "Name\*", "Description", and "Vlan Id".
- IPv4 Address:** Contains a table with columns "IP Address", "Primary", and "Preferred". A plus sign icon is used to add a new address.
- IPv6 Address:** Contains a similar table with columns "IP Address", "Primary", and "Preferred", also with a plus sign icon.

At the bottom of the window are "Ok" and "Cancel" buttons.

3. Under the Basic Information section, configure the following parameters:
  - In the Name field, enter the new logical interface unit name.
  - In the Description field, enter a description.
  - In the Vlan Id field, enter the virtual LAN identifier value for 802.1q VLAN tags.
4. To configure the IPv4 address, under the IPv4 Address section, click the plus sign (+).  
 Configure the following parameters:
  - In the Prefix field, enter the IPv4 address as **IP prefix**.
  - In the Suffix field, enter the IP suffix value.
  - To configure this address to be the primary address of the protocol on the interface, select the **Primary** check box.

If the logical unit has more than one address, the primary address is used by default as the source address when packet transfer originates from the interface and the destination address does not indicate the subnet.

  - To configure this address to be the preferred address on the interface, select the **Preferred** check box.

If you configure more than one address on the same subnet, the preferred source address is chosen by default as the source address when you initiate frame transfers to destinations on the subnet.

- To complete the configuration, click **Ok**.
5. To configure the IPv6 address, under the IPv6 Address section, click the plus sign (+).  
Configure the following parameters:
    - In the Prefix field, enter the IPv6 address as **IP prefix**.
    - In the Suffix field, enter the IP suffix value.
    - To use this address as a primary address, select the **Primary** check box.
    - To use this address as a preferred address, select the **Preferred** check box.
    - To complete the configuration, click **Ok**.
  6. To complete the configuration of a new logical interface, click **Ok**.

To go back to the Physical Interfaces page from the Logical Interfaces page, click **Back**. You can edit, delete, activate, or deactivate any logical interfaces that are listed in the Logical Interfaces page.

**Related  
Documentation**

- [Creating a Static Route for a Device on page 541](#)
- [Managing Static Routes on page 545](#)
- [Creating a Routing Instance for a Device on page 549](#)
- [Managing Routing Instances on page 552](#)

## Modifying a Syslog

To modify a syslog:

1. Under the Security section, click **Syslog**.

The Modify Syslog page appears, as shown in [Figure 284 on page 560](#).

**Figure 284: Device Configuration-Modify Syslog Page**

**Modify Syslog**

**General Settings**

Time-format: ☐

Source Address:

Log-Rotate-Frequency:

Allow-duplicates: ☐

**Host**

Name	Contents	Match	Advanced Options
messages	any - any;		
default-log-messages	any - info;		

**File**

Name	Contents	Match	Advanced Options
messages	any - any;		
default-log-messages	any - info;	{requested 'commit' operation}   (copying configuration to juniper.save)   (commit complete)   {AdminStatus}   {FRU power}   {FRU removal}   {FRU insertion}   {link UP}   {transitioned}   {transferred}   {transfer-file}   {license add}   {license delete}   {package -X update}   {package -X delete}   GRES	Structured Data : true

Ok Cancel

2. In the General Settings section, configure the following parameters:
  - To include the additional information in the system log time stamp, select the **Time-format** check box.
  - In the Source Address field, specify the source address for log messages.
  - In the Log-Rotate-Frequency field, specify the interval for checking log file size and archiving messages.
  - To allow the repeated messages in the system log output files, select the **Allow-duplicates** check box.
3. You can send system logging information to one or more destinations. To send a security log to a remote server:

Under the Host section, configure the following parameters:

- To create a new host, click the plus sign (+).

The Host Configuration page appears, as shown in [Figure 285 on page 561](#).

**Figure 285: Modify Syslog-Host Configuration Page**

The screenshot shows the 'Host Configuration' dialog box. It includes a 'Name\*' field with a dropdown menu, a 'Match' text area, a 'Contents' section with a table for Facility and Severity, and an 'Advanced Options' section with checkboxes for 'Allow duplicates', 'Explicit priority', and 'Facility override', and a 'Log prefix' text field. The 'Ok' and 'Cancel' buttons are at the bottom.

- From the Host Name list, select the host name to notify.
- Under the Contents section, to configure the logging of system messages to the system console:
  - Click the plus signs (+), and the Contents page appears.
  - To specify the class of messages to log, from the Facility list, select the message class.
  - From the Severity list, select the message severity. Messages with severities of the specified level and higher are logged.
  - To configure the Contents section, click **Ok**.
- To allow the repeated messages in the system log output files, select the **Allow-duplicates** check box.
- To include the priority and facility in messages, select the **Explicit priority** check box.
- To select an alternate facility to substitute for the default facilities, from the Facility override list, select the alternate facility.
- In the Log prefix field, specify a text string to include in each message directed to a remote destination.

- In the Match field, specify a text string that must appear in a message for the message to be logged to a destination.
  - In the Port field, enter the port number.
  - In the Source Address field, specify the source address for log messages.
  - To write system log messages to the log file in structured-data format, select the **Structured data** check box.
  - To create a new host configuration, click **Ok**.
4. To send a security log to a file:

Under the File section, configure the following parameters:

- To create a new file to log the system messages, click the plus sign (+).

The File Configuration page appears, as shown in [Figure 286 on page 562](#).

**Figure 286: Modify Syslog-File Configuration Page**

The screenshot shows the 'File Configuration' dialog box. It has a title bar with 'File Configuration' and a close button. The main area contains the following elements:

- Name\*:** A text input field.
- Match:** A large text area for specifying a text string.
- Contents:** A section with a collapse/expand arrow. It contains a toolbar with a plus sign, a pencil, and a minus sign. Below the toolbar is a table with two columns: 'Facility' and 'Severity'.
- Advanced Options:** A section with a collapse/expand arrow. It contains two checkboxes: 'Explicit priority' and 'Structured data'.
- Buttons:** 'Ok' and 'Cancel' buttons at the bottom right.

- In the File Name field, enter the name of file to log the data.
- Under the Content section, configure the following parameters:
  - Click the plus signs (+), and the Contents page appears.
  - To specify the class of messages to log, from the Facility list, select the message class.
  - From the Severity list, select the message severity. Messages with severities of the specified level and higher are logged.
  - To configure the Contents section, click **Ok**.
- To include the priority and facility in messages, select the **Explicit priority** check box.

- In the Match field, specify a text string that must appear in a message for the message to be logged to a destination.
  - To write system log messages to the log file in structured-data format, select the **Structured data** check box.
  - To create a new file configuration, click **Ok**.
5. To configure the logging of system messages to user terminals:
- Under the User section, configure the following parameters:
- To configure a new user, click the plus sign (+).

The User Configuration page appears, as shown in [Figure 287 on page 563](#).

**Figure 287: Modify Syslog-User Configuration Page**

The screenshot shows the 'User Configuration' dialog box. It includes a 'Name\*' field, a 'Match' text area, and a 'Contents' section. The 'Contents' section contains a table with two columns: 'Facility' and 'Severity'. Above the table are icons for adding (+), editing (pencil), and deleting (-). Below the table is an 'Allow duplicates' checkbox. At the bottom of the dialog are 'Ok' and 'Cancel' buttons.

- In the User Name field, enter the name of the user to notify.
  - Under the Content section, configure the following parameters:
    - Click the plus signs (+), and the Contents page appears.
    - To specify the class of messages to log, from the Facility list, select the message class.
    - From the Severity list, select the message severity. Messages with severities of the specified level and higher are logged.
    - To configure the Contents section, click **Ok**.
  - To allow the repeated messages in the system log output files, select the **Allow-duplicates** check box.
  - In the Match field, specify a text string that must appear in a message for the message to be logged to a destination.
  - To create a new user, click **Ok**.
6. To configure the system to send syslog, click **Ok**.

**Related Documentation** • [Creating Security Logs on page 535](#)

## CHAPTER 48

# Updating Security Director Devices

- [Security Director Devices Workspace Overview on page 565](#)
- [Updating Devices with Pending Services on page 567](#)
- [Importing Firewall, NAT, and IPS Policies from a Device to Security Director on page 573](#)
- [NSM Migration on page 580](#)
- [Managing Consolidated Configurations on page 586](#)
- [Managing Commit Confirm on page 587](#)

### Security Director Devices Workspace Overview

The Security Director Devices workspace is used to update all security-specific configurations on devices. The Security Director Devices page lists only SRX Series devices. The Devices workspace is used by the Junos Space Network Management Platform to manage the network devices running Junos OS software. In addition, Junos Space Network Management Platform can record the presence of non-Juniper devices, that is, unmanaged devices in the network, thereby providing better visibility into the network and simplifying debugging and problem isolation.

[Table 45 on page 565](#) shows the different columns supported on the Security Director Devices page.

**Table 45: Security Director Devices Workspace Columns**

Column Name	Description
Name	Name of the device.
OS Version	Junos OS version running on the device.
Platform	Platform of the device. For example, SRX Series, VSRX.
Last Updated	Last configuration pushed from Security Director to the device.
IP Address	IP address of the device.
Connection Status	Connection status of the device. The status shows either UP or Down.

Table 45: Security Director Devices Workspace Columns (*continued*)

Column Name	Description
Configuration Status	<p>Configuration status of the device. The following are the different configuration states for a device:</p> <ul style="list-style-type: none"> <li>• Synchronizing—During the device update, the status is shown as Synchronizing.</li> <li>• Sync Failed—The synchronization operation failed.</li> <li>• In Sync—The synchronization operation has completed successfully; Security Director and the device are synchronized.</li> </ul>
Schema Version	Schema version of the device.
Management Status	<p>The following are the different management states that can be shown for a device:</p> <ul style="list-style-type: none"> <li>• Unmanaged—The device is discovered but not used by any Security Director policies.</li> <li>• SD Changed—A policy is assigned to the device and the configuration is published.</li> <li>• In Sync—The published policies are updated or pushed to the device successfully.</li> <li>• Device Changed—Out-of-band changes were made to a device in a security configuration managed by Security Director.</li> </ul>
Consolidated Configuration Status	<p>Collection of pending configurations created for one or more devices by using the Junos Space Network Application Platform or Security Director.</p> <p>The following different candidate configuration states are shown at different configuration levels:</p> <ul style="list-style-type: none"> <li>• Does Not Exist—After upgrading to Security Director Release 13.3, the old Security Director related CLIs and Candidate Configuration status are removed. The Candidate Configuration is shown as Does Not Exist.</li> <li>• Create—After publishing the firewall policy and when you update the configuration to the Network Application Platform, a job is created and the candidate configuration status is changed to Create.</li> <li>• Approve—Approving a candidate configuration enables it to be deployed. Unapproved candidate configurations cannot be deployed.</li> <li>• Reject—Rejecting a candidate configuration prevents it from being deployed. Both approved and unapproved candidate configurations can be rejected.</li> </ul>
Assigned Services	List of all assigned services: firewall, NAT, IPS, and VPN. When a device is assigned to any firewall policy including NAT, IPS and VPN, the policy name is shown in this column.
Pending Services	List of the policy names that are assigned and published. Versioning information is included for firewall and NAT policies.
Installed Services	List of the policy names that are published and updated to the device (this includes policy names for firewall, NAT, IPS, and VPN). Versioning information is included for firewall and NAT policies.
Domain	Domain of the user.

**Related Documentation**

- [Updating Devices with Pending Services on page 567](#)

## Updating Devices with Pending Services

To update a device with pending services:

1. Select **Security Director > Security Director Devices**.

The Security Director Devices page appears, as shown in [Figure 288 on page 567](#).

**Figure 288: Security Director Devices Page**

Name	ID	Platform	Last Update	Actions	Connection	Configuration Status	Scheduling	Management	Consistent Config	Assigned S.	Pending Ser.	Installed by
HA178Node-178 (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
10.205.50.213	12.1345-D10	SRX3400H	10.205.50.213	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist	Test NAT			
Node-178 (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
IPS-LSYS1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
NAT-LSYS1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
FW-Group1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist	Test NAT			
SRX-5600-2	12.1345-D10	SRX3400	10.205.61.41	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist	SRX-5600-2, 4			
Firewall-LSYS1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	SD Changed	Does Not Exist	999	999 id		
KeyDevice1(SRX-5600-2)	12.1345-D10	SRX3400	10.205.61.41	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
IPSec-LSYS1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
scale-10.205.61.33	12.1R1.9	SRX5600	10.205.61.33	Up	In Sync	12.1R1.9	Unmanaged	Does Not Exist	to do it			
NAT1(Node-178) (Cluster)	12.1345-D10	SRX3400	10.205.50.178	Up	In Sync	12.1345-D10	Unmanaged	Does Not Exist				
rev-211	12.1345-D15.2	SRX1400	10.205.50.211	Up	Unknown	12.1345-D15.2	Unmanaged	Does Not Exist				

2. Select the check box next to the device on which you want to update the pending services.
3. Click **Update**.

The Update page appears, as shown in [Figure 289 on page 567](#).

**Figure 289: Update Window**

**Preview Configuration**

**Select service types**

☐ Firewall-Policy  
☐ IPS Policy  
☐ VPN  
☐ NAT

OK Cancel

4. Select the type of service you want to update on the device in the Select Service Types pane. Once you select the type of service, the selected service is saved for your username and every time you log-in, by default, this service will be selected to update. You can retain the same service or select any other services.
5. Select the **Schedule at a later time** check box if you want to schedule the update at a later date and time.
6. Click **Update**.

## Updating Configuration in Network Application Platform

You can update the pending services to a device through Network Application Platform. When you finish modifying a device configuration, you can review and deploy the configuration by using the Review/Deploy Configuration page on Network Application Platform. You can review and deploy configurations created using the Schema-based Configuration Editor or Configuration Guides. You can review these configurations in a device-centric view, approve or reject appropriate configuration changes, and deploy them to one or more devices in a single commit operation. If there are any non Security Director related changes in the device, an administrator can review those configurations also and update the devices.

You can send Security Director changes to a Staged Configuration state in the Network Application Platform. To push the Security Director changes to Staged Configuration, right-click a device on the Security Director Devices and select **Update Configuration in Platform**. Once you push Security Director changes to staged configuration, the following tasks are triggered in Network Application Platform:

- Job is created.
- Change Request is created with respect to the current staged configuration.

After successfully updating the configuration in the Platform, the Change Requests of Security Director are available as part of Staged Configuration for a device in the Network Application Platform. Subsequent update to Staged Configuration pushes multiple Change Requests from Security Director incrementally.

The update to Staged Configuration on a cluster publishes the Change Requests to all its members. The change requests generated for the Staged Configuration of the current primary node is published to the other nonactive members of the cluster. You can deploy Staged Configuration on any cluster member from the Network Application Platform. This also addresses failovers before Staged Configuration is deployed. In the event of a failover, the Change Requests of Security Director are also available in the Staged Configuration of a new primary node.

When the staging configuration with the change requests of Security Director are deployed to the associated devices, the following state changes occur on the Security Director Devices page:

- Security Director marks the pending services whose configuration is part of the Staged Configuration as Installed.
- The Last Updated column for the device is updated.
- The Management Status column is changed to In Sync if all the service types are updated from the Staged Configuration.
- When the Staged Configuration of a cluster member is deployed, the Network Application Platform continues to maintain the Staged Configuration for other members of a cluster. If the Staged Configuration of other members is deployed again, the configuration might fail because of a conflicting change already present in the device. Therefore, on successful deployment of Staged Configuration on any member of a

cluster, Security Director removes the Security Director specific Change Requests from the Staged Configuration of other members.

If you make any changes to a device with out of band changes on security configuration managed by Security Director, the Management Status for that device is shown as Device Changed. You can check the status of the device in the Security Director Devices workspace by right-clicking the device and select **View Device Change**. To make the device status back to In-Sync, you must right click the device and select **Update**.

In the Select service types, you must select only services that are changed, and update the device. Do not select all the services when the CLI changes are related only to a particular service. Once you update from Security Director, the device status must be changed to In-Sync.



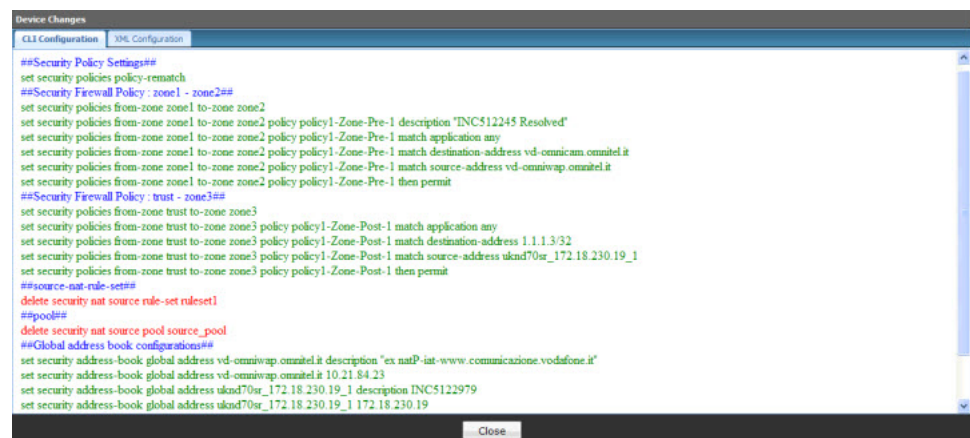
**NOTE:** If you make changes with NAT and firewall policies through the device CLI, and while updating the device you must select both firewall policy and NAT policy in the Select service types window. If you select either firewall policy or NAT policy alone for update, the device status remains Device Changed and will not be changed to In-Sync after the update.

To view the description entered for the device:

1. In the Manage Security Devices page, right-click the device for which policies are published, and select **Preview Configuration**.
2. The Preview Configuration window appears. Select the service type and click **OK**.

The publish window appears showing the descriptions for the policy rules and objects in the CLI to be pushed to the device, as shown in [Figure 290 on page 569](#).

**Figure 290: Device Changes Page Showing Device Comments**





**NOTE:** Descriptions entered for the address or service or NAT pool objects used in the firewall or NAT policies, and descriptions for NAT or firewall policy rules, are also pushed to the device. This feature is supported for devices running Junos OS Release 12.1 and later.



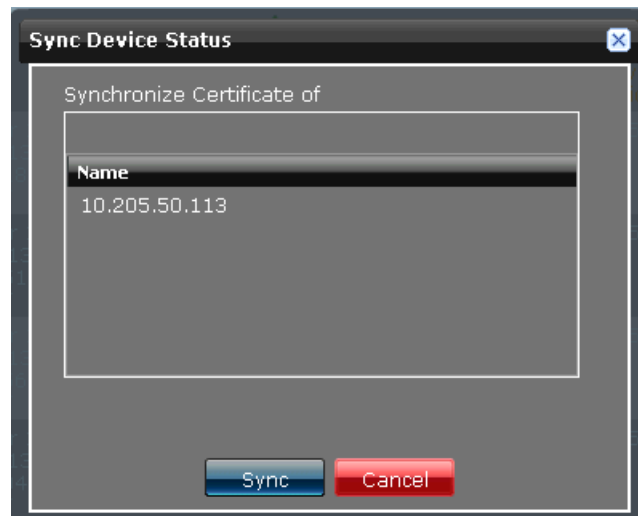
**NOTE:** A warning message appears when the management status for any device is changed to Device Changed.

To refresh the certificate for any device:

1. In the Update Device page, select the device for which you want to refresh the certificate. Right-click and select **Refresh certificate list** option.

You can select one or more devices to refresh the certificate. The Sync Device Status page appears, as shown in [Figure 291 on page 570](#).

**Figure 291: Sync Device Status Page**



2. Select the device(s) for certificate synchronization and click **Sync**.
3. A job ID is created. You can click the job ID to get the status of the certificate synchronization.



**NOTE:** The certificate synchronization is not applicable for logical systems.

Security Director allows you to rerun updates on failed devices. The Job Management framework gives you the option of retrying a job on all or a subset of the main objects, such as devices. You can retry a job more than once. The failed objects list reflects the jobs you choose to retry. You can retry only on the update devices jobs and not on any other jobs. You can retry a failed update job only if you have Update Device permission

under Security Director Devices section of RBAC. Also, you must trigger a new update in case there are issues in reaching the device while updating a service.

For example, Job 1 fails on devices A, B, C, and D, and it succeeds on devices E, F, G, and H. Job 2 retries Job 1. For Job 2, you can select devices A, B, C, and D to be retried.

If you choose only to retry devices A and, device A might succeed while device B fails again. Job 3 retries Job 2. For Job 3, you can choose to retry device B. Job 4 retries Job 1. For Job 4, you can choose to retry all the failed devices: A, B, C, and D.

For more detailed information about retrying failed updates, consult the following links:

- For the online help content on the device, click **Security Director > Jobs > Job Management** help.
- For the document about Junos Space on web, see the *Junos Space Network Application Platform User Guide*.

All the assigned services of firewall, NAT, IPS, and VPN are listed in the Assigned Services column. When a device is assigned to any Firewall policy (this includes for NAT, IPS and VPN), the policy name is shown in this column. The All Device Policy of firewall is not shown as an assigned service, because this service, by nature, is applicable to all the devices.

All the installed services of firewall, NAT, IPS, and VPN that are currently updated on the device are listed in the Installed Services column. When any service is published and updated to the device (this includes for firewall, NAT, IPS and VPN), the policy name is shown in Installed Services column. Versioning information is added for the services listed under the Pending Services and Installed Services columns. The versioning information is available only for firewall and NAT policies.

Search options are available for the Assigned Services, Pending Services, and Installed Services columns, and for the type of services. The following search criteria are applicable for the search option that is available on the Security Director Devices page:

- Searching with an OR combination is not supported.
- Searching with compound negate is not supported.
- Compound search queries with AND and negate are supported.

Use the following keywords to search for a particular service:

- For an assigned service name, use the *assignedServices* keyword.

For example, use *assignedServices:storesrx* to list all the devices that are assigned to the *storesrx* firewall policy.

Use *-assignedServices:storesrx* to list all the devices that are not assigned to the *storesrx* firewall policy.

- For an assigned service type, use the *assignedServiceTypes* keyword. This finds all devices having minimum one firewall policy use. This keyword applies to firewall, NAT, IPS, and VPN policies.

For example, use *-assignedServiceTypes:FWPolicy* to list all the devices that are not assigned to any firewall policy.

Use *-assignedServiceTypes:FWPolicy AND assignedServiceTypes:NAT* to list all the devices that are not assigned to any firewall policy but that are assigned to any NAT policy.

- For pending service name, use the *pendingServices* keyword.

For example, use *pendingServices:(storesrx)* to find all devices where *storesrx* is published and the update is pending.

Use *-pendingServices:(storesrx)* To find all the devices that do not have policies with name having text *storesrx* published.

- For pending service type, use the *pendingServiceTypes* keyword. This keyword applies to firewall, NAT, IPS, and VPN services.

For example, use *pendingServiceTypes:FWPolicy* to list all the devices that have any firewall policy as a pending service.

The keyword *pendingServiceTypes:FWPolicy AND pendingServiceTypes:NAT* to list all the devices that have firewall and NAT policies as pending services.

- For installed service name, use the *installedServices* keyword.

For example, use *installedServices:storesrx* to list all the devices with firewall policy *storesrx* updated on it.

Use *-installedServices:storesrx* to find all devices where *storesrx* is not updated.

- For installed service type, use the *installedServiceTypes* keyword. This keyword applies to firewall, NAT, IPS, and VPN policies.

You can export all the columns on the Security Director Devices page to a CSV file. To export the columns to the CSV file, click **Export to CSV** option from the Actions drop-down list. You cannot select a device or devices and export only those devices to a CSV file. However, you can apply filters to the list of devices and export the filtered data to a CSV file.

You can also export the job details of publish or preview and update jobs to a CSV file. The messages columns will also be captured in the exported CSV file. A filter option is available for all the columns in the Job Management workspace.

Security Director does not allow deletion of all the firewall policies in the device. The Update job fails if all the firewall policies are deleted in the device. You cannot enable or disable this parameter in the device and Security Director does not allow deletion of all firewall policies from the device.

Update fails under the following scenarios:

- Update empty firewall rules to the device
- Delete all the existing rules from the device

The warning messages are displayed during the update and preview workflow if all the firewall policies are removed from the device. For the preview workflow *Device Update*

*job will fail because the Update will remove all Firewall Policies from the device. Security Director does not support deleting all Firewall Policies. warning message is displayed. For the update workflow Device Update failed because all Firewall Policies would have been deleted on device update. Security Director does not allow deleting all Firewall policies. warning message is displayed.*

You can import VPNs from this workspace. To import VPNs:

1. On the Security Director Devices page, select the device to import its VPN configurations. Right-click, or from Actions select **Import VPNs**
2. To know more about importing VPNs, see [“Importing an Existing VPN Environment of SRX Series Devices” on page 273](#).

If the device hostname is changed and you see a discrepancy with the Network Application Platform and Security Director, you can resync with the Network Application Platform. Right-click the device, and select **Resynchronize with Platform**. The Sync Device Status page appears to confirm the sync action. To sync the changes, click **Sync**.

**Related  
Documentation**

- [Security Director Devices Workspace Overview on page 565](#)
- [Importing Firewall, NAT, and IPS Policies from a Device to Security Director on page 573](#)
- [NSM Migration on page 580](#)
- [Managing Consolidated Configurations on page 586](#)

---

## Importing Firewall, NAT, and IPS Policies from a Device to Security Director

Security Director enables you to import firewall, NAT, and IPS policies from a device. All objects supported by Security Director are imported during the policy import process. Rules that contain objects not supported by Security Director are imported with the disabled rule state. You can import IPS policies along with the firewall policies, however, you cannot import IPS policies alone. For IPS, only the active policies are imported. After import, Security Director creates a policy with IPS mode set to Advanced. If you are using predefined device templates, any policy rules with an IPS mode as Basic is migrated as Advanced mode in the imported policy.

You can select a list of policies to be imported to Security Director. Security Director displays a summary of the rules and objects used in the policies to be imported. After you verify the information and resolve any conflicts, the policies are imported from the device to Security Director. Every time a new import is initiated, Security Director creates a new policy, even if a policy with that name was imported previously. In such a case, Security Director names the new policy based on the results of the duplicate name resolution.

**NOTE:**

- Imported policies are created without any device assigned to them. To use these policies, you must associate a device with the policy.
- If you import any disabled rule, Security Director configures them as inactive state. If any node in the disabled rule is in the inactive rule, such node is not imported by Security Director. In the next device update, such nodes are deleted.
- Prior to importing IPS and Application Firewall configurations into Security Director, the IPS or Application Firewall Signatures must be downloaded on to the Junos Space.

To import a firewall, NAT, or IPS policy:

1. Select **Security Director > Security Director Devices**.

The Manage Security Devices page appears, as shown in [Figure 292 on page 574](#).

**Figure 292: Manage Security Devices Page**

Security Director Devices > Update Device										
0 Item Selected										
Name	OS Version	Platform	Last Update...	IP Address	Connection...	Configuration Status	Schema Ver...	Management...	Consolidated Config...	Assigned S...
NAT(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
10.205.50.213	12.1X45-D10	SRX3400		10.205.50.213	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	Test NAT
Node-178 (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
IPS-LSYS1(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
NAT-LSYS1(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
FW-Group1(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	Test NAT
SRX5600-2	12.1X45-D10	SRX3400		10.205.61.41	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	SRX-0500 -2_4 SRX-0500 -2_4
Firewall-LSYS1(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	BD Changed	Does Not Exist	000 000 v2 Test NAT
TestDevice1(SRX-5600-2)	12.1X45-D10	SRX3400		10.205.61.41	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
VPN-LSYS1(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
scale-10.205.61.33	12.1R1.9	SRX5600		10.205.61.33	Up	In Sync	12.1R1.9	Unmanaged	Does Not Exist	to do
NAT(Node-178) (Cluster)	12.1X45-D10	SRX3400		10.205.50.178	Up	In Sync	12.1X45-D10	Unmanaged	Does Not Exist	
en-211	12.1X45-D15.2	SRX1600		10.205.50.211	Up	Unknown	12.1X45-D15.2	Unmanaged	Does Not Exist	

2. Select the device for which you want to import the policy. Right-click on the device, and then click **Import**.

The Service Import Summary page appears, as shown in [Figure 293 on page 575](#).

Figure 293: Service Import Summary Page

Policy	Policy Type	Rules	Errors	Summary
<input checked="" type="checkbox"/> NAT Policies				
<input checked="" type="checkbox"/> ind-h26-41	Device	9	0	
<input checked="" type="checkbox"/> Preval Policies				
<input checked="" type="checkbox"/> ind-h26-41	Device	3	0	

This page provides the following information:

- Policy name and type (firewall, NAT, or IPS)
- Number of rules with errors or warnings
- Summary showing:
  - Number of addresses, services, or NAT pool objects
  - Rules with unsupported objects

3. Select the policy that you want to import, and click **Next**.

If conflicts are present, the Object Conflict Resolution page appears, as shown in [Figure 294 on page 575](#).

Figure 294: Object Conflict Resolution Page

Name	Value	Imported Value	Action	New Name
HOST_v4	192.168.1.10	192.168.1.1	Rename Object	HOST_v4_1
HOST_v6	2FOE:3E00:0000:0022:F376:F37ab3F	2001:db8:b5a3:8d3:1339:8a2e:370:7348	Rename Object	HOST_v6_1
ADDR-GROUP-v4	[HOST_v4, HOST_v6]	[HOST_v4, 10.159.2.0/25, DNS]	Rename Object	ADDR-GRO_1
IPS-Host	4.3.2.1	1.1.1.1	Rename Object	IPS-Host_1
IPS-Address-Group	[IPS-Host, HOST_v4]	[IPS-Host, IPS-Host-1, IPS-Network, IPS-Range]	Rename Object	IPS-Address_1
TCP-2967	1. one_Tp, Protocol: TCP, Source Port: 1-65535, Destination Port: 2967, Inactiv...	1. TCP-2967, Protocol: TCP, Source Port: 1-65535, Destination Port: 2967, Inactiv...	Rename Object	TCP-2967_1
ICMP_App	1. 6, ICMP Code: 1, ICMP Type: 23 2. 1, ICMP Code: 0, ICMP Type: 29	1. icmp, ICMP Code: 0, ICMP Type: 11 2. icmp, ICMP Code: 0, ICMP Type: 4, 1...	Rename Object	ICMP_App_1
CUSTOM-APP-GROUP-1	ICMP_App TCP-2967	ICMP_Death_Unreachable TCP-2967 TCP-443 UDP-1434	Rename Object	CUSTOM-AP_1
IPS-Service-6	1. one_Tp, ALG: Rtp, Protocol: TCP, Source Port: 32, Destination Port: 21, Inactiv...	1. IPS-Service-6, ICMP Code: 124, ICMP Type: 123	Rename Object	IPS-Service_1
IPS-Service-Group	IPS-Service-6	IPS-Service-1 IPS-Service-2 IPS-Service-3 IPS-Service-4 IPS-Service-5 IPS-Service...	Rename Object	IPS-Service_1
Severity-Info	Name: Severity-Info, Type: signature, Severity: info, Definition type: Custom, Ra...	Name: Severity-Info_1, Type: signature, Severity: Info, Definition type: Custom...	Rename Object	Severity-In_1
static-coast-ug	Name: static-coast-ug, Type: static, Numbers: HTTP-HTTPS-ICMPS-HTTPSCOT	Name: static-coast-ug_1, Type: static, Numbers: Severity-Info	Rename Object	static-coas_1
dynamic-false-positives	Name: dynamic-false-positives, Type: dynamic, Filters: true, any, Critical, Major	Name: dynamic-false-positives_1, Type: dynamic, Filters: Frequently, occasionally...	Rename Object	dynamic-fal_1

An object conflict occurs when the name of the object to be imported matches an existing object, but the definition of the object does not match. You can use the available Tooltip view to see more information for Value, Imported Value, and Action

columns. To see the tooltip for an object, mouse over its value, imported value, or action columns.

Conflicting objects can be address, service, NAT pool objects, IPS Signature, static group, or dynamic group. The inactive rules on the device are disabled in the imported policy and the unused objects, such as unused IPS signatures are removed during the IPS import. Security Director imports attacks that are used in the policy. The unused attacks such as address or service, are deleted by the Security Director in the next policy publish. You can take the following actions for the conflicting objects from the action column:

- Keep the existing object, and ignore the new object.
- Overwrite the existing object with the new object.
- Accept the proposed name, or enter a new name.

Once the initial naming conflict has been resolved, the object conflict resolution checks for further conflicts with the new name and definition until conflict is completely resolved.

You can select more than one conflicting object to perform the action. Select one or more conflicting object, right-click and select required action, as shown in [Figure 295 on page 576](#).

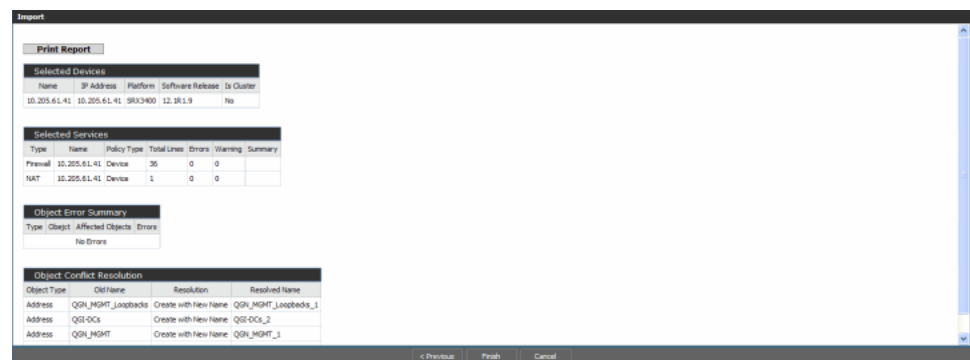
**Figure 295: Same Action Applied to Two Conflicting Objects**



The same action is applied to all the selected conflicting objects.

- After all object conflicts are resolved, click **Next**. A summary of the import process appears, along with the conflict resolution page, as shown in [Figure 296 on page 576](#).

**Figure 296: Policy Import Status Page**



To print the summary report, click **Print Report** at the beginning of the page.



**NOTE:** If Security Director finds further conflicts, the Object Conflict Resolution page is refreshed to display the new conflicts.

- Click **Finish** to initiate the import process. After the import is complete, a comprehensive report for each policy imported is provided, as shown in [Figure 297 on page 577](#).

**Figure 297: Firewall Policy Final Import Status Page**

Task	Status	Details
Reading import Files	In Progress	Started at Oct 3, 2012 4:02:54 PM UTC+05:30
Reading import Files	Success	Finished at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Addresses	In Progress	Started at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Addresses	Success	Finished at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Services	In Progress	Started at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Services	Success	Finished at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Nat Prefixes	In Progress	Started at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Nat Prefixes	Success	Finished at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Nat Pools	In Progress	Started at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Nat Pools	Success	Finished at Oct 3, 2012 4:02:54 PM UTC+05:30
Importing Nat Policy	In Progress	Importing 10.205.119.23 Started at Oct 3, 2012 4:02:55 PM UTC+05:30
Importing Nat Policy	Success	Imported as 10.205.119.23 Finished at Oct 3, 2012 4:02:55 PM UTC+05:30
Summary		<a href="#">Summary Report</a>

Page 1 of 1 | Displaying 1 - 13 of 13

Close

- Click **Summary Report** to view the import summary, as shown in [Figure 296 on page 576](#).
- Go to the Firewall Policy workspace to view the imported policies. At this point Security Director will have created a device policy without associating any devices with it. At this point you can continue to import policy objects for all other devices as many number of times as required. All imported device policies will show up as device policies.

Go to the NAT Policy workspace to view the imported policies. All imported device policies show up as group policies in Security Director. At this point you can continue to import policy objects for all other devices. You can perform all normal NAT policy functions on these imported policies.

When you import a device, all the new objects are created in the current domain. If there is an object by name A1 in the global domain and you are importing a device in D1 domain, and the device also has A1 object, the A1 object from the global domain is used if there are no conflicts. The behavior is same when you import a device in the global domain. However, if there is a conflict, Security Director does not allow the overwrite of A1 object in the global domain. In such cases, you have the following options as a resolution:

- Create a new object in D1 domain

- Reuse existing object from global domain

If you are importing a device in the global domain, overwrite existing object is allowed. The overwrite existing object option is allowed only for the conflicting objects from the current domain where the device import operation is triggered.

If the A1 object is present in both global and D1 domains, and in the device as well, the following points explain the usage of such objects:

- The A1 object, which is the final object created in Security Director, is checked for equality with the object from the device. If they are equal, Security Director object is reused. For example, if the object A1 is created in the global after the another object A1 is created in D1 domain, the object from the global domain is reused. Otherwise, the object from D1 domain is reused.
- If the final created object in Security Director is not equal to the object from the device, the object which is created first in Security Director is checked for equality with the object from the device. If they are equal, Security Director object is reused.
- If the objects A1 from both global and D1 domains are not equal to the object from the device, there is a conflict resolution. During the conflict resolution, the object from the current domain, in which the import device operation is triggered, is taken for a resolution with the object from the device. All the tree options such as creating a new object, overwriting an existing object, and ignore.

The behavior is same during the NSM migration as well.

In Security Director, firewall rules are not disabled if IPS policy, policy-based VPN, or AppFW is configured during the device import.

Security Director imports IPS on or off state in firewall rule. By default, after the import, firewall policy mode for IPS will be in *not configured* state. If the device configuration has an active IPS policy, the mode is set to Advanced after the import. If the mode is not set to Advanced, such active policies are not selected by Security Director.

Firewall rules configured with application signature that include predefined, and custom signature are imported. If the imported firewall rules have signatures not available in Security Director, such firewall rules will be in disabled state after the import. The reason for the disabled state is given in the Description field along with the information on the missing application signature.

If a device firewall policy is imported to Security Director, it automatically creates rule groups based on the zone pair. If a zone pair contains more than 300 rules, based on the auto group feature, the rule groups are broken into multiple rule groups each containing 200 rules. Group names for such groups are decided based on the following logic:

The configuration that is imported from the configuration group is imported to Security Director and pushed to the device as an effective configuration. At the time of publish, a warning message is displayed.



**NOTE:** If the VPN was created outside of Security Director (CLI and so on), the VPN is not imported. Firewall rules can point to VPNs that were created outside of Security Director (CLI and so on), and can be used in any Security Director rule with a tunnel action.

The following are application firewall import criteria in firewall rule:

- Multiple firewall rules can share the same application firewall rule set.
- Application firewall rule set name is automatically generated during policy publish. You cannot customize the application firewall rule set names.
- Application firewall rule set can contain both blacklisted and whitelisted applications.
- <ZONE-NAME>-Intra (in case *from zone* and *to zone* are same)
- <SRX ZONE NAME>-to-<DST ZONE NAME>
- <SRX ZONE NAME>-to-<DST ZONE NAME>-X

X is a counter that allows multiple groups when a policy count exceeds 200.

For Security Director managed devices, if you make any changes to a device, which is outside of changes managed by Security Director, the Management Status for that device is shown as Device Changed. Right-click the device and select **View Device Change** to see the changes for the device. To import the changes alone, right-click the device and select **Import Device Changes**. This imports the changes alone from the device and the same workflow of import occurs for OCR.



---

**NOTE:**

- In Junos OS Release 12.1 and later releases, comments are imported during the policy import process.
  - You can also import similar logical systems policies to other devices.
  - The following rules are not supported by NAT. After the import, Security Director will disable these rules.
    - Persistent NAT for source-nat interface
    - Persistent NAT for source-nat pool
    - IPv6 to IPv4 translation with the destination address 2001:470:b:227::1/96
    - Matching Protocol in source and destination rule (supported only for Junos OS Release 11.4 and later releases)
    - Matching address object for source and destination address in source, or destination, or static NAT rules
  - Security Director does not assign devices to the imported policies. You must explicitly assign devices once the import is complete.
  - From Security Director Release 12.2 and later, Security Director categorizes the zone-based rules in firewall policies, after importing from a device, into logical rule groups based on zone pairs. For the rules between different from or to zones, the rules are grouped under rule group name *Interzone: ZoneA to ZoneB*, and if from or to zones are same, rules are grouped under rule group name *Intrazone: Zonename*.

If the number of rules within the rule group exceeds 200, Security Director splits the rule groups and appends *-n* with each rule group name, where *n* is a digit greater than or equal to zero (last group name can have upto 299 rules).
  - Security Director supports import of scheduler objects.
  - The same OCR is generated when you import UTM policies. If there is a global configuration, device profile is created and you must manually assign devices to that profile. If not manually assigned, those device profiles will be deleted.
  - The import is disabled in the Global domain for a device in the child domain.
- 

**Related Documentation**

- [NSM Migration on page 580](#)

---

## NSM Migration

---

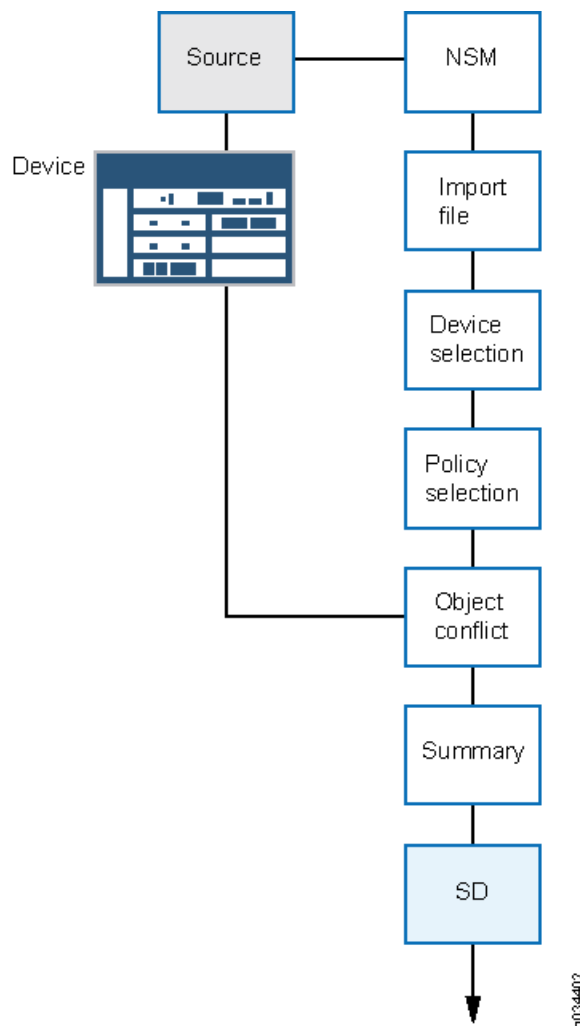
You can migrate firewall and NAT policies from Network and Security Manager (NSM) for a set of devices. All objects supported by Security Director (addresses, services,

address group, service group) can be imported with the policy, with the exception of polymorphic objects. Rules referring to these objects are disabled after the migration.

At any time, only a single migration from the NSM workflow can be triggered on Security Director. Migrating policies from NSM requires the NSM database to be exported in .xdiff format. You must copy this file to your local machine and provide the path of the .xdiff file to migrate policies from NSM to Security Director.

Figure 298 on page 581 shows the device import workflow.

**Figure 298: High-Level Device Import Workflow**



You can migrate NSM database from the NSM Release 2010.3 to 2012.2 into Security Director.

The following features are supported during the NSM migration:

- Firewall policies with global rules (including support for the global address book)
- NAT policies with support for the global address book

- Nested address group support (Junos OS Release 11.2 and later releases)
- Negate address support in firewall rules
- Service offload support in firewall rules
- Source address or source port option in Static NAT
- Source port option in Source NAT

To import policies from NSM:

1. Select **Security Director > Security Director Devices > NSM Migration**.

The Upload NSM xdiff file to start migration window appears, as shown in [Figure 299 on page 582](#).

**Figure 299: NSM Xdiff File Upload Page**



**NOTE:** The supported NSM versions for the database import are 2010.3 through 2012.2.

2. Browse to the path where the .xdiff file is stored, and select the appropriate .xdiff file, generated from NSM. The .xdiff file is imported to the Security Director server.

The Devices page appears showing the name of the available devices, the Junos OS version of each device, and the platform.

**Figure 300: NSM Migration Devices Page**

Name	IP Address	OS Version	Platform	Domain
<input checked="" type="checkbox"/> SRX-119.8	10.205.119.8	11.2	srx240b	global
<input checked="" type="checkbox"/> nsm-srx220-2	10.205.90.213	11.2	srx220h	global

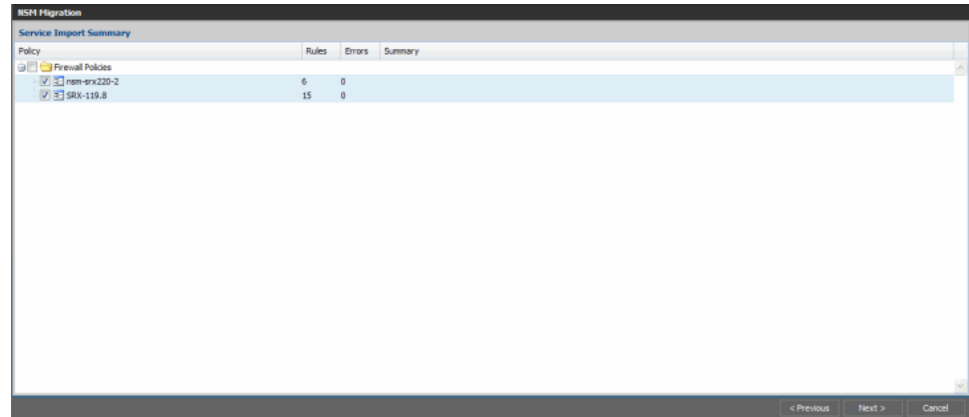


**NOTE:** NSM to Security Director migration is not supported for ScreenOS devices.

3. Select the devices for which you want to import the policies, and select **Next**.

The Service Import Summary page appears, as shown in [Figure 301 on page 583](#).

**Figure 301: Service Import Summary Page**



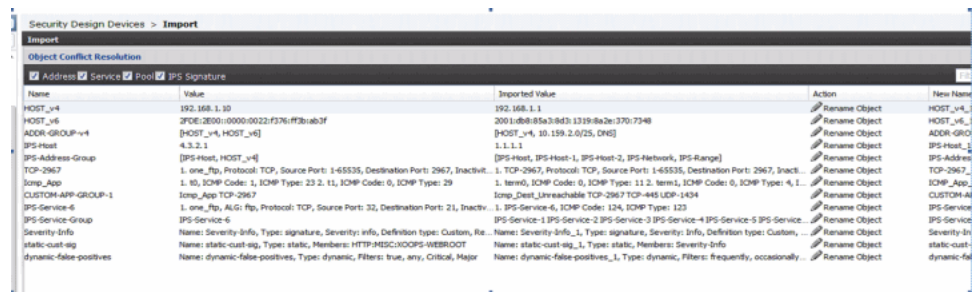
This page provides the following information:

- Policy name and type (firewall or NAT)
- Number of rules with errors or warnings
- Summary showing:
  - Number of addresses, services, or NAT pool objects
  - Rules with unsupported objects

4. Select the policy that you want to import, and click **Next**.

If conflicts are present, Object Conflict Resolution page appears, as shown in [Figure 302 on page 583](#).

**Figure 302: NSM-Object Conflict Resolution Page**



An object conflict occurs when the name of the object to be imported matches an existing object, but the definition of the object does not match.

Conflicting objects can be address, service, or NAT pool objects. You can take the following actions for the conflicting objects from the action column:

- Keep the existing object, and ignore the new object.
- Overwrite the existing object with the new object.

- Accept the proposed name, or enter a new name.

Once the initial naming conflict has been resolved, the object conflict resolution checks for further conflicts with the new name and definition until resolution is complete.

5. After all object conflicts are resolved, click **Next**. A summary of the import process appears, along with the conflict resolution page, as shown in [Figure 303 on page 584](#).

**Figure 303: NSM Migration Status Page**

NSM Migration

Print Report

Managed Devices

Name	IP Address	Platform	Software Release	Domain name	Is Cluster
SRX-119.8	10.205.119.8	srx240b	11.2	global	No
nsn-srx220-2	10.205.50.213	srx220h	11.2	global	No

Managed Services

Type	Name	Policy Type	Total Lines	Errors	Warning	Summary
Firewall	nsn-srx220-2	Group	6	0	0	
Firewall	SRX-119.8	Group	15	0	0	

Object Error Summary

Type	Object	Affected Objects	Errors
No Errors			

Object Conflict Resolution

Object Type	Old Name	Resolution	Resolved Name
No Conflicts			

< Previous Finish Cancel

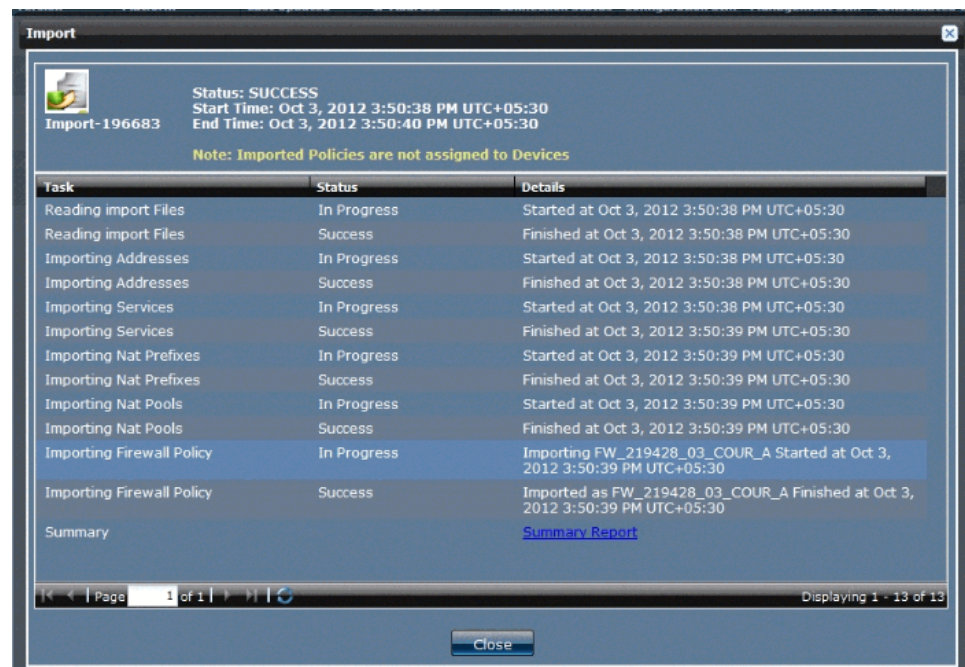
To print the summary report, click **Print Report** at the beginning of the page.



**NOTE:** If Security Director finds further conflicts, the Object Conflict Resolution page is refreshed to display the new conflicts.

6. Click **Finish** to initiate the import process. After the import is complete, a comprehensive report for each policy imported is provided, as shown in [Figure 304 on page 585](#).

Figure 304: NSM Migration Final Status Report Page



7. Click on **Summary Report** to view the import summary as shown in [Figure 303 on page 584](#)
8. Go to the Firewall Policy or NAT Policy workspace to view the imported policies. At this point Security Director will have created a group policy without associating any devices with it. At this point you can continue to import policy objects for all other devices. All imported device policies will show up as group policies in Security Director. You can perform all normal firewall, or NAT policy functions on these imported policies.

**NOTE:**

- If a group has more than 300 rules, Security Director automatically breaks the group into multiple rule groups each containing 200 rules. The only exception is that these groups are placed last in the list of groups. The size of the last group is calculated by the upper threshold of 300 rules and lower threshold of 100 rules.
- Security Director attaches \_DE to the device exception policies name. You cannot directly assign device exception policies to group policy. Assign devices to the device exception policies first, and then assign those devices to the group policies.
- Security Director supports import of scheduler objects from NSM.

**Related Documentation**

- [Importing Firewall, NAT, and IPS Policies from a Device to Security Director on page 573](#)

## Managing Consolidated Configurations

A consolidated configuration is a collection of pending configurations created for one or more devices by using Junos Space applications or the Junos Space Network Application Platform. Such configurations could be created using the Config Editor, Device Templates, or Security Director, for example. The main purpose of collecting them is to review them all in a device-centric view, and then potentially to deploy them to one or more devices in a single commit.

In Junos Space, different users can create change requests, configuration templates, and so forth for a particular device. A single reviewer can then view all of these configurations for multiple devices to decide which of them to deploy, and in which sequence. However, permissions for the Manage Consolidated Configurations task could be restricted to specific subtasks; for example, the person who generates a consolidated configuration might not have the permissions to approve the consolidated configuration for deployment.

A consolidated configuration that has been approved can be deployed immediately or scheduled for a later time. A consolidated configuration cannot be approved until it has been submitted for review.

- [Generating a Consolidated Configuration on page 586](#)

## Generating a Consolidated Configuration

The detailed documentation on the consolidated configuration can found at:

- For the online help content on the device, click **Security Director > Devices help**.
- For the document on web, see *Junos Space Network Application Platform User Guide*.

The consolidated configuration status shown in the platform can also be seen from Security Director. To view the consolidated configuration status from Security Director, click **Security Director Devices**. The status is shown in the Consolidated Config Status column, as shown in [Figure 305 on page 586](#).

**Figure 305: Consolidated Config Status from Security Director**

Security Director Devices										
Actions		0 Item Selected								
Name	Domain	OS Version	Platform	Last Updated	IP Address	Connection Status	Configuration Status	Schema Version	Management St...	Candidate Config Status
10.205.50.113	Global	11.4R10.4	SRX210H	10.205.50.113	10.205.50.113	Up	In Sync	11.4R10.4	Unmanaged	Does Not Exist
10.205.50.211	Global	12.1X48-D10.2	SRX1400	Apr 8, 2014 1:12:24 PM IST	10.205.50.211	Up	In Sync	12.1X48-D10.2	In Sync	Does Not Exist
10.205.51.41	Global	12.102140108_psh_121_x86_linux64-0-623052	SRX3400	10.205.51.41	10.205.51.41	Up	In Sync	12.1021.5 (Mismatch with device OS version)	SD Changed	Does Not Exist
keys1(10.205.51.41)	Global	12.102140108_psh_121_x86_linux64-0-623052	SRX3400	10.205.51.41	10.205.51.41	Up	In Sync	12.1021.5 (Mismatch with device OS version)	Unmanaged	Does Not Exist
keys2(10.205.51.41)	Global	12.102140108_psh_121_x86_linux64-0-623052	SRX3400	10.205.51.41	10.205.51.41	Up	In Sync	12.1021.5 (Mismatch with device OS version)	Unmanaged	Does Not Exist
keys3(10.205.51.41)	Global	12.102140108_psh_121_x86_linux64-0-623052	SRX3400	10.205.51.41	10.205.51.41	Up	In Sync	12.1021.5 (Mismatch with device OS version)	Unmanaged	Does Not Exist
Node-7576-Keys1(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
Node-7576-Keys2(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
Node-7576-Keys3(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
Node-7576-Keys4(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
Node-7576-Keys5(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
Node-7576-Keys6(10.205.50.211)	Global	12.1X48-D10.2	SRX1400	10.205.50.211	10.205.50.211	Up	In Sync	12.1X48-D10.2	Unmanaged	Does Not Exist
pmphilip-119.1	Global	12.1X48-D15	SRX050	Apr 8, 2014 2:47:39 PM IST	10.205.119.1	Up	In Sync	12.1X48-D15	In Sync	Does Not Exist
SRX-119	Global	10.4R2.7	SRX2400	10.205.119.9	10.205.119.9	Up	In Sync	12.1021.5 (Mismatch with device OS version)	Unmanaged	Does Not Exist

On Security Director Devices page, the Staged Configuration status of each device is shown in the Candidate Configuration column.

[Table 46 on page 587](#) shows different candidate configuration status at different configuration levels.

**Table 46: Different Status of Candidate Configuration**

CC Status	Description
Does Not Exist	After upgrading to Security Director Release 13.3, the old Security Director related CLIs and Candidate Configuration status are removed. The Candidate Configuration is shown as Does Not Exist.
Create	<p>After publishing the firewall policy, navigate to Security Director Devices page. Right-click the device and select <b>Update Configuration to Platform</b> option.</p> <p>Once the configuration is updated to Platform, job is created and the candidate configuration status is changed to Create.</p>
Approve	Approving a candidate configuration enables it to be deployed. Unapproved candidate configurations cannot be deployed.
Reject	Rejecting a candidate configuration prevents it from being deployed. Both approved and unapproved candidate configurations can be rejected.



**NOTE:**

- If the Security Director policy is not published, it will not appear in the consolidated configuration. To update a policy through consolidated configuration, the policy must be published in Security Director. There is no workflow available to publish Security Director policies within the Junos Space Network Application Platform.
- When devices with prepared or approved consolidated configurations are updated from Security Director, the consolidated configuration status for such devices is reverted to the generated state. An associated warning is displayed during the update workflow.

**Related Documentation**

- [Updating Devices with Pending Services on page 567](#)

## Managing Commit Confirm

The Network Application Platform supports the Junos OS confirmed-commit feature for all the commit operations made after a device is discovered. This feature is supported for the devices that support confirmed-commit NETCONF capability. By default, the commit confirm option is disabled.

To enable commit confirm option:

1. Select **Network Management Platform > Administration > Applications**.

The Application page appears.

2. On the Applications page, right-click **Network Management Platform** and select **Modify Applications Settings**
3. Under the Devices section, select the **Enable commit confirmed for configuration deployment** check box.

The commit confirm operation is now enabled.

The confirmed-commit remote procedure call (RPC) is followed by the commit RPC value to confirm the commit. Confirming the commit operation before the device update prevents many error conditions where Junos Space loses the connection to the device because of incorrect configuration edits. The default commit confirm timeout value for Security Director is 2 minutes, and the maximum value that you can configure is 300 minutes.

To configure the timeout value:

1. Select **Network Management Platform > Administration > Applications**.

The Application page appears.

2. On the Applications page, right-click **Security Director** and select **Modify Security Director Settings**.

Under the Update-Device section, you can configure the timeout value for Per device commit confirm timeout in minutes. There is a similar rollback option for IPS configuration failures.

The commit confirm addresses the concerns in the following error scenarios:

**The configuration is committed for a device; however, the connection to the device is lost because of mistakes in the configuration.**

The following behavior is observed after the commit confirm:

1. The device is locked by the Network Application Platform.
2. The configuration is pushed to the device.
3. If the connection to the device is lost, no further RPC is sent from the Network Application Platform to the device to confirm the configuration. The device waits for a commit-configuration RPC to arrive within a specified timeout period before committing the configuration.
4. The device automatically rolls back and unlocks, because no <commit-configuration> RPC is received. Auto rollback occurs after the timeout value configured by the Network Application Platform expires.
5. A job is created, and occurrences of all the auto rollbacks are recorded.

**The configuration is committed to a device. After the commit, the IPS policy is compiled. If the compilation fails, the update job is marked as FAILURE; however, the device commit is not reverted.**

This use case is valid if the Rollback commit on IPS compilation failure flag is enabled under Network Management Platform > Administration > Applications > Security Director > Update-Device.

The following behavior is observed after the commit confirm:

1. The device is locked by the Network Application Platform.
2. The configuration is pushed to the device.
3. The Network Application Platform sends commit-confirm RPC with a timeout value.
4. The IPS policy is compiled.
5. If the compilation fails, Network Application Platform sends an RPC to the device instructing it to roll back the configuration.

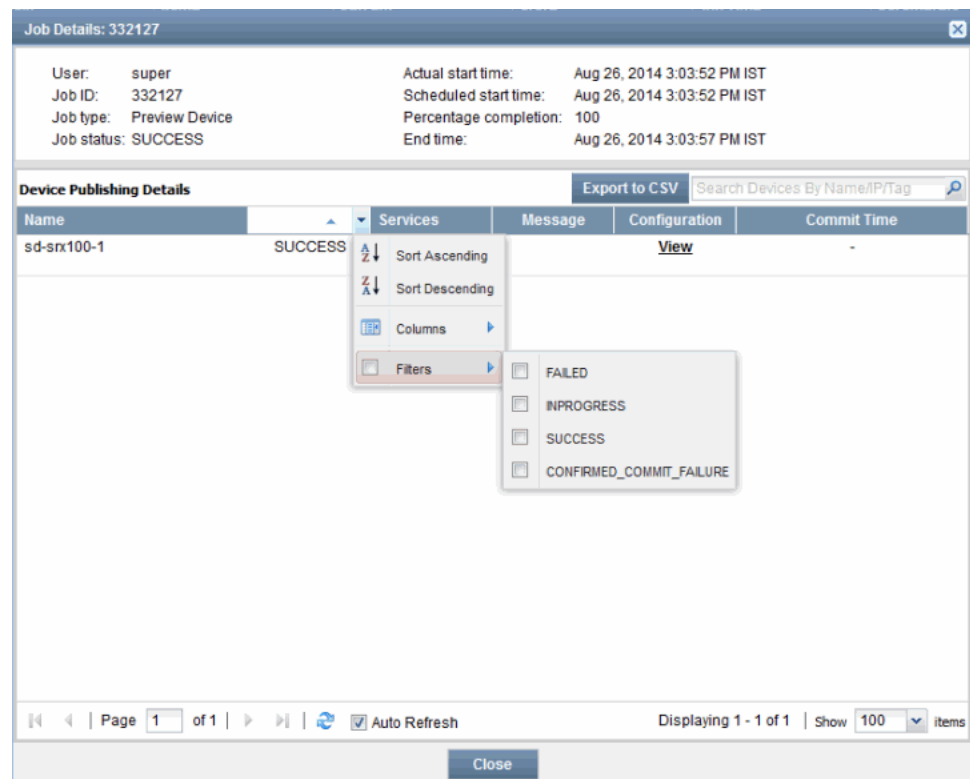
The update job is marked as FAILED with an appropriate message.

6. If the compilation is not completed within the timeout specified in step 3, you cannot conclude that the compilation is passed or failed.

The update job is marked as PASSED in Security Director, and device does not execute the rollback command.

To facilitate searching for devices for which a device update failed because of commit confirm, an additional CONFIRMED\_COMMIT\_FAILURE filter is provided in the Job Details window, as shown in [Figure 306 on page 590](#).

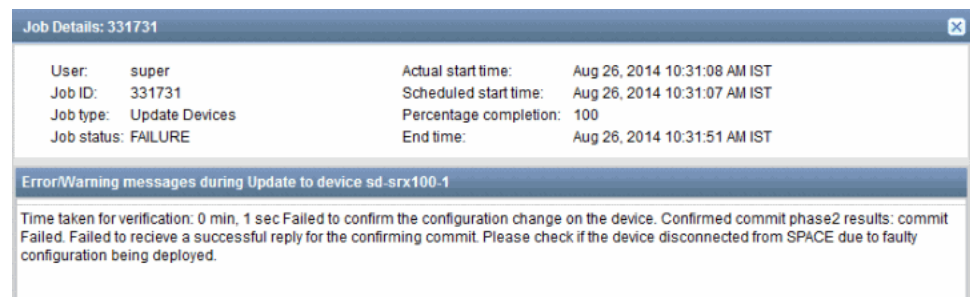
Figure 306: Job Details Window



The Commit Time field in the Job Details window displays the device confirmed commit timestamp.

If the commit confirm fails, the job status is updated as CONFIRMED\_COMMIT\_FAILURE, and the following error message is displayed, as shown in [Figure 307 on page 590](#).

Figure 307: Confirmed Commit Warning Message



#### Related Documentation

- [Updating Devices with Pending Services on page 567](#)

## PART 2

# Index

- [Index on page 593](#)



# Index

## Symbols

#, comments in configuration statements.....	xxxiii
( ), in syntax descriptions.....	xxxiii
< >, in syntax descriptions.....	xxxiii
[ ], in configuration statements.....	xxxiii
{ }, in configuration statements.....	xxxiii
(pipe), in syntax descriptions.....	xxxiii

## A

address and address groups overview.....	121
address groups	
creating.....	136
deleting.....	138
managing.....	137
modifying.....	137
addresses	
assign domain.....	135
cloning.....	128
creating.....	124
delete unused.....	134
deleting.....	128
duplicate objects.....	129
exporting.....	128
find usage.....	131
importing.....	129
managing.....	127
modifying.....	127
replace.....	132
unused.....	134
Anti-Spam profile	
creating.....	349
Anti-Spam Profile	
cloning.....	352
delete.....	351
delete unused.....	352
find usage.....	352
managing.....	351
modify.....	351
show unused.....	352
Anti-Virus profile	
creating.....	355

Anti-Virus Profile	
cloning.....	360
delete.....	360
delete unused.....	361
find usage.....	361
managing.....	359
modify.....	360
show unused.....	361
application groups	
deleting.....	119, 120
modifying.....	119
application signatures	
creating.....	230
managing.....	233
applications	
delete unused.....	117
deleting.....	113
duplicate objects.....	113
find usage.....	114
modifying.....	112
replace.....	115
unused.....	117

## B

braces, in configuration statements.....	xxxiii
brackets	
angle, in syntax descriptions.....	xxxiii
square, in configuration statements.....	xxxiii

## C

comments, in configuration statements.....	xxxiii
configurations	
consolidated.....	586
consolidated configurations	
generating.....	586
managing.....	586
Content Filtering Profile	
cloning.....	368
creating.....	363
delete.....	367
delete unused.....	368
find usage.....	368
managing.....	367
modify.....	367
show unused.....	368
conventions	
text and syntax.....	xxxii
curly braces, in configuration statements.....	xxxiii

Custom URL Category List		
cloning.....	392	
creating.....	389	
delete.....	391	
delete unused.....	392	
find usage.....	392	
managing.....	391	
modify.....	391	
show unused.....	392	
customer support.....	xxxiv	
contacting JTAC.....	xxxiv	
<b>D</b>		
dashboard		
overview.....	21	
Device Profile		
creating.....	395	
documentation		
comments on.....	xxxiii	
Dynamic signature group		
creating.....	486	
<b>E</b>		
extranet device		
cloning.....	289	
managing.....	288	
modifying.....	288	
Extranet Device		
deleting.....	288	
<b>F</b>		
Firewall policy		
adding rules.....	180	
Adding rules before or after.....	206	
address book.....	121	
assigning devices.....	218	
cloning.....	206	
cloning rules.....	216	
copying or pasting rules.....	217	
creating.....	159	
custom column.....	225, 226	
<i>See also</i> deleting		
<i>See also</i> exporting		
<i>See also</i> managing		
<i>See also</i> modifying		
deleting.....	205	
deleting devices.....	223	
deleting rules.....	215	
enabling or disabling rules.....	216	
expanding or collapsing rules.....	217	
exporting.....	207	
grouping rules.....	216	
inline object.....	176	
<i>See also</i> creating		
manage lock.....	174	
manage versioning.....	210	
modifying.....	202	
multiple group policy.....	155	
ordering rules.....	185	
overview.....	151	
priority and precedence.....	188	
promoting.....	207	
publishing.....	194	
versioning.....	208	
Firewall Policy		
comparing.....	203	
font conventions.....	xxxi	
<b>G</b>		
Global search.....	8	
<b>I</b>		
Indexing overview.....	7	
Ipolicy templates		
expanding or collapsing rules.....	491	
IPS policy		
Adding rule before or after.....	516	
adding rules.....	507	
cloning rules.....	514	
copying and pasting rules.....	515	
creating.....	494	
deleting rules.....	514	
enabling or disabling rules.....	514	
expanding or collapsing rules.....	515	
grouping rules.....	515	
manage lock.....	503	
ordering rules.....	504	
IPS Policy		
publishing.....	509	
IPS signature		
cloning.....	485	
creating.....	482	
deleting.....	485	
filtering.....	484	
modifying.....	485	
IPsec VPN		
deleting.....	285	
modifying.....	283	

- modifying endpoint settings.....284
  - overview.....257
  - publishing.....281
- IPsec VPNs
  - creating.....259
- M**
- manuals
  - comments on.....xxxiii
- N**
- NAT
  - NAT policy
    - publishing.....433
  - NAT pool
    - managing.....459
- NAT policy
  - assigning devices.....448
  - cloning.....438
  - creating.....409
  - cutting/copying and pasting rules.....446
  - deleting.....437
  - deleting devices.....448
  - deleting rules.....445
  - enabling or disabling rules.....445
  - expanding or collapsing rules.....446
  - exporting.....438
  - global address book.....406
  - grouping rules.....445
  - manage lock.....423
  - manage versioning.....440
  - modifying.....437
  - overview.....403
  - publishing.....433
  - versioning.....439
- NAT pool
  - duplicate objects.....460
  - find usage.....462
  - replace.....463
  - unused.....464
- NAT pools
  - delete unused.....465
- O**
- Object Builder overview.....103
- P**
- parentheses, in syntax descriptions.....xxxiii
- policy template
  - adding rules.....488
  - creating.....487
  - managing.....489
- policy templates
  - copying and pasting rules.....491, 492
  - grouping rules.....490
- S**
- scheduler
  - creating.....238
  - overview.....237
- Scheduler
  - deleting.....240
  - find usage.....241
  - managing.....240
  - modifying.....240
  - show unused.....241
- Security Director devices
  - importing policies.....574
  - updating.....567
- Security Director Overview.....3
- Security Intelligence
  - dynamic address group.....327, 328, 329
    - See also* creating
    - See also* delete
    - See also* managing
    - See also* modify
  - policy.....323, 324, 325
    - See also* creating
    - See also* delete
    - See also* managing
    - See also* modify
  - profiles.....317, 320, 321
    - See also* creating
    - See also* delete
    - See also* managing
    - See also* modify
- security policy profiles
  - creating.....244
  - managing.....248
  - overview.....243
- service and service groups overview.....107
- service groups
  - creating.....118
  - managing.....119
- services
  - creating.....108
  - managing.....112

Signature database	
downloading.....	473
installing.....	475
Static signature group	
creating.....	486
support, technical See technical support	
syntax conventions.....	xxxii

## T

technical support	
contacting JTAC.....	xxxiv

## U

URL Pattern	
creating.....	383
URL Patterns	
cloning.....	386
delete.....	386
delete unused.....	387
find usage.....	386
managing.....	385
modify.....	385
show unused.....	386
UTM Device Profile	
delete.....	399
UTM Device Profiles	
cloning.....	399
delete unused.....	400
managing.....	398
modify.....	399
show unused.....	399
UTM policy	
cloning.....	347
delete.....	347
delete unused.....	348
find usage.....	347
managing.....	346
modify.....	347
show unused.....	348

## V

VPN profiles	
creating.....	292
overview.....	291

## W

Web Filtering Profile	
cloning.....	380
creating.....	371

delete.....	380
delete unused.....	381
find usage.....	380
managing.....	379
modify.....	379
show unused.....	380