



Junos[®] Space

Security Director User Guide

Release

13.1



Published: 2013-05-23

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

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.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos Space Security Director: User Guide

13.1

Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

Revision History

May 2013—Junos Space Security Director User Guide, Release 13.1

The information in this document is current as of the date listed in the revision history.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. The Junos OS has no known time-related limitations through the 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	xix
	Junos Space Documentation and Release Notes	xix
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Security Director Overview	
Chapter 1	Security Director Overview	3
	Security Director Overview	3
Chapter 2	Security Director Dashboard	7
	Security Director Dashboard	7
Part 2	Getting Started	
Chapter 3	Getting Started with Security Director	13
	Getting Started	13
	Provisioning Firewall Policies	13
	Provisioning NAT Policies	13
	Provisioning IPsec VPNs	14
	IPS Management	14
	AppFW Management	14
Part 3	Object Builder	
Chapter 4	Object Builder Overview	19
	Object Builder Overview	19
Chapter 5	Service and Service Groups	21
	Service and Service Group Overview	21
	Creating Services	22
	Managing Services	25
	Modifying a Service	25
	Deleting a Service	25
	Cloning a Service	26
	Find Duplicate Service Objects	26
	Find Service Usage	27
	Replace Services	28
	Show Unused Services	30

	Delete All Unused Services	30
	Creating Service Groups	31
	Managing Service Groups	32
	Modifying a Service Group	32
	Deleting a Service Group	32
	Cloning a Service Group	33
Chapter 6	Addresses and Address Groups	35
	Address and Address Groups Overview	35
	Creating Addresses	35
	Managing Addresses	37
	Modifying an Address	38
	Deleting an Address	38
	Cloning an Address	38
	Exporting Addresses	39
	Importing Addresses	39
	Find Duplicate Address Objects	39
	Find Address Usage	42
	Replace Addresses	42
	Show Unused Addresses	44
	Delete All Unused Addresses	44
	Creating Address Groups	45
	Managing Address Groups	46
	Modifying an Address Group	46
	Deleting an Address Group	46
	Cloning an Address Group	47
Chapter 7	Extranet Devices	49
	Creating Extranet Devices	49
	Managing Extranet Devices	50
	Modifying an Extranet Device	50
	Deleting an Extranet Device	50
	Cloning an Extranet Device	51
Chapter 8	Application Signatures	53
	Creating Application Signatures	53
	Managing Application Signatures	55
	Filtering Application Signatures	55
	Modifying Application Signatures	56
	Deleting Application Signatures	56
	Cloning Application Signatures	56
	Creating an Application Signature Group	57
Chapter 9	Schedulers	59
	Scheduler Overview	59
	Creating a Scheduler	60
	Managing Scheduler	62
	Modifying a Scheduler	62
	Deleting a Scheduler	62
	Find Scheduler Usage	63

	Show Unused Schedulers	63
Chapter 10	NAT Pools	65
	Creating NAT Pools	66
	Managing NAT Pools	69
	Deleting NAT Pools	69
	Modifying NAT Pools	69
	Cloning NAT Pools	70
	Show Duplicate NAT Pools	70
	Find NAT Pool Usage	72
	Replace Addresses	73
	Show Unused NAT Pools	74
	Delete All Unused NAT Pools	75
Chapter 11	Policy Profiles	77
	Security Policy Profiles Overview	77
	Creating Policy Profiles	78
	Managing Policy Profiles	81
	Deleting Policy Profiles	81
	Modifying Policy Profiles	81
	Cloning Policy Profiles	82
Chapter 12	VPN Profiles	83
	VPN Profiles Overview	83
	Creating VPN Profiles	84
	Managing VPN Profiles	87
	Deleting VPN Profiles	88
	Modifying VPN Profiles	88
	Cloning VPN Profiles	88
Chapter 13	Variables	91
	Creating Variable Definitions	91
	Managing Variable Definitions	94
	Deleting Variable Definitions	94
	Modifying Variable Definitions	95
	Cloning Variable Definitions	95
Chapter 14	Template Definitions	97
	Creating Template Definitions	97
	Managing Template Definitions	98
	Deleting Template Definitions	99
	Modifying Template Definitions	99
Chapter 15	Templates	101
	Creating Templates	101
	Managing Templates	102
	Deleting Templates	102
	Modifying Templates	103

Part 4

Chapter 16

Firewall Policy

Firewall Policy	107
Firewall Policies Overview	107
Rule Base Overview	108
Example: UnManaging a Previously Managed Rule Base	109
Custom Column Overview	109
Custom Column Data Search	109
Multiple Group Policy Membership Overview	110
General Rules About Priority and Precedence	110
Example: New Precedence of a Policy Set to the Same Precedence as an Existing Policy	111
Sorting of Firewall Policy Left Pane	111
Global Address Book Overview	114
Differences Between Global and Zone-Based Address Books	114
Nested Address Group Support	114
Mixed-Version Support	115
Migrating from Zone to Global Addressing	115
Example: Configuring Address Book Entries in Global Address Book	116
Creating Firewall Policies	117
Unlocking Locked Policies	132
Inline Creation of Objects in Policy	134
Policy Priority Precedence Setting	139
Adding Rules to a Firewall Policy	143
Ordering the Rules in a Firewall Policy	147
Publishing Firewall Policies	149
Managing Firewall Policies	155
Modifying Firewall Policies	156
Comparing Firewall Policies	158
Deleting Firewall Policies	159
Adding Rules to a Firewall Policy	160
Cloning Firewall Policies	160
Promoting a Firewall Policy	161
Exporting a Firewall Policy	161
Policy Versioning	162
Managing Policy Versioning	164
Deleting Rules in a Firewall Policy	169
Cloning a Rule in a Firewall Policy	169
Grouping Rules in a Firewall Policy	170
Enabling/Disabling Rules in a Firewall Policy	170
Expanding/Collapsing All Rules in a Firewall Policy	171
Cutting/Copying and Pasting Rules or Rule Groups in a Firewall Policy	171
Assigning Devices to a Firewall Policy	172
Deleting Devices from a Firewall Policy	173
Rule Operations on the Filtered Rules	173
Managing Custom Column Data	175
Modifying Custom Columns Definitions	175
Deleting a Custom Columns Definition	176
Exporting a Custom Columns Definition	176

Part 5	VPN	
Chapter 17	VPN	179
	IPsec VPN Overview	179
	Creating IPsec VPNs	181
	Creating IPsec VPNs	181
	Publishing IPsec VPNs	192
	Managing IPsec VPNs	194
	Modifying IPsec VPNs	194
	Modifying Endpoint Settings in a VPN	195
	Deleting IPsec VPNs	196
Part 6	NAT Policies	
Chapter 18	NAT Policy	201
	NAT Overview	201
	Creating NAT Policies	205
	Unlocking Locked Policies	218
	Global Address Book Overview	219
	Differences Between Global and Zone-Based Address Books	220
	Adding Rules to a NAT Policy	221
	Ordering the Rules in a NAT Policy	227
	Publishing NAT Policies	227
	Managing NAT Policies	230
	Modifying NAT Policies	231
	Deleting NAT Policies	231
	Cloning NAT Policies	231
	Exporting a NAT Policy	232
	Configuring NAT Rule Sets	232
	NAT Policy Versioning	232
	Managing NAT Policy Versioning	234
	Deleting Rules in a NAT Policy	238
	Grouping Rules in a NAT Policy	239
	Enabling/Disabling Rules in a NAT Policy	239
	Expanding/Collapsing All Rules in a NAT Policy	240
	Cutting/Copying and Pasting Rules or Rule Groups in a NAT Policy	240
	Assigning Devices to a NAT Policy	242
	Deleting Devices from a NAT Policy	242
	Rule Operations on the Filtered Rules	243
Part 7	Global Search	
Chapter 19	Global Search	247
	Indexing Overview	247
	Global Search	247

Part 8	Downloads	
Chapter 20	Downloads	253
	Downloading the Signature Database	253
	Installing the Signature Database	255
Part 9	IPS Management	
Chapter 21	IPS Management Overview	261
	IPS Management Overview	261
Chapter 22	IPS Management	263
	Creating IPS Signatures	263
	Managing IPS Signatures	265
	Filtering IPS Signatures	266
	Modifying IPS Signatures	266
	Deleting IPS Signatures	266
	Cloning IPS Signatures	267
	Creating Static Signature Groups	267
	Creating Dynamic Signature Groups	267
	Creating IPS Signature Sets	268
	Creating IPS Signature Sets	268
	Adding Rules to an IPS Signature Set	269
	Managing IPS Signature Sets	270
	Deleting IPS Signature Sets	271
	Cloning IPS Signature Sets	271
	Enable or Disable Rules in an IPS Signature-set	271
	Grouping Rules in an IPS Signature Set	272
	Expanding/Collapsing All Rules in an IPS Signature Set	272
	Cutting/Copying And Pasting Rules or Rule Groups in an IPS Signature Set	273
	Adding Rules to an IPS Signature Set	273
	Creating IPS Policies	274
	Managing Policy Locks	283
	Ordering the Rules in a IPS Policy	284
	Adding Rules to an IPS Policy	285
	Publishing IPS Policies	287
	Managing IPS Policies	291
	Deleting IPS Policy Rules	292
	Enabling or Disabling Rules in an IPS Policy	292
	Cloning a Rule in an IPS Policy	292
	Grouping Rules in an IPS Policy	293
	Expanding/Collapsing All Rules in an IPS Policy	293
	Cutting/Copying And Pasting Rules or Rule Groups in an IPS Policy	293
	Adding Rules to an IPS Policy	294
	Rule Operations on the Filtered Rules	294

Part 10	Security Director Devices	
Chapter 23	Security Director Devices	299
	Updating Devices with Pending Services	299
	Importing Firewall, NAT, and IPS Policies from a Device to Security Director . . .	303
	NSM Migration	309
	Managing Consolidated Configurations	315
	Generating a Consolidated Configuration	315
Part 11	Index	
	Index	321

List of Figures

Part 1	Security Director Overview	
Chapter 1	Security Director Overview	3
	Figure 1: Security Director Home Page	4
	Figure 2: Junos OS schema Mismatch Warning Message	5
Chapter 2	Security Director Dashboard	7
	Figure 3: Object Count Gadget	8
	Figure 4: Address Types Gadgets	9
Part 3	Object Builder	
Chapter 4	Object Builder Overview	19
	Figure 5: Variable Objects: Concurrent Edit Save Warning Message	20
Chapter 5	Service and Service Groups	21
	Figure 6: Create Service: Basic View Page	22
	Figure 7: Create Service: Advanced Settings Page	23
	Figure 8: Window Showing Duplicate Services	26
	Figure 9: Window Showing Service Usage	28
	Figure 10: Replace Services Window	29
	Figure 11: Service: Confirm Replace Warning Message	29
	Figure 12: Service Replace Successful Message	30
	Figure 13: Create Service Group Page	31
Chapter 6	Addresses and Address Groups	35
	Figure 14: Create Address Page	36
	Figure 15: Page Showing Duplicate Address Objects	40
	Figure 16: Merge Address Page	40
	Figure 17: Merge Operation Confirmation Message	40
	Figure 18: Duplicate Objects Delete Confirmation Page	41
	Figure 19: Duplicate Objects Usage Window	41
	Figure 20: Window Showing Address Usage	42
	Figure 21: Replace Addresses Window	43
	Figure 22: Address: Confirm Replace Warning Message	43
	Figure 23: Address Replace Success Message	44
	Figure 24: Create Address Group Page	45
Chapter 7	Extranet Devices	49
	Figure 25: Create Extranet Device Page	49
Chapter 8	Application Signatures	53
	Figure 26: Application Signatures Page	53

	Figure 27: Create Application Signature Page	54
Chapter 9	Schedulers	59
	Figure 28: Scheduler Main Page	60
	Figure 29: Create Scheduler	61
	Figure 30: Scheduler Find Usage Window	63
Chapter 10	NAT Pools	65
	Figure 31: Create NAT Pool Page	66
	Figure 32: Inline Address Group Creation for NAT Pool	68
	Figure 33: Show Duplicates of NAT Pool	71
	Figure 34: Merge NAT Pool	71
	Figure 35: Delete Duplicate NAT Pool Objects	72
	Figure 36: Confirm Merge Operation	72
	Figure 37: NAT Pool Usage Window	73
	Figure 38: Replace NAT Pools	74
Chapter 11	Policy Profiles	77
	Figure 39: New Policy Profile Page	78
	Figure 40: Create Policy Profile - Advanced Settings	80
Chapter 12	VPN Profiles	83
	Figure 41: VPN Profile: Phase 1	84
	Figure 42: VPN Profile: Phase 2	86
	Figure 43: Create Phase 2 Proposal	86
Chapter 13	Variables	91
	Figure 44: Create Polymorphic Object Page	92
	Figure 45: Inline Address Group Creation for a Polymorphic Object	93
Chapter 14	Template Definitions	97
	Figure 46: Create Template Definition Page	98
Chapter 15	Templates	101
	Figure 47: Create Template Page	102
Part 4	Firewall Policy	
Chapter 16	Firewall Policy	107
	Figure 48: Custom Column Data Search	110
	Figure 49: Sorting Order in the Firewall Policy Left Pane	111
	Figure 50: Policy View Setting	113
	Figure 51: Firewall Policy Tabular View	117
	Figure 52: Create Firewall Policy	119
	Figure 53: Turning an IPS Policy On or Off	120
	Figure 54: Policy With Error Saved As Draft	121
	Figure 55: Lock Failure Error Message for the Second User	122
	Figure 56: Inactivity Timeout Error	122
	Figure 57: Policy Lock Expired Message	122
	Figure 58: Save the Edited Policy with a Different Name	123
	Figure 59: Unsaved Changes Warning Message	123
	Figure 60: Policy Unlock by Admin Message	123

Figure 61: Policy Lock Release Message	124
Figure 62: Creating Custom Column	125
Figure 63: Creating Custom Column Page	125
Figure 64: Create Custom Column Confirm Page	125
Figure 65: Source Identity Page	126
Figure 66: Select Devices Page	127
Figure 67: Tooltip Showing Object Information	128
Figure 68: Advanced Search Dialog for Firewall Policies	129
Figure 69: Firewall Policy: Manage Policy Locks	133
Figure 70: Modify Security Director Settings	133
Figure 71: Inline Address Object Creation in the Source Address Window	134
Figure 72: Inline Address Object Create Page	135
Figure 73: Address Selector Page Showing the New Inline Object	135
Figure 74: Inline Address Group Creation	136
Figure 75: Inline Service Object Creation in the Service List	137
Figure 76: Inline Service Object Creation Page	137
Figure 77: Service Selector Page Showing the New Object	138
Figure 78: Policy: Priority And Precedence Page	140
Figure 79: Priority Precedence Tool Tlp	140
Figure 80: Priority And Precedence Right-Click Page	142
Figure 81: Setting Priority And Precedence Value Page	142
Figure 82: Tunnel Option for Device Rule	144
Figure 83: TCP-Session Options	145
Figure 84: Concurrent Policy Edit Error Message	147
Figure 85: Policy Publish Page	150
Figure 86: Devices on Which the Policies Will Be Published	150
Figure 87: Policy Publish: CLI Configuration	151
Figure 88: Device Validation Warning Message	151
Figure 89: Policy Publish: LSYS Device CLI Configuration	152
Figure 90: Policy Publish: XML Configuration	153
Figure 91: Modify Policy Page	157
Figure 92: Compare Policy	158
Figure 93: Compare Policy Result	159
Figure 94: Clone Policy Page	160
Figure 95: Promote Policy Page	161
Figure 96: Snapshot Policy Window	163
Figure 97: Modify Security Director Settings	164
Figure 98: Rollback Service Summary Page	165
Figure 99: Object Conflict Resolution Window	165
Figure 100: Rollback OCR Summary Report	166
Figure 101: Rollback Snapshot Policy Report	166
Figure 102: Manage Versions Window	167
Figure 103: Compare Versions Window	167
Figure 104: Compare Versions: Results Window	168
Figure 105: Confirm Delete Operation Message	168
Figure 106: ExpandAll Warning Message for More Than Thousand Rules	171
Figure 107: Nested Rule Group Paste Operation Warning Message	172
Figure 108: Variable Objects Rule Paste Error	172
Figure 109: Modifying a Custom Column	175

	Figure 110: Deleting a Custom Column	176
Part 5	VPN	
Chapter 17	VPN	179
	Figure 111: VPN Landing Page	181
	Figure 112: VPN Profile Tooltip	182
	Figure 113: Create VPN Page—Route-Based VPN	183
	Figure 114: Create VPN: Add as Endpoint Page	184
	Figure 115: Create VPN—Tunnel, Route, and Global Setting Pane	184
	Figure 116: Create VPN: Hub and Spoke Configuration	185
	Figure 117: Create VPN Page Showing Custom Routing Instance Option	187
	Figure 118: Create VPN Policy-Based—Add as Endpoint Page	188
	Figure 119: Create VPN Page—External Interface Selection	189
	Figure 120: VPN: Concurrent Save Error Message	190
	Figure 121: Inline Address Object Creation Page	191
	Figure 122: Inline Address Group Creation for VPN Object	192
Part 6	NAT Policies	
Chapter 18	NAT Policy	201
	Figure 123: NAT Tabular View	205
	Figure 124: Create NAT Policy Page	206
	Figure 125: Lock Failure Error Message for the Second User	207
	Figure 126: Inactivity Timeout Error	207
	Figure 127: Policy Lock Expired Message	207
	Figure 128: NAT Locked Policy: Save As Window	208
	Figure 129: NAT Policy: Unsaved Changes Message	208
	Figure 130: NAT Policy: Policy Unlock by Admin Message	208
	Figure 131: NAT Policy Lock Release Message	208
	Figure 132: Setting Source NAT Pool Page	210
	Figure 133: Create Source NAT Pool Page	210
	Figure 134: Setting the Destination Pool Page	211
	Figure 135: Create Destination NAT Pool Page	211
	Figure 136: Create Inline NAT Address Object	211
	Figure 137: Create NAT Address Page	212
	Figure 138: Inline Address Group Creation for NAT Policy	212
	Figure 139: Advanced Search Box for NAT Policies	214
	Figure 140: Policy View Settings	217
	Figure 141: NAT Policy: Manage Policy Locks	218
	Figure 142: Modify Security Director Settings	219
	Figure 143: Destination Traffic Match Type Selector Page	223
	Figure 144: Port Configuration for Static NAT	224
	Figure 145: Concurrent NAT Policy Editing Error	226
	Figure 146: NAT Policy CLI Configuration	228
	Figure 147: Snapshot Policy	233
	Figure 148: Modify Security Director Settings	234
	Figure 149: Rollback Service Summary Report	235
	Figure 150: Object Conflict Resolution Window	235

	Figure 151: Rollback OCR Summary Report	236
	Figure 152: Rollback Policy Summary Report	236
	Figure 153: Compare Versions With Swap Option	237
	Figure 154: Versions Comparing Summary Report	237
	Figure 155: Snapshot Delete Confirm Window	238
	Figure 156: ExpandAll Warning Message for More Than Thousand Rules	240
	Figure 157: Nested Rule Group Operation Warning Message	241
	Figure 158: Destination NAT Rule Paste Error	241
	Figure 159: Static NAT Rule Paste Error	241
	Figure 160: Group Policy Paste Error	241
Part 7	Global Search	
Chapter 19	Global Search	247
	Figure 161: Indexing Status Message	247
	Figure 162: Global Search Results	248
Part 8	Downloads	
Chapter 20	Downloads	253
	Figure 163: Signature Download Logs	253
	Figure 164: Signature Database Page	254
	Figure 165: Download Configuration Page	254
	Figure 166: Install Configuration Page	256
Part 9	IPS Management	
Chapter 22	IPS Management	263
	Figure 167: View All IPS Signatures Page	264
	Figure 168: Create IPS Signature Page	264
	Figure 169: IPS Signature Set Tabular View	269
	Figure 170: Nested Rule Group Paste Warning Message	273
	Figure 171: IPS Policies Tabular View	275
	Figure 172: Policy View Settings	277
	Figure 173: IPS Advance Search Window	278
	Figure 174: Lock Failure Error Message for the Second User	280
	Figure 175: Inactivity Timeout Error	281
	Figure 176: Policy Lock Expired Message	281
	Figure 177: Unsaved Changes Warning Message	281
	Figure 178: Policy Unlock by Admin Message	281
	Figure 179: Policy Lock Release Message	282
	Figure 180: IPS Policy: Manage Policy Locks	283
	Figure 181: Modify Security Director Settings	284
	Figure 182: IPS Policy Publish Page	288
	Figure 183: Policy Publish: Affected Devices Page	288
	Figure 184: Policy Publish: CLI Configuration	289
	Figure 185: Policy Publish: XML Configuration	289
	Figure 186: Nested Rule Groups Paste Operation Warning Message	294

Part 10

Chapter 23

Security Director Devices

Security Director Devices	299
Figure 187: Security Director Devices Page	299
Figure 188: Update Window	300
Figure 189: Device Changes Page Showing Device Comments	301
Figure 190: Sync Device Status Page	302
Figure 191: Manage Security Devices Page	304
Figure 192: Service Import Summary Page	304
Figure 193: Object Conflict Resolution Page	305
Figure 194: Same Action Applied to Two Conflicting Objects	306
Figure 195: Policy Import Status Page	306
Figure 196: Firewall Policy Final Import Status Page	307
Figure 197: High-level Device Import Workflow	310
Figure 198: NSM Xdiff File Upload Page	311
Figure 199: NSM Migration Devices Page	311
Figure 200: Service Import Summary Page	312
Figure 201: NSM—Object Conflict Resolution Page	312
Figure 202: NSM Migration Status Page	313
Figure 203: NSM Migration Final Status Report Page	314
Figure 204: Consolidated Config Status from Security Director	316

List of Tables

	About the Documentation	xix
	Table 1: Text and Syntax Conventions	xix
Part 1	Security Director Overview	
Chapter 2	Security Director Dashboard	7
	Table 2: Security Director Workspaces	7
Part 4	Firewall Policy	
Chapter 16	Firewall Policy	107
	Table 3: Sorting Order for Firewall Policies	111
	Table 4: Migration Matrix	115
	Table 5: IPS Configuration Mode	120
	Table 6: Firewall policy Right Pane Search Options	128
	Table 7: Specific Security Director Search Behavior	131
	Table 8: Examples of Different Advanced Search Parameters	131
	Table 9: Priority and Precedence for Firewall Policies	141
	Table 10: Setting Precedence Values for Different Priorities	157
	Table 11: Various Rule Operation on the Filtered Rules	173
Part 6	NAT Policies	
Chapter 18	NAT Policy	201
	Table 12: Persistent NAT Support	202
	Table 13: Translated Address Pool Selection for Source NAT	203
	Table 14: Translated Address Pool Selection for Destination NAT And Static NAT	203
	Table 15: Junos OS Protocol Names	213
	Table 16: Specific Security Director Search Behavior	215
	Table 17: Example: Different Advanced Search Parameters for NAT	215
	Table 18: Example: Rule Set Names for Different Ingress And Egress Values of Source NAT Rules	225
	Table 19: Example: Rule Set Names for Destination NAT and Static NAT	225
	Table 20: Various Rule Operation on the Filtered Rules	243
Part 7	Global Search	
Chapter 19	Global Search	247
	Table 21: Security Director Global Search	248

Part 9	IPS Management	
Chapter 22	IPS Management	263
	Table 22: IPS Configuration Mode	274
	Table 23: Specific Security Director Search Behavior	279
	Table 24: Examples of Different Advanced Search Parameters	279
	Table 25: Various Rule Operation on the Filtered Rules	295
Part 10	Security Director Devices	
Chapter 23	Security Director Devices	299
	Table 26: Different Status of Consolidated Configuration	316

About the Documentation

- [Junos Space Documentation and Release Notes on page xix](#)
- [Documentation Conventions on page xix](#)
- [Documentation Feedback on page xxi](#)
- [Requesting Technical Support on page xxi](#)

Junos Space Documentation and Release Notes

For a list of related Junos Space documentation, see <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Space 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/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

Documentation Conventions

[Table 1 on page xix](#) defines the text and syntax conventions used in this guide.

Table 1: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

Table 1: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces or emphasizes important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric metric>;</code>
(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.	<code>broadcast multicast</code> <code>(string1 string2 string3)</code>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<code>rsvp { # Required for dynamic MPLS only</code>
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	<code>community name members [</code> <code>community-ids]</code>
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop address; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.

Table 1: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release 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:
<https://www.juniper.net/alerts/>
- 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

Security Director Overview

- [Security Director Overview on page 3](#)
- [Security Director Dashboard on page 7](#)

CHAPTER 1

Security Director Overview

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

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.

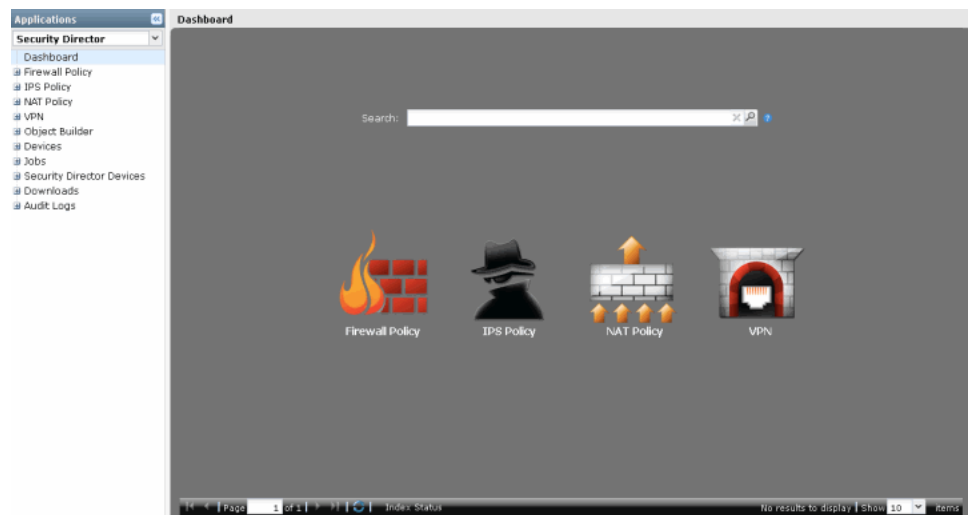
A set of gadgets displayed on the dashboard graphically illustrates the critical elements related to your security configurations. These gadgets help you keep track of the objects created and their usage across security configurations.

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 create 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 home page.

Figure 1: Security Director Home Page



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 Dashboard on page 7](#)

CHAPTER 2

Security Director Dashboard

- [Security Director Dashboard on page 7](#)

Security Director Dashboard

Table 2 on page 7 lists the workspaces on the Security Director dashboard.

Table 2: Security Director Workspaces




Icons	Workspace Name	Tasks
	Firewall Policy	Create, manage, and publish firewall policies.
	IPS Management	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.

Table 2: Security Director Workspaces (*continued*)

Icons	Workspace Name	Tasks
—	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 3 on page 8 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 3: Object Count Gadget

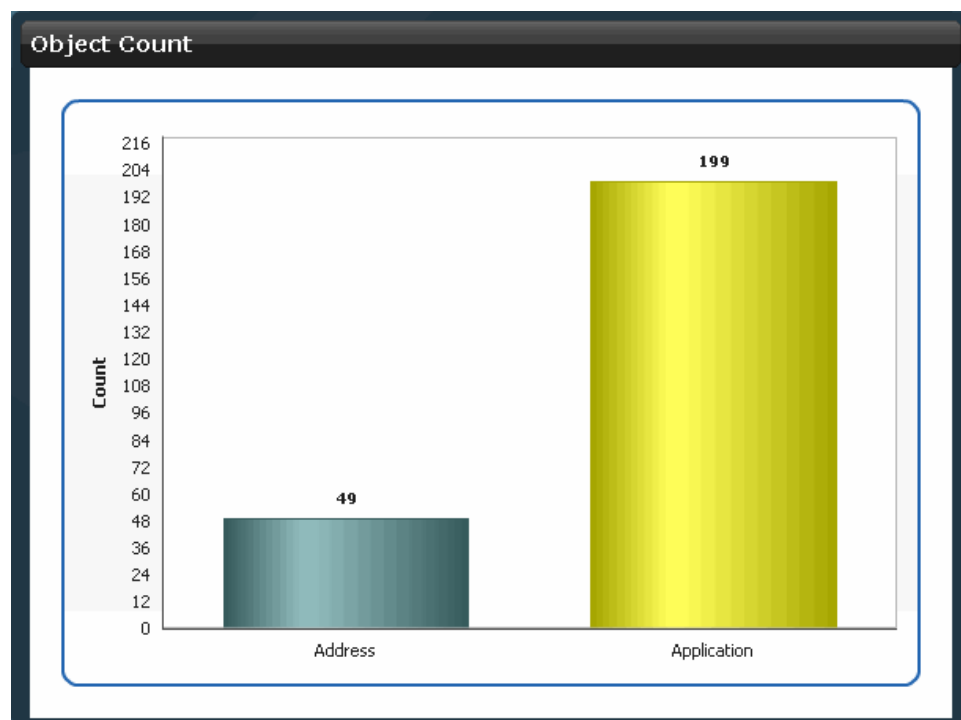
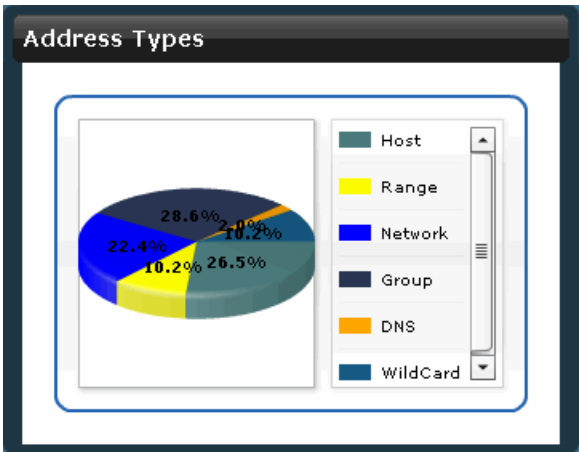


Figure 4 on page 9 shows the Address Types gadget. This gadget shows the different address types created using the Address Creation Wizard.

Figure 4: Address Types Gadgets



PART 2

Getting Started

- [Getting Started with Security Director on page 13](#)

CHAPTER 3

Getting Started with Security Director

- [Getting Started on page 13](#)

Getting Started

The Getting Started assistant provides instructions on how to perform tasks related to a firewall policy, a NAT policy, a VPN, an IPS configuration, and an AppFirewall configuration in Security Director.

The Getting Started section displays instructions on how to perform the following tasks:

1. [Provisioning Firewall Policies on page 13](#)
2. [Provisioning NAT Policies on page 13](#)
3. [Provisioning IPsec VPNs on page 14](#)
4. [IPS Management on page 14](#)
5. [AppFW Management on page 14](#)

Provisioning Firewall Policies

To provision firewall policies:

1. Discover devices. See “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See “[Creating Addresses](#)” on page 35.
3. Create a policy profile. See “[Creating Policy Profiles](#)” on page 78.
4. Create a service. See “[Creating Services](#)” on page 22.
5. Create firewall policies. See “[Creating Firewall Policies](#)” on page 117.
6. Publish firewall policies. See “[Publishing Firewall Policies](#)” on page 149
7. Update devices. See “[Updating Devices with Pending Services](#)” on page 299.

Provisioning NAT Policies

To provision NAT policies:

1. Discover devices. See “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See “[Creating Addresses](#)” on page 35.
3. Create firewall policies. See “[Creating Firewall Policies](#)” on page 117.
4. Publish firewall policies. See “[Publishing Firewall Policies](#)” on page 149
5. Create NAT pools. See “[Creating NAT Pools](#)” on page 66
6. Create NAT policies. See “[Creating NAT Policies](#)” on page 205.
7. Publishing NAT policies. See “[Publishing NAT Policies](#)” on page 227
8. Update devices. See “[Updating Devices with Pending Services](#)” on page 299.

Provisioning IPsec VPNs

To provision IPsec VPNs:

1. Discover devices. See “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.
2. Create addresses. See “[Creating Addresses](#)” on page 35.
3. Create a VPN profile. See “[Creating VPN Profiles](#)” on page 84.
4. Create an IPsec VPN. See “[Creating IPsec VPNs](#)” on page 181.
5. Publish the IPsec VPN. See “[Publishing IPsec VPNs](#)” on page 192.
6. Update devices. See “[Updating Devices with Pending Services](#)” on page 299.

IPS Management

To manage IPS:

1. Discover devices. See “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.
2. Download IPS signature. See “[Downloading the Signature Database](#)” on page 253.
3. Pushing IPS signature to the device. See “[Installing the Signature Database](#)” on page 255.
4. Create a firewall policy with IPS enabled. See “[Creating Firewall Policies](#)” on page 117.
5. Publish firewall policies. See “[Publishing Firewall Policies](#)” on page 149.
6. Update devices. See “[Updating Devices with Pending Services](#)” on page 299.
7. Create IPS signatures. See “[Creating IPS Signatures](#)” on page 263.
8. Create IPS signature set. See “[Creating IPS Signature Sets](#)” on page 268.
9. Create IPS policies. See “[Creating IPS Policies](#)” on page 274.

AppFW Management

To manage AppFW:

1. Discover devices. See “Discovering Devices” section in the *Junos Space Network Application Platform User Guide*.
2. Download an application signature. See [“Downloading the Signature Database” on page 253](#).
3. Push an application signature to the device. See [“Installing the Signature Database” on page 255](#).
4. Create a firewall policy with AppFW enabled. See [“Creating Firewall Policies” on page 117](#).
5. Publish firewall policies. See [“Publishing Firewall Policies” on page 149](#).
6. Update devices. See [“Updating Devices with Pending Services” on page 299](#).
7. Create application signature. See [“Creating Application Signatures” on page 53](#).

PART 3

Object Builder

- [Object Builder Overview on page 19](#)
- [Service and Service Groups on page 21](#)
- [Addresses and Address Groups on page 35](#)
- [Extranet Devices on page 49](#)
- [Application Signatures on page 53](#)
- [Schedulers on page 59](#)
- [NAT Pools on page 65](#)
- [Policy Profiles on page 77](#)
- [VPN Profiles on page 83](#)
- [Variables on page 91](#)
- [Template Definitions on page 97](#)
- [Templates on page 101](#)

CHAPTER 4

Object Builder Overview

- [Object Builder Overview on page 19](#)

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
- Application signatures
- Extranet devices
- NAT pools
- Policy profiles
- VPN profiles
- Variables
- Template and template definitions

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.

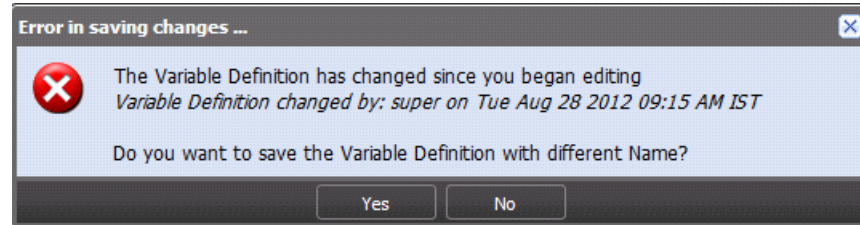
Concurrent editing is supported for the following objects:

- 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 5 on page 20](#). This is an example error message received for the Variables object.

Figure 5: Variable Objects: Concurrent Edit Save Warning Message



Related Documentation

- [Address and Address Groups Overview on page 35](#)
- [Service and Service Group Overview on page 21](#)
- [Security Policy Profiles Overview on page 77](#)
- [VPN Profiles Overview on page 83](#)

CHAPTER 5

Service and Service Groups

- [Service and Service Group Overview on page 21](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)
- [Creating Service Groups on page 31](#)
- [Managing Service Groups on page 32](#)

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.

Related Documentation

- [Creating Services on page 22](#)
- [Creating Service Groups on page 31](#)
- [Managing Services on page 25](#)
- [Managing Service Groups on page 32](#)

Creating Services

To create a service:

1. Select Security Director > Object Builder > Services.

The Manage Services page appears, listing all available services.

2. From the left pane, under Services, select **Create Service**.




The Create Service page appears, as shown in [Figure 6 on page 22](#).

Figure 6: Create Service: Basic View Page

Create Service

Name:

Description:

Protocols:   

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

3. Click on the plus sign (+) to configure a new protocol.

Figure 7: Create Service: Advanced Settings Page

The screenshot shows a 'New Protocol' dialog box with the following fields and options:

- Name:** A text input field.
- Description:** A larger text input field.
- Type:** A dropdown menu currently set to 'TCP'.
- Destination Port:** A text input field.
- Advanced Settings:** A section with a collapse icon and the following options:
 - Disable Inactivity Timeout:** A checkbox that is currently unchecked.
 - Inactivity Timeout:** A spin box with up and down arrows.
 - ALG:** A dropdown menu.
 - Source Port:** A text input field.

At the bottom of the dialog are 'Add' and 'Cancel' buttons.

The Advanced Settings fields are not mandatory fields.

4. Enter the name of the service in the Name field.
5. Enter a description for the service in the Description field.
6. In the Protocols pane, click Add icon to add a new protocol.

The New Protocol dialog box appears, populated with the default values.

7. Enter a name for the new protocol in the Name section.
8. Enter a description for the new protocol in the Description field.
9. Enter destination ports for the selected types in the Destination Port field.
10. 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 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.
 - 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.
11. Click **Add** in the New Protocol dialog box.
 12. Click **Create** to create the service.

Related Documentation

- [Service and Service Group Overview on page 21](#)
- [Creating Service Groups on page 31](#)
- [Managing Services on page 25](#)
- [Managing Service Groups on page 32](#)

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 25](#)
2. [Deleting a Service on page 25](#)
3. [Cloning a Service on page 26](#)
4. [Find Duplicate Service Objects on page 26](#)
5. [Find Service Usage on page 27](#)
6. [Replace Services on page 28](#)
7. [Show Unused Services on page 30](#)
8. [Delete All Unused Services on page 30](#)

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 8 on page 26](#). Predefined services are also listed under duplicate objects.

Figure 8: 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
	ipsec-global (2 members)		Merge
	ping (2 members)		Merge
	ping6 (2 members)		Merge
	icmp6-all	Service	predefined service
	ping6	Service	predefined service
	scp-any (2 members)		Merge
	sun-rpc (2 members)		Merge

3. 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.

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.

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) or security objects (service groups) .

Procedure to manually rebuild the Index, see "[Indexing Overview](#)" on page 247

Find Service Usage

To find service usage:

1. 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, as shown in [Figure 9 on page 28](#).

Figure 9: Window Showing Service Usage



Procedure to manually rebuild the Index, see ["Indexing Overview"](#) on page 247

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:

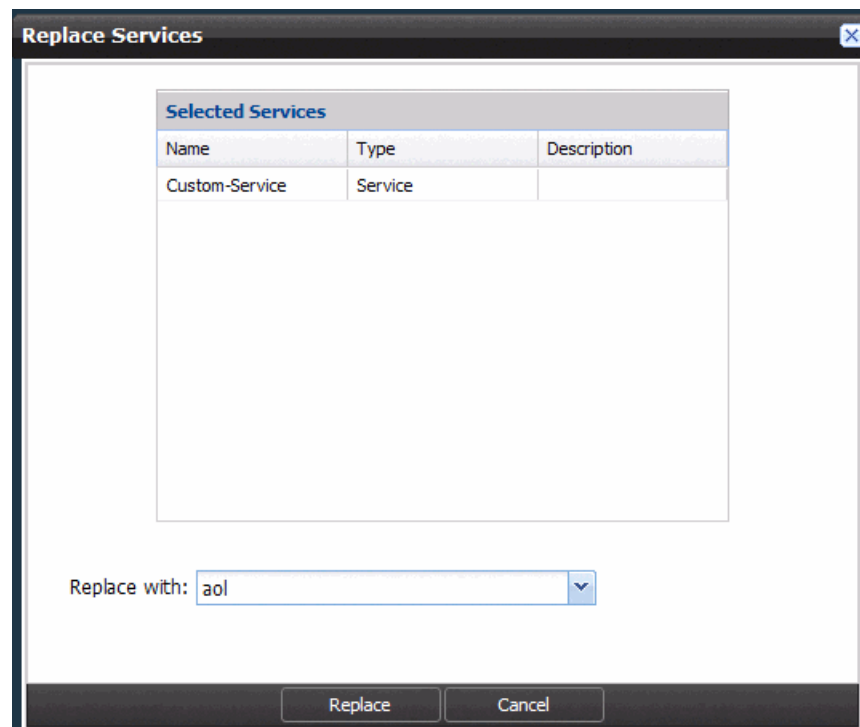
1. Select **Security Director > Object Builder > Services**.

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.

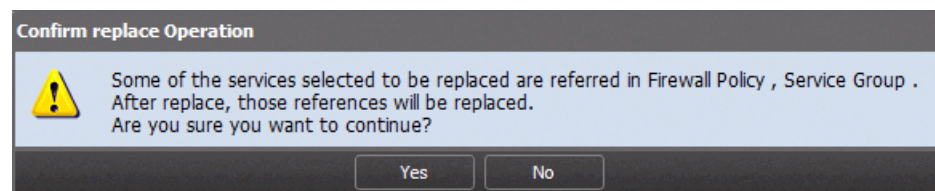
A window appears, showing the service or services you have selected to be replaced, along with a drop-down list of the services that are available to replace the service or services you have selected. See [Figure 10 on page 29](#).

Figure 10: Replace Services Window



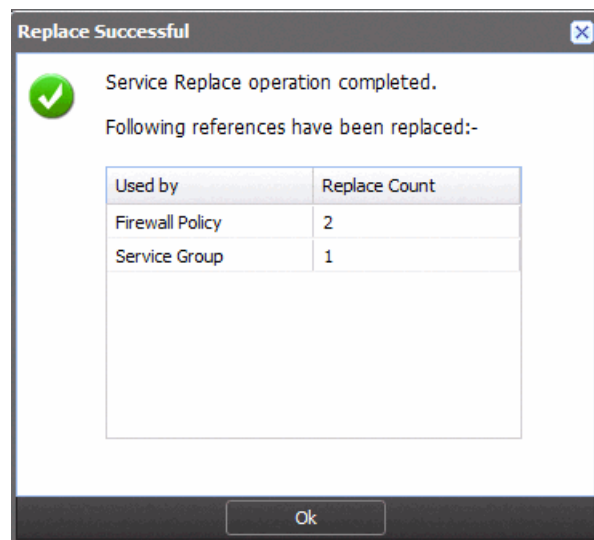
3. In the Replace Services window, select the service, service group, or nested service group that will replace the selected service or services, and click **Replace**. If the selected services are used in any other references, you will receive the following warning message before replacing, as shown in [Figure 11 on page 29](#). Click **Yes** to replace.

Figure 11: 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 12 on page 30](#).

Figure 12: 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 247](#)

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 21](#)
- [Creating Services on page 22](#)
- [Creating Service Groups on page 31](#)
- [Managing Service Groups on page 32](#)

Creating Service Groups

To create a service group:

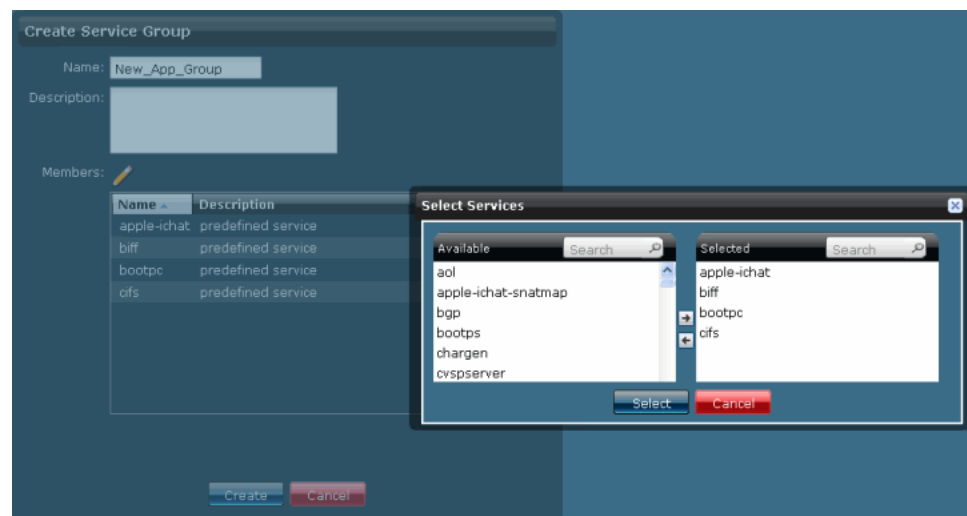
1. Select **Security Director > Object Builder > Services**.

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

2. From the left pane, select **Create Service Group** under Services.

The Create Service Group page appears, as shown in [Figure 13 on page 31](#).

Figure 13: Create Service Group Page



3. In the Name field, enter a name for the new service group.
4. In the Description field, enter a description for the new service group.
5. In the Members pane, click the **Add** icon to add a new service to this service group.

The Select Services dialog box appears.

6. From the Available pane in the dialog box, select the service you want to group, and click the **Add** icon.

The service you have selected appears in the Selected section of the dialog box. Repeat Steps 5 and 6 to add more services to this service group.

7. Click **Create**.

The service group appears on the Services page.

Related Documentation

- [Service and Service Group Overview on page 21](#)
- [Managing Service Groups on page 32](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)

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 32](#)
2. [Deleting a Service Group on page 32](#)
3. [Cloning a Service Group on page 33](#)

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 21](#)
- [Creating Service Groups on page 31](#)
- [Creating Services on page 22](#)
- [Managing Services on page 25](#)

CHAPTER 6

Addresses and Address Groups

- [Address and Address Groups Overview on page 35](#)
- [Creating Addresses on page 35](#)
- [Managing Addresses on page 37](#)
- [Creating Address Groups on page 45](#)
- [Managing Address Groups on page 46](#)

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 35](#)
- [Managing Addresses on page 37](#)
- [Creating Address Groups on page 45](#)
- [Managing Address Groups on page 46](#)

Creating Addresses

To create an address:

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

The Address page appears.

2. From the left pane, select **Create Address** under Addresses.

The Create Address page appears, as shown in [Figure 14 on page 36](#).

Figure 14: Create Address Page

3. In the Name field, enter a name for the new address.
4. In the Description field, enter a description for the new address.
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 35](#)
- [Managing Addresses on page 37](#)
- [Creating Address Groups on page 45](#)
- [Managing Address Groups on page 46](#)

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 38](#)
2. [Deleting an Address on page 38](#)
3. [Cloning an Address on page 38](#)

4. [Exporting Addresses on page 39](#)
5. [Importing Addresses on page 39](#)
6. [Find Duplicate Address Objects on page 39](#)
7. [Find Address Usage on page 42](#)
8. [Replace Addresses on page 42](#)
9. [Show Unused Addresses on page 44](#)
10. [Delete All Unused Addresses on page 44](#)

Modifying an Address

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

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**.

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.

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**.

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 15 on page 40](#).

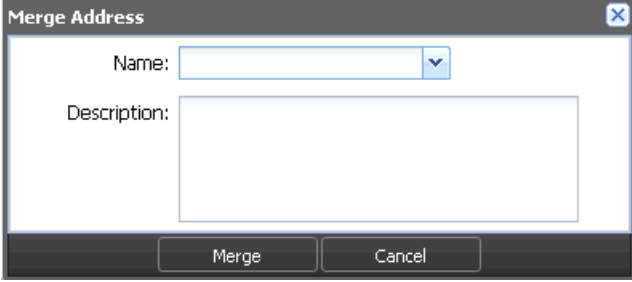
Figure 15: Page Showing Duplicate Address Objects

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
dis (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

- 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 16 on page 40](#). In the Name field, provide a new object name or select existing object names from the list.

Figure 16: Merge Address Page



The dialog box titled "Merge Address" contains a "Name:" field with a dropdown arrow and a "Description:" text area. At the bottom are "Merge" and "Cancel" buttons.

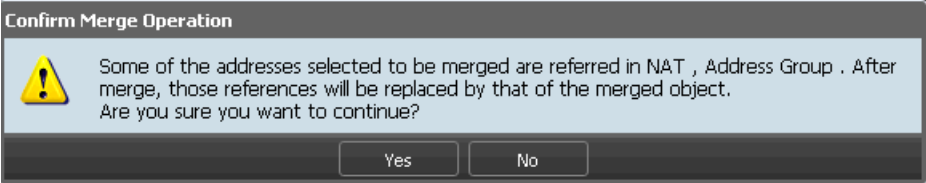


NOTE: You can merge all the objects in a group by clicking the **Merge** button after selecting all the objects by clicking the group name.



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 17 on page 40](#).

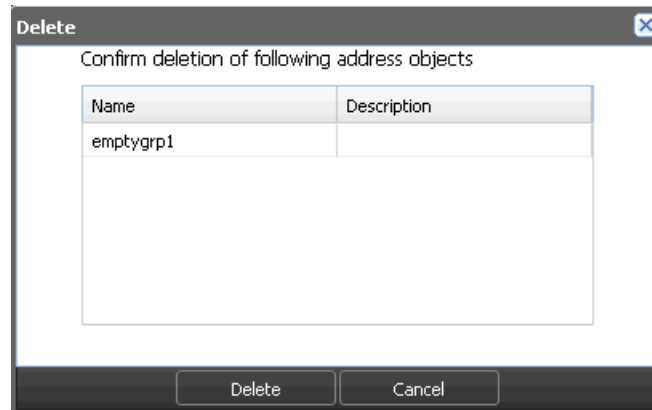
Figure 17: Merge Operation Confirmation Message



The dialog box titled "Confirm Merge Operation" features a yellow warning triangle icon. The text inside 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 are "Yes" and "No" buttons.

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 18 on page 41](#).

Figure 18: 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), as shown in [Figure 19 on page 41](#).

Figure 19: Duplicate Objects Usage Window



Procedure to manually rebuild the Index, see [“Indexing Overview” on page 247](#)

Find Address Usage

To find address usage:

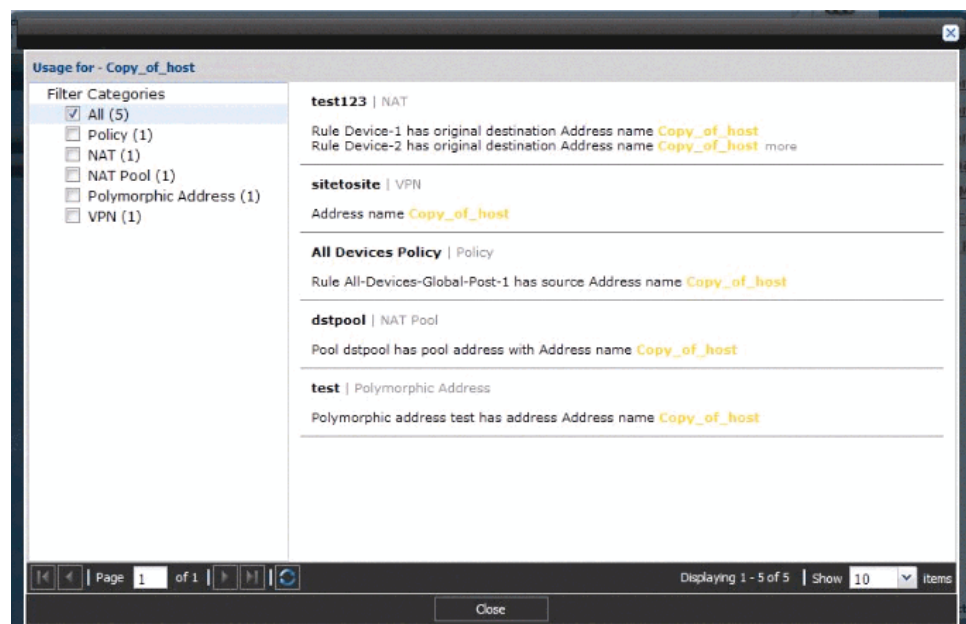
1. Select **Security Director > Object Builder > Addresses**.

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, as shown in [Figure 20 on page 42](#).

Figure 20: Window Showing Address Usage



Procedure to manually rebuild the Index, see ["Indexing Overview" on page 247](#)

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:

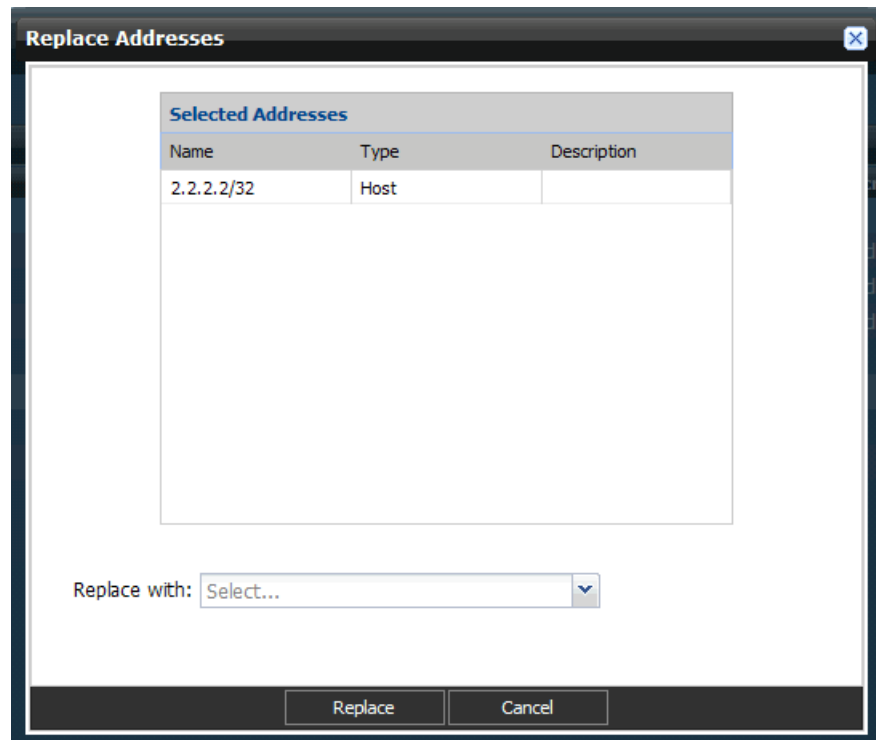
1. Select **Security Director > Object Builder > Addresses**.

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.

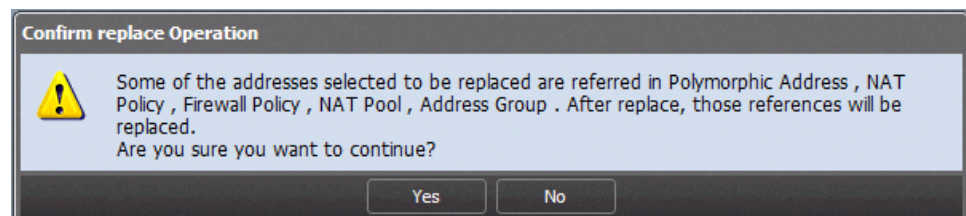
A window appears, showing the address or addresses you have selected to be replaced, along with a drop-down list of the addresses that are available to replace the address or addresses you have selected. See [Figure 21 on page 43](#).

Figure 21: Replace Addresses Window



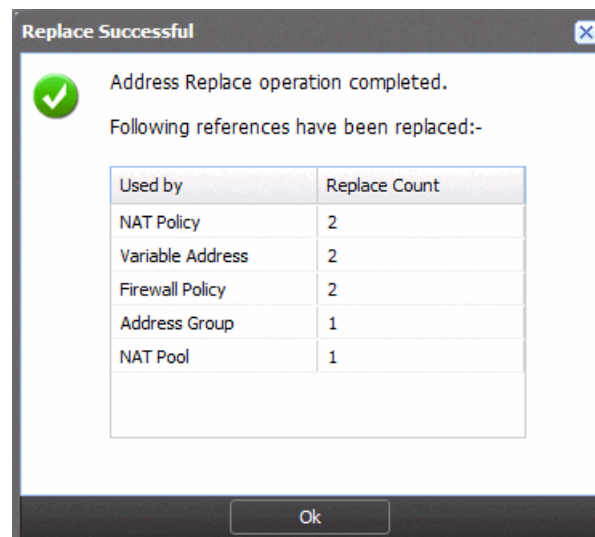
3. In the Replace Addresses window, select the address, address group, or nested address group that will replace the selected address or addresses, and click **Replace**. If the selected addresses are used in any other references, you will receive the following warning message before replacing, as shown in [Figure 22 on page 43](#). Click **Yes** to replace.

Figure 22: 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 23 on page 44](#).

Figure 23: 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.

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 drawer, 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.

Procedure to manually rebuild the Index, see [“Indexing Overview” on page 247](#)

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 drawer 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.

- Related Documentation**
- [Address and Address Groups Overview on page 35](#)
 - [Creating Addresses on page 35](#)
 - [Creating Address Groups on page 45](#)
 - [Managing Address Groups on page 46](#)

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. From the left pane, select the **Create Address Group** under Address.

The Create Address Group page appears, as shown in [Figure 24 on page 45](#).

Figure 24: 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

3. In the Name field, enter a name for the new address group.
4. In the Description field, enter a description for the new address group.
5. In the Addresses pane of the Create Address Group window, click the **Add** icon to add a new address to this address group.

The Select Addresses dialog box appears.

6. Select the addresses you want to add to the address group and click **Select**.
7. Click **Create**.

The address group appears on the Address page.

- Related Documentation**
- [Address and Address Groups Overview on page 35](#)
 - [Managing Address Groups on page 46](#)
 - [Creating Addresses on page 35](#)
 - [Managing Addresses on page 37](#)

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 46](#)
2. [Deleting an Address Group on page 46](#)
3. [Cloning an Address Group on page 47](#)

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.
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 35](#)
- [Creating Address Groups on page 45](#)
- [Creating Addresses on page 35](#)
- [Managing Addresses on page 37](#)

CHAPTER 7

Extranet Devices

- [Creating Extranet Devices on page 49](#)
- [Managing Extranet Devices on page 50](#)

Creating Extranet Devices

To create extranet devices:

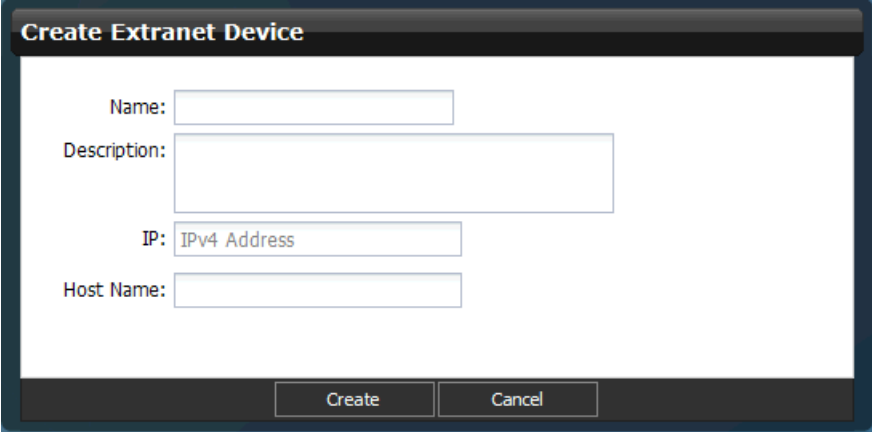
1. Select **Security Director > Object Builder > Extranet Devices**.

The Address page appears.

2. From the left pane, select the **Create Extranet Device** under Extranet Devices.

The Create Extranet Device page appears, as shown in [Figure 25 on page 49](#).

Figure 25: Create Extranet Device Page



The screenshot shows a 'Create Extranet Device' dialog box. It contains the following fields and controls:

- Name:** A text input field.
- Description:** A larger text input field.
- IP:** A text input field with the placeholder text 'IPv4 Address'.
- Host Name:** A text input field.
- Buttons:** 'Create' and 'Cancel' buttons at the bottom right.

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 50](#)

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 > Object Builder > 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 50](#)
- [Deleting an Extranet Device on page 50](#)
- [Cloning an Extranet Device on page 51](#)

Modifying an Extranet Device

To modify an extranet device:

1. Select **Security Director > Object Builder > 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 > Object Builder > 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 > Object Builder > 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 49](#)

CHAPTER 8

Application Signatures

- Creating Application Signatures on page 53
- Managing Application Signatures on page 55

Creating Application Signatures

To create an application signature:

1. Select **Security Director > Object Builder > Application Signatures**.

All application signatures that are downloaded appears on the Application Signatures page as shown in [Figure 26 on page 53](#). 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 26: Application Signatures Page

Application Signatures		DB Version 2941 (2011-12-05) Update		0 Items Selected , Total: 871 Items		Select: Page Name	Search
	Name	Category	Sub-Category	Risk	Pre-defined/Custom		
	163	Web	Portal	High	Pre-defined		
	2CH	Social-Networking		Low	Pre-defined		
	4CHAN	Social-Networking	Applications	Moderate	Pre-defined		
	4SHARED	Web	File-Sharing	Moderate	Pre-defined		
	4TUBE	Multimedia	Adult	Moderate	Pre-defined		
	9P	Infrastructure	Networking	Low	Pre-defined		
	AATK	Multimedia	Web-Based	Moderate	Pre-defined		
	ADDICTINGGAMES	Gaming	Web-Based	Low	Pre-defined		
	ADOBE-UPDATER	Infrastructure	Software-Update	Moderate	Pre-defined		
	ADRIIVE	Web	File-Sharing	Low	Pre-defined		
	ADULTFRIENDFINDER	Social-Networking	Applications	Low	Pre-defined		
	AFP	Infrastructure	File-Servers	Low	Pre-defined		
	AICOU-TIC	Infrastructure	Encryption	Low	Pre-defined		
	AIM	Messaging	Instant-Messaging	Critical	Pre-defined		
	AIMEXPRESS	Messaging	Instant-Messaging	Low	Pre-defined		
	ALLMUSIC-LOOKUP	Web	Search	High	Pre-defined		
	AMAZON	Web	Shopping	Critical	Pre-defined		
	AMEBA	Web	Blogging	Critical	Pre-defined		

2. Click **Create Application Signature**.

The Create Application Signature page appears.

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 signature type.

6. If you select Application as the signature type, enter the following information:
 - a. Select the category of the application signature from the Application Signature drop-down menu.
 - b. Select the subcategory of the application signature from the Sub-Category drop-down menu.
 - c. Select the category of risk from the Risk drop-down menu, as shown in [Figure 27 on page 54](#).



Figure 27: Create Application Signature Page

Create Application Signature

Name:

Description:

Signature type:

 Application  Nested Application

Tags

Category: Sub-Category: Risk:

Pattern-0

Signature Details

Min Data: Port Range:

CTS Pattern:

STC Pattern:

Create Cancel

- d. Enter appropriate information in the Min Data field.
 - e. Enter the range of ports in the Port Range field.
 - f. Enter appropriate information in the CTS Pattern field.
 - g. Enter appropriate information in the STC Pattern field.
 - h. Click **Create**.
7. If you select Nested Application as the signature type, enter the following information.
 - a. Select the category of the application signature from the Application Signature drop-down menu.
 - b. Select the subcategory of the application signature from the Sub-Category drop-down menu.

- c. Select the category of risk from the Risk drop-down menu.
- d. Click the check box next to the Chain Order field if you want to do so.
- e. Enter the range of ports in the Max Transactions field.
- f. Select the type of protocol from the Protocol drop-down menu.
- g. Select the context of the signature from the Context drop-down menu.
- h. Select the direction from the Direction drop-down menu.
- i. Enter appropriate information in the Pattern field.
- j. Click the Add Signature button to add more signatures.
- k. Click **Create**.

Related Documentation • [Managing Application Signatures on page 55](#)

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 > Object Builder > 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 55](#)
- [Modifying Application Signatures on page 56](#)
- [Deleting Application Signatures on page 56](#)
- [Cloning Application Signatures on page 56](#)
- [Creating an Application Signature Group on page 57](#)

Filtering Application Signatures

To filter application signatures:

1. Select **Security Director > Object Builder > 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, and Risk, Predefined/Custom, Object Type, Activation Date, and Modify Date. Every parameter has different subparameters.

2. Click the check box next to the subparameters within a parameter.

Modifying Application Signatures

To modify application signatures:

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

4. Click **Modify**.

Deleting Application Signatures

To delete application signatures:

1. Select **Security Director > Object Builder > 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. 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 > Object Builder > 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 Create Application Signature page. You can create the application signature here.

Creating an Application Signature Group

To create an application signature group:

1. Select **Security Director > Object Builder > 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 include in the application signature group.
3. Right-click the application signature group and select **Create Application Group**.

The Create Application Signature Group page appears.

4. Enter a name for the application signature group in the Name field.
5. Click the check box next to the Disable option if you want to disable this application signature group.
6. Click the **Add** icon to add more application signatures to this group.

The Application Signature Selector window appears. You can add more application signatures from this window.

7. Click **Update**.
8. Click **Create**.

CHAPTER 9

Schedulers

- [Scheduler Overview on page 59](#)
- [Creating a Scheduler on page 60](#)
- [Managing Scheduler on page 62](#)

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 60](#)

- [Managing Scheduler on page 62](#)

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 > Object Builder > Scheduler**.

The main Scheduler page appears, as shown in [Figure 28 on page 60](#).

Figure 28: 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, startTime=00:00, stopTime=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, startTime=00:00, stopTime=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, startTime=00:00, stopTime=12:00, TUESDAY, Exclude=false, AllDay=false, startTime=00:00, stopTime=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, startTime=00:00, stopTime=12:00, startTime=14:00, stopTime=16:00

2. Click the plus sign (+) to create a new scheduler. The Create Scheduler window appears, as shown in [Figure 29 on page 61](#).

Figure 29: 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: Start Time2:

Stop Time1: 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 &, <, >, 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 59](#)
 - [Managing Scheduler on page 62](#)

Managing Scheduler

You can modify, delete, and clone a scheduler listed on the Scheduler main page.

To open the Scheduler page:

- Select **Security Director > Object Builder > 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 62](#)
- [Deleting a Scheduler on page 62](#)
- [Find Scheduler Usage on page 63](#)
- [Show Unused Schedulers on page 63](#)

Modifying a Scheduler

To modify a scheduler:

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

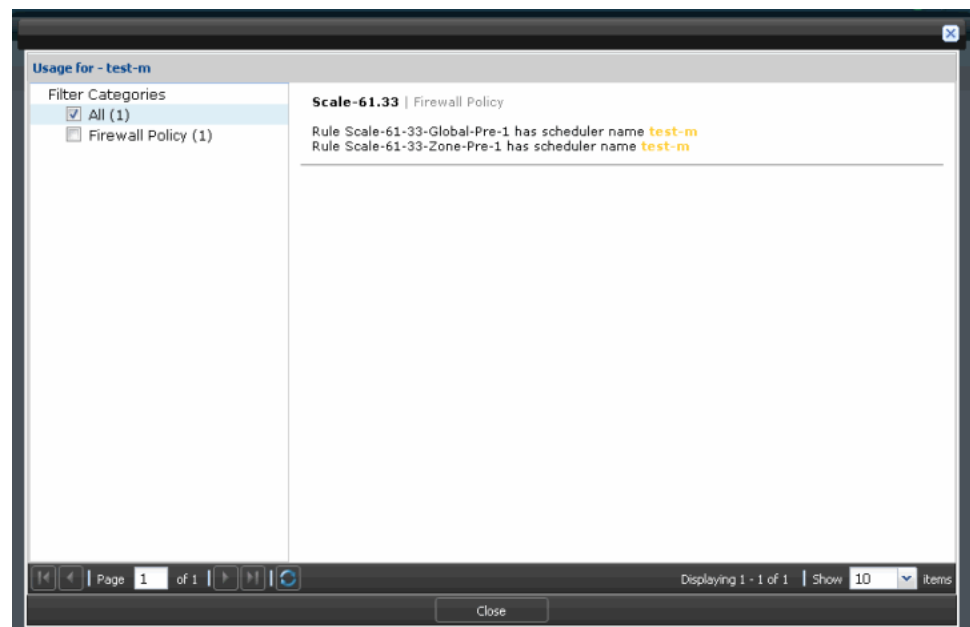
1. Select **Security Director > Object Builder > Scheduler**.

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 30 on page 63](#).

Figure 30: Scheduler Find Usage Window



Show Unused Schedulers

To show unused schedulers:

1. Select **Security Director > Object Builder > 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 59](#)
 - [Creating a Scheduler on page 60](#)

CHAPTER 10

NAT Pools

- [Creating NAT Pools on page 66](#)
- [Managing NAT Pools on page 69](#)

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 > Object Builder > 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 31 on page 66](#).



Figure 31: Create NAT Pool Page

Create NAT Pool

Name:

Description:

Pool Type:

Pool Address:  

Routing Instance

Device:

Routing Instance:

Advanced

Host Address Base:

Translation:

Overflow Pool Type:

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 you select Port/Range in the Translation menu, a new menu, Port, appears.
 - Select an appropriate option from the Port menu.
 - If you select Overload in the Translation menu, a new option, Port Overloading Factor, appears.
 - Select an appropriate value from the Port Overloading Factor selector.
12. Select the appropriate option from the Overflow Pool Type menu.
 - If you select Pool in the Overflow Pool Type menu, a new field, Overflow Pool, appears.
 - Select the appropriate NAT pool from the Overflow Pool selector.
13. Click **Create**.

To create an address group:

1. Click the second plus sign (+) to create the new address object. [Figure 32 on page 68](#) shows the page that appears.

Figure 32: Inline Address Group Creation for NAT Pool

Create NAT Pool

Name:

Description:

Addresses:

Available		Selected
10.159.2.0/25 (10.159.2.0...	<input type="button" value="Up"/> <input type="button" value="Down"/>	
10.159.3.0/24 (10.159.3.0...	<input type="button" value="Up"/> <input type="button" value="Down"/>	
10.159.4.0/24 (10.159.4.0...	<input type="button" value="Up"/> <input type="button" value="Down"/>	
64.34.14.0/24 (64.34.14.0...	<input type="button" value="Up"/> <input type="button" value="Down"/>	
64.4.111.0_27 (64.4.111....	<input type="button" value="Up"/> <input type="button" value="Down"/>	
64.5.145.253 (64.5.145.2...	<input type="button" value="Up"/> <input type="button" value="Down"/>	
64.5.195.25 (64.5.195.25)	<input type="button" value="Up"/> <input type="button" value="Down"/>	

Page 1 of 1

☐ Host ☐ Network ☐ Wildcard ☐ Range ☐ Other

2. In the Name field, enter the name of an address group.
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 Create NAT Pool window.



NOTE: You can create address object inline similar to address group inline.

Related Documentation

- [NAT Overview on page 201](#)
- [Managing NAT Pools on page 69](#)
- [Creating NAT Policies on page 205](#)

- [Managing NAT Policies on page 230](#)

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 > Object Builder > 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 69](#)
- [Modifying NAT Pools on page 69](#)
- [Cloning NAT Pools on page 70](#)
- [Show Duplicate NAT Pools on page 70](#)
- [Find NAT Pool Usage on page 72](#)
- [Replace Addresses on page 73](#)
- [Show Unused NAT Pools on page 74](#)
- [Delete All Unused NAT Pools on page 75](#)

Deleting NAT Pools

To delete a NAT pool:

1. Select **Security Director > Object Builder > 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 > Object Builder > 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 > Object Builder > 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 > Object Builder > 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 33 on page 71](#).

Figure 33: Show Duplicates of NAT Pool

Object Builder > NAT Pools > **Show Duplicates**

[Return To NAT Pool View](#)

Name	Pool Address	Pool Type	Description	
nat_171_182_211_61 (3 members) Merge				
<input checked="" type="checkbox"/> nat_171_182_211_61	h_171.182.211.61	Destination		
<input checked="" type="checkbox"/> dst_pool_171_182_211_61	h_171.182.211.61	Destination		
<input type="checkbox"/> dst_pool_171_182_211_61	h_171.182.211.61	Destination		
dst_pool_171_182_210_169 (3 members) Merge				
<input type="checkbox"/> dst_pool_171_182_210_169	h_171.182.210.169	Destination		
<input type="checkbox"/> dst_pool_171_182_210_169	h_171.182.210.169	Destination		
<input type="checkbox"/> nat_171_182_210_169	h_171.182.210.169	Destination		

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

A merge window appears, as shown in [Figure 34 on page 71](#). In the Name field, provide a new object name or select existing object names from the list.

Figure 34: Merge NAT Pool

Merge NAT Pool ✕

Name: ▼

Description:

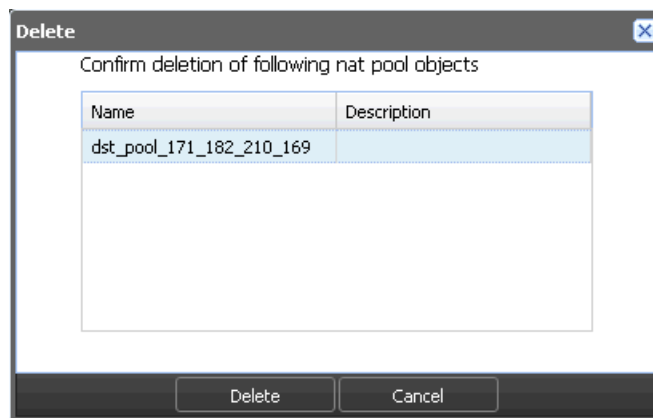
Merge Cancel



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.

- 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 35 on page 72](#).

Figure 35: Delete Duplicate NAT Pool Objects

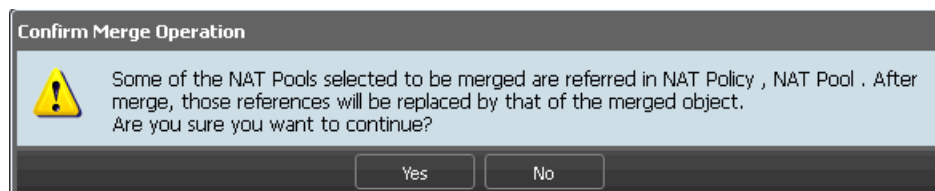


Click **Delete** to delete the selected objects or **Cancel** to cancel the deletion.

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 36 on page 72](#).

Figure 36: Confirm Merge Operation



Procedure to manually rebuild the Index, see "[Indexing Overview](#)" on page 247

Find NAT Pool Usage

To find address usage:

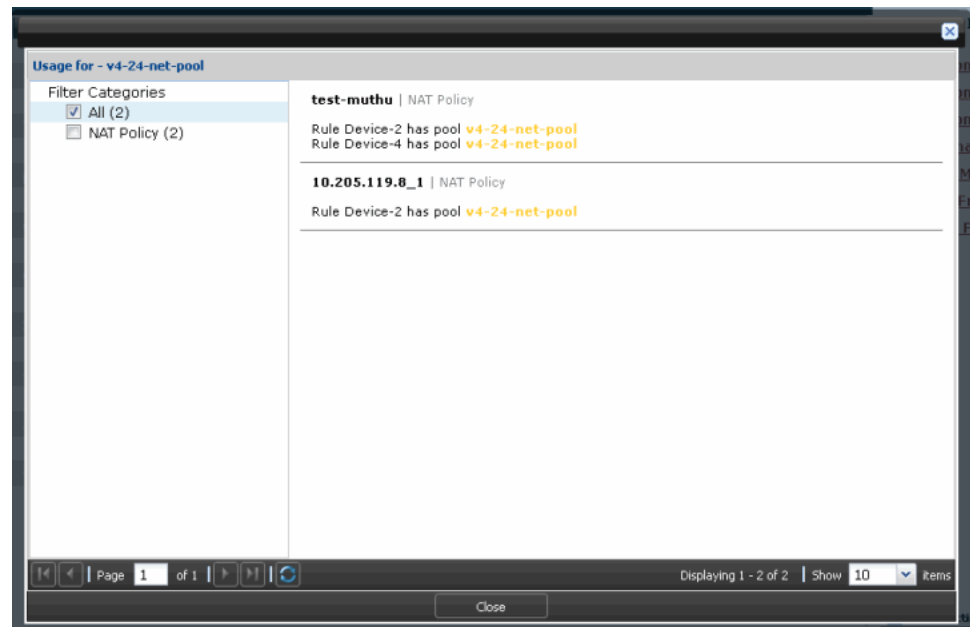
1. Select **Security Director > Object Builder > NAT Pools**.

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 37 on page 73](#).

Figure 37: NAT Pool Usage Window



Procedure to manually rebuild the Index, see [“Indexing Overview” on page 247](#)

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:

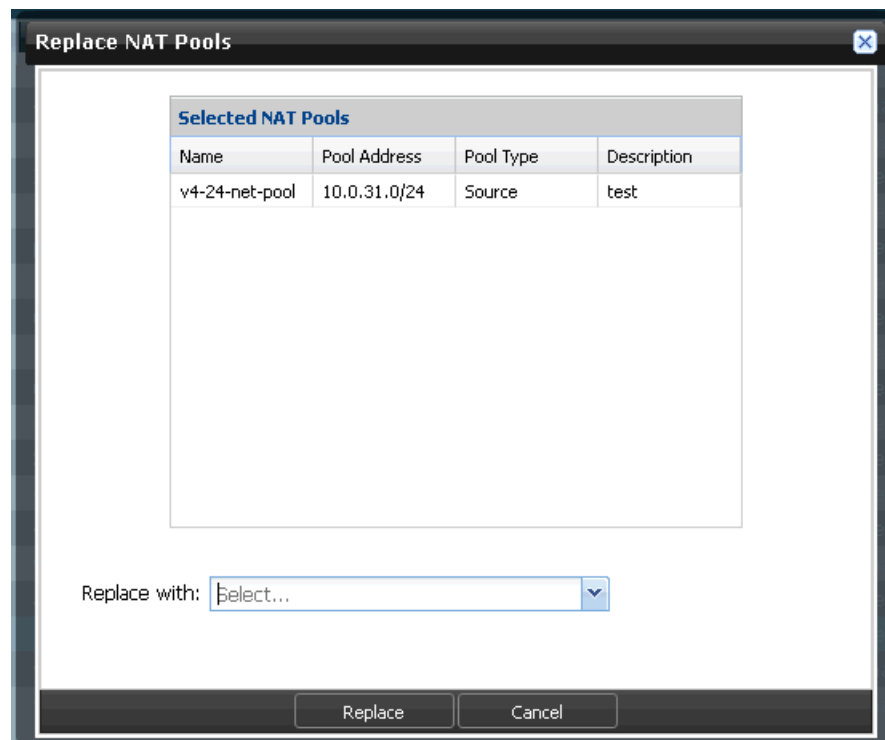
1. Select **Security Director > Object Builder > NAT Pools**.

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 38 on page 74](#).

Figure 38: 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 > Object Builder > 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 247](#)

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 201](#)
- [Creating NAT Pools on page 66](#)
- [Creating NAT Policies on page 205](#)
- [Managing NAT Policies on page 230](#)

CHAPTER 11

Policy Profiles

- [Security Policy Profiles Overview on page 77](#)
- [Creating Policy Profiles on page 78](#)
- [Managing Policy Profiles on page 81](#)

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 78](#)
- [Managing Policy Profiles on page 81](#)

Creating Policy Profiles

To create a security policy profile:

1. Select **Security Director > Object Builder > 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 39 on page 78](#).

Figure 39: New Policy Profile Page

New Policy Profile

Name:

Description:

Template:

Logging | **Authentication** | **Advanced Settings**

☐ Log At Session Init

☐ Log At Session Close

☐ Enable Count

Alarm Threshold:

0 Bytes/Second

0 Kilobytes/Minute

Create Cancel

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.
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 40 on page 80](#).
 - 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 40: 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 77](#)
 - [Managing Policy Profiles on page 81](#)

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 > Object Builder > 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 81](#)
- [Modifying Policy Profiles on page 81](#)
- [Cloning Policy Profiles on page 82](#)

Deleting Policy Profiles

To delete a policy profile:

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

CHAPTER 12

VPN Profiles

- [VPN Profiles Overview on page 83](#)
- [Creating VPN Profiles on page 84](#)
- [Managing VPN Profiles on page 87](#)

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 84](#)
- [Managing VPN Profiles on page 87](#)

Creating VPN Profiles

To create a VPN profile:

1. Select **Security Director > Object Builder > 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 41 on page 84 shows the Phase 1 tab.

Figure 41: VPN Profile: Phase 1

The screenshot shows the 'VPN Profile' configuration window with the 'Phase 1' tab selected. The 'Name' field contains 'vp1' and the 'Description' field is empty. Below the tabs, the 'Authentication Type' is set to 'Preshared Key'. The 'Mode' section has 'Main' selected. The 'Proposals' section has 'Predefined' selected, with 'Basic' selected under the predefined options. The 'Advanced Settings' section is expanded, showing 'Enable NAT Traversal' checked, 'Keep Alive Interval(secs)' set to 5, 'Enable DPD' checked, 'Always Send DPD' unchecked, 'DPD Interval(secs)' set to 10, and 'DPD Threshold' set to 5. At the bottom 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
7. Select the VPN mode that you want to use by clicking the radio buttons next to Mode.

- 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. You can create only custom VPN proposal.
 - 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.
 - d. Select the appropriate authentication mechanism from the Authentication drop-down menu.
 - e. Select the appropriate encryption mechanism from the Encryption drop-down menu.
 - f. Select the life time interval from the Life Time (in seconds) selector.
 - g. Click **Create**.
 9. Expand the Advanced Settings pane by clicking the down arrow.

You can configure the advanced settings for Phase 1 here.
 10. Select the **Enable NAT Traversal** check box to enable this option.
 11. Select the appropriate keepalive interval from the Keep Alive Interval (secs) selector.
 12. Select the **Enable DPD** check box if you want to use this option.
 13. Select the **Always Send DPD** check box if you want to use this option.
 14. Select the appropriate dead peer detection interval from the DPD Interval (secs) selector.
 15. Select the appropriate dead peer detection threshold from the DPd Threshold selector.
 16. Click the **Phase 2** tab.

[Figure 42 on page 86](#) shows the Phase 2 tab.

Figure 42: VPN Profile: Phase 2

17. 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 43 on page 86](#).

Figure 43: Create Phase 2 Proposal

- Enter name of the custom proposal in the Name field.
- Select the authentication from the Authentication drop-down menu.

- Select the required protocol from the Protocol drop-down menu.
- Select the necessary encryption from the Encryption drop-down menu.
- 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.

18. Select an appropriate option from Perfect Forward Privacy drop-down menu.
19. Expand the Advanced Settings pane by clicking the down arrow.
20. Select the **Establish tunnel immediately** check box if you want to enable this option.
21. Select the **Enable VPN Monitor** check box if you want to enable this option.
This is a per-VPN option.
22. Select the appropriate option from the DF Bit drop-down menu.
23. Select the appropriate idle time interval from the Idle time (secs) selector.
24. Select the appropriate value from the Install Time selector.
25. Select the **Enable Anti Replay** check box if you to enable this option.
26. Click **Create**.

**Related
Documentation**

- [VPN Profiles Overview on page 83](#)
- [Managing VPN Profiles on page 87](#)

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 > Object Builder > 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 88](#)
- [Modifying VPN Profiles on page 88](#)
- [Cloning VPN Profiles on page 88](#)

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 > Object Builder > 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 > Object Builder > 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 83](#)
- [Creating VPN Profiles on page 84](#)

CHAPTER 13

Variables

- [Creating Variable Definitions on page 91](#)
- [Managing Variable Definitions on page 94](#)

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 Polymorphic Object page appears, as shown in [Figure 44 on page 92](#). You can create a variable definition on this page.



Figure 44: Create Polymorphic Object Page


Create Polymorphic Object



Name:


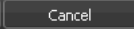
Description:

Type: ☒ Address ☐ Zone

Default Address:  

	Context Value	Address
		

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**.

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

1. Click the second plus sign (+) to create the new address group. [Figure 45 on page 93](#) shows the page that appears.

Figure 45: Inline Address Group Creation for a Polymorphic Object

Create Polymorphic Object

Name:

Description:

Addresses:

Available	Selected
10.159.2.0/25 (10.159.2.0...	
10.159.3.0/24 (10.159.3.0...	
10.159.4.0/24 (10.159.4.0...	
64.34.14.0/24 (64.34.14.0...	
64.4.111.0_27 (64.4.111....	
64.5.145.253 (64.5.145.2...	
64.5.195.25 (64.5.195.25)	

Page 1 of 1

☐ Host ☐ Network ☐ Wildcard ☐ Range ☐ Other

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 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 94](#)

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 94](#)
- [Modifying Variable Definitions on page 95](#)
- [Cloning Variable Definitions on page 95](#)

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**.

Template Definitions

- [Creating Template Definitions on page 97](#)
- [Managing Template Definitions on page 98](#)

Creating Template Definitions

To create a Template Definition:

1. Select **Security Director > Object Builder > Manage Template Definitions**.

The Manage Template Definitions page appears. This page displays all the template definitions you have created.

2. Click **Create Template Definition** icon.

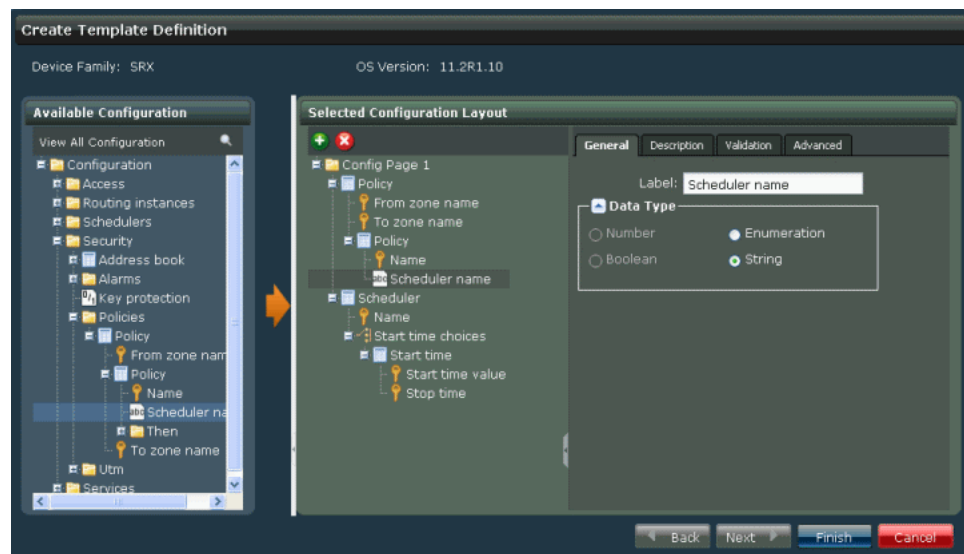
The Create Template Definition page appears.

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 46 on page 98](#).

Figure 46: 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 98](#)

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 > Object Builder > 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 99](#)
- [Modifying Template Definitions on page 99](#)

Deleting Template Definitions

To delete a template definition:

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

Templates

- [Creating Templates on page 101](#)
- [Managing Templates on page 102](#)

Creating Templates

To create a template:

1. Select **Security Director > Object Builder > Manage SD Templates**.

The Manage SD Templates page appears. This page displays all the templates you have created.

2. Click **Create 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 47 on page 102](#).

Figure 47: 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 102](#)

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 > Object Builder > 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 102](#)
- [Modifying Templates on page 103](#)

Deleting Templates

To delete a template:

1. Select **Security Director > Object Builder > 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 > Object Builder > 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 4

Firewall Policy

- [Firewall Policy on page 107](#)

CHAPTER 16

Firewall Policy

- [Firewall Policies Overview on page 107](#)
- [Multiple Group Policy Membership Overview on page 110](#)
- [Global Address Book Overview on page 114](#)
- [Creating Firewall Policies on page 117](#)
- [Unlocking Locked Policies on page 132](#)
- [Inline Creation of Objects in Policy on page 134](#)
- [Policy Priority Precedence Setting on page 139](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Publishing Firewall Policies on page 149](#)
- [Managing Firewall Policies on page 155](#)

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.

- **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
- 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.



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.
- 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.

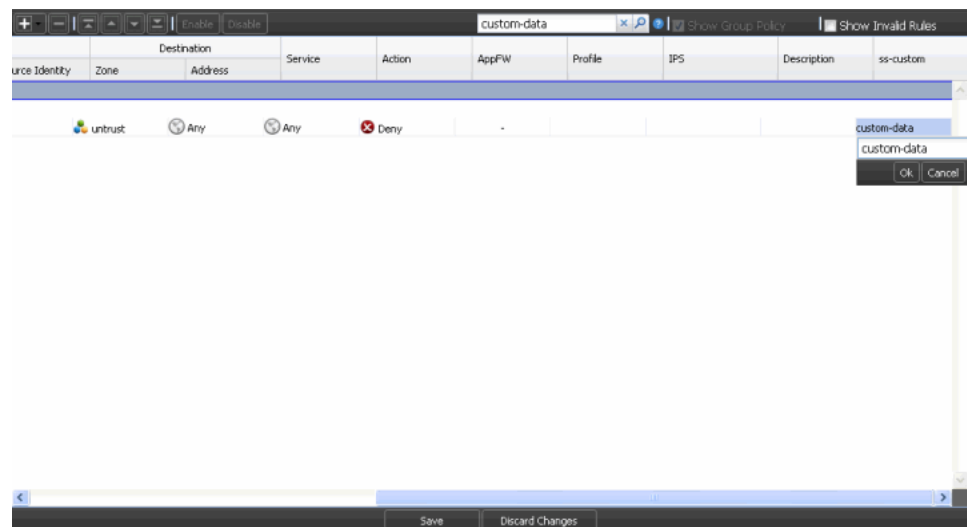
Custom Column Overview

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.

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.

Figure 48: Custom Column Data Search



Related Documentation

- [Creating Firewall Policies on page 117](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Managing Firewall Policies on page 155](#)
- [Publishing Firewall Policies on page 149](#)

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. 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 49: Sorting Order in the Firewall Policy Left Pane

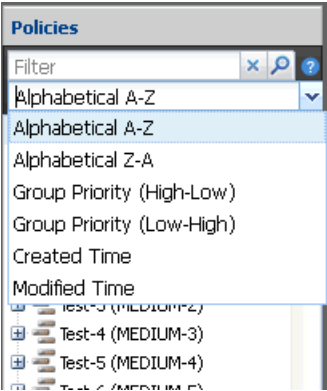


Table 3 on page 111 shows the different sorting orders available for firewall policies.

Table 3: 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.

Table 3: Sorting Order for Firewall Policies (*continued*)

Sorting Order	Description
Modified Time	Last modified policies are placed at the bottom (last).

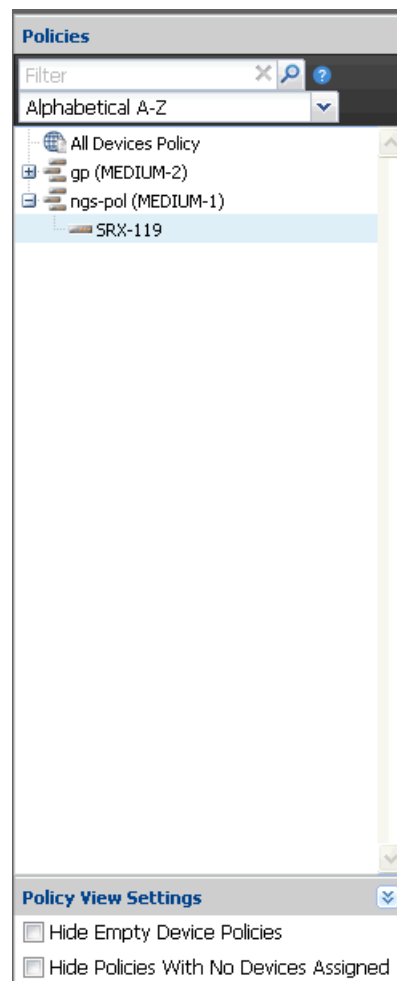


NOTE: You cannot set the precedence value greater than the available precedence values that are assigned to the available priority policies. Based on the priority of the policies, the precedence values are applied.

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 50 on page 113](#). 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 50: 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 50 on page 113](#).
3. Policies without any assigned devices are hidden in the left pane.

**Related
Documentation**

- [Managing Firewall Policies on page 155](#)
- [Policy Priority Precedence Setting on page 139](#)
- [Publishing Firewall Policies on page 149](#)

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 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.

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 4 on page 115 gives the migration matrix covering all scenarios:

Table 4: 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 107](#)
 - [Creating Firewall Policies on page 117](#)
 - [Managing Firewall Policies on page 155](#)

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 two 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 51 on page 117](#).

Figure 51: Firewall Policy Tabular View

S.No.	Name	Zone	Source	Destination	Service	Action
Zone (5 rules)						
Device Rules (5 rules)						
1	cs03-asa5510	trust	cs03-prv	untrust	RTP-Cisco-192-1	Tunnel
2	asa5510-cs03	untrust	RTP-Cisco-192-1	trust	cs03-prv	Tunnel
3	rtp-to-cs03	tunnel31	rtp-prv-10-160	trust	cs03-prv	Permit
4	cs03-to-rtp	trust	cs03-prv	tunnel31	Juniper_Skrm	Permit
5	cs03-prv	trust	cs03-prv	untrust	rtp-prv-10-160	Permit
All Devices Post Rules (0 rule)						
Global (2 rules)						
Device Rules (2 rules)						
1	cp-quad-zero	--	quad-zero	--	Any	Deny
2	default-deny-rule	--	Any	--	Any	Deny

The right pane of the firewall policy Inventory Landing Page (ILP) 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. Click **Create Policy** from the left pane.

The Create Policy page appears. You can create a group policy or a device policy on this page.

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. By default, the Manage Zone Policy option is selected and used to manage zone-based firewall rules.
- d. Select **Manage Global Policy** to manage the global firewall rules for SRX Series devices.

You can select either one or both options. Security Director does not allow you to unselect both options.

- e. To set the priority for a policy, select **High**, **Medium**, or **Low** from the Priority list.
- f. Enter a Precedence value less the number of existing policies of the same priority. The number of existing policies are displayed as part of the Precedence field.

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

- g. Select the profile for the group policy from the Profile menu.
- h. Select the IPS mode from the IPS Configuration Mode menu.
- i. Click the **Show Assigned Devices** check box to make the devices on which policies have been configured available for selection.
- j. 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 52 on page 119](#).

Figure 52: Create Firewall Policy

By default, all devices appear under Select Devices tab whether or not they have been assigned to an all devices policy. To see which devices are unassigned, select the **Show only devices without policy assigned** option to see the devices that are not assigned to an all devices policy.

k. 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.
 - b. Enter a description for the device policy in the Description field.
 - c. Select the profile for the device policy, from the Profile list.
 - d. Select the IPS mode from the IPS Configuration Mode list. The following [Table 5 on page 120](#) shows different IPS configuration modes and the purpose:

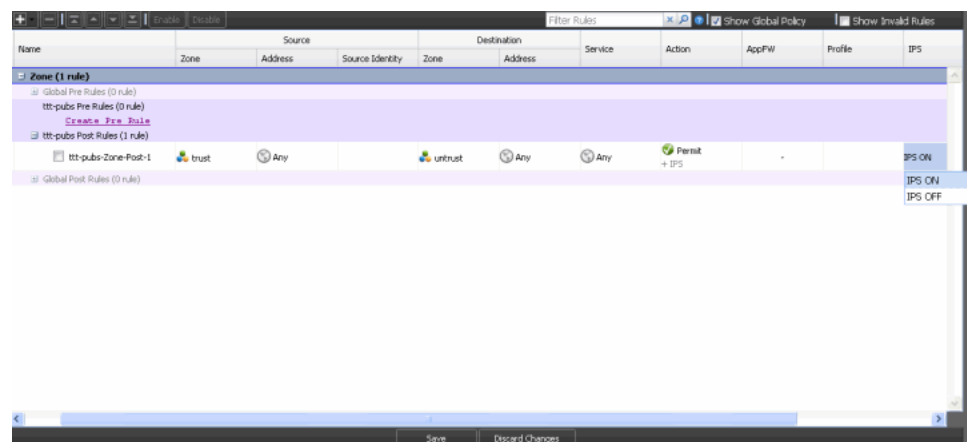
Table 5: IPS Configuration Mode

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.

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 53 on page 120](#). This is available for each rule and you can set on or off only for advanced and basic modes.

Figure 53: 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.

All these IPS modes are available for logical systems also.

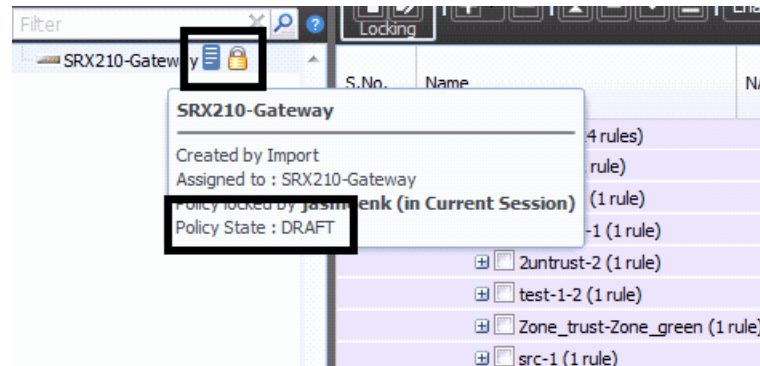
- e. Select the device on which the device policy will be published from the Device list.
- f. Click **Create**.

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 54 on page 121](#); 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 54: 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.

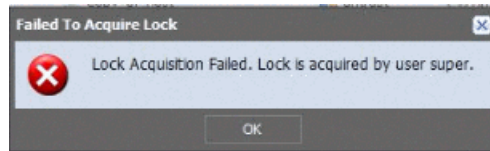


NOTE: SRX Series logical systems support complete firewall policy configuration in Security Director. The captive portal is configured in the root logical system and referred from the user logical system. If IPS policy is assigned to a logical system, it enables only the basic IPS mode. When the logical system is published, you'll received 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 51 on page 117](#). 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 55 on page 122](#).

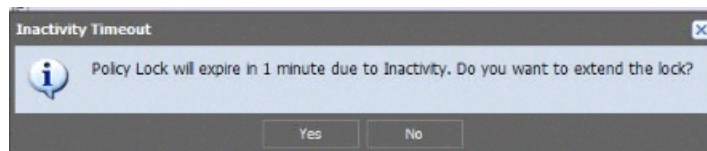
The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

Figure 55: Lock Failure Error Message for the Second User



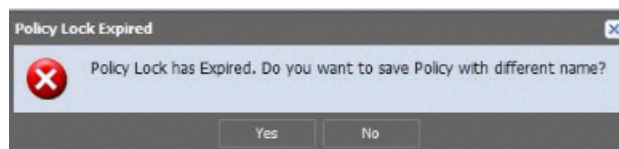
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 56 on page 122](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see [“Unlocking Locked Policies” on page 132](#)

Figure 56: Inactivity Timeout Error



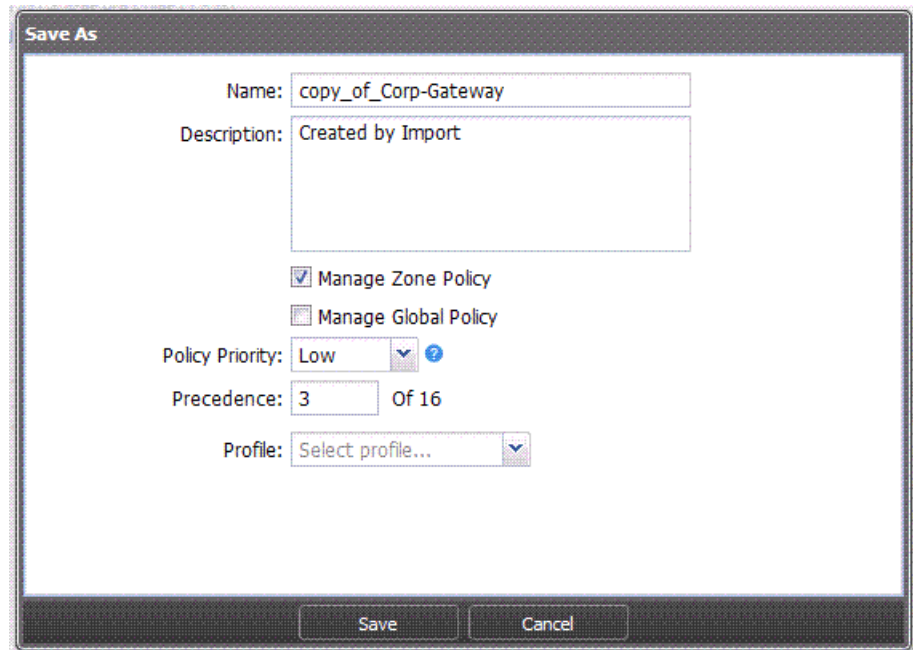
Click **Yes** to extend the locking period. If you click **No**, and if there is activity on the policy within the last minute of the lock's life, the timer will be reset and the lock will not be released. If you ignore the message, when the policy lock timeout interval expires 1 minute later, you are prompted to either save the edited policy with a different name or lose the changes, as shown in [Figure 57 on page 122](#).

Figure 57: Policy Lock Expired Message



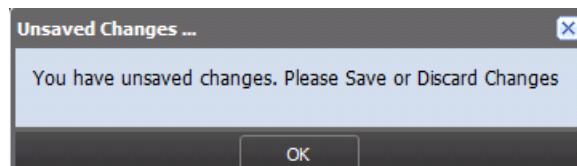
If you click **Yes** to save the edited policy with a different name, the following window appears, as shown in [Figure 58 on page 123](#). If you navigate away from the locked policy, you will get an option to save the edited policy with different name.

Figure 58: Save the Edited Policy with a Different Name



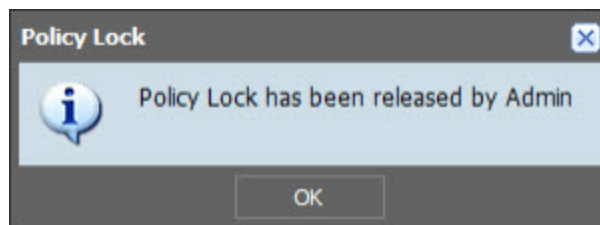
After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 59 on page 123](#).

Figure 59: Unsaved Changes Warning Message

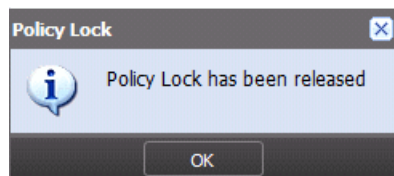


If Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 60 on page 123](#).

Figure 60: 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 61 on page 124](#).

Figure 61: 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.

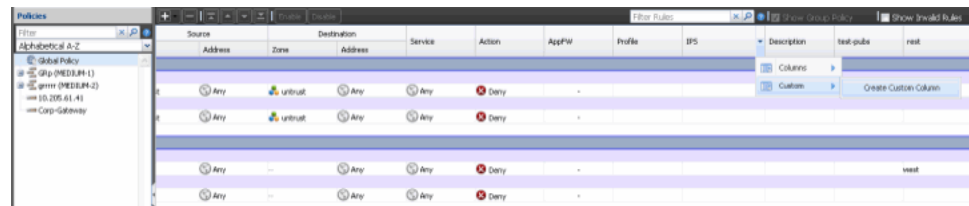
To create a custom column definition for the firewall policy:

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 62: 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 63: 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 64: Create Custom Column Confirm Page

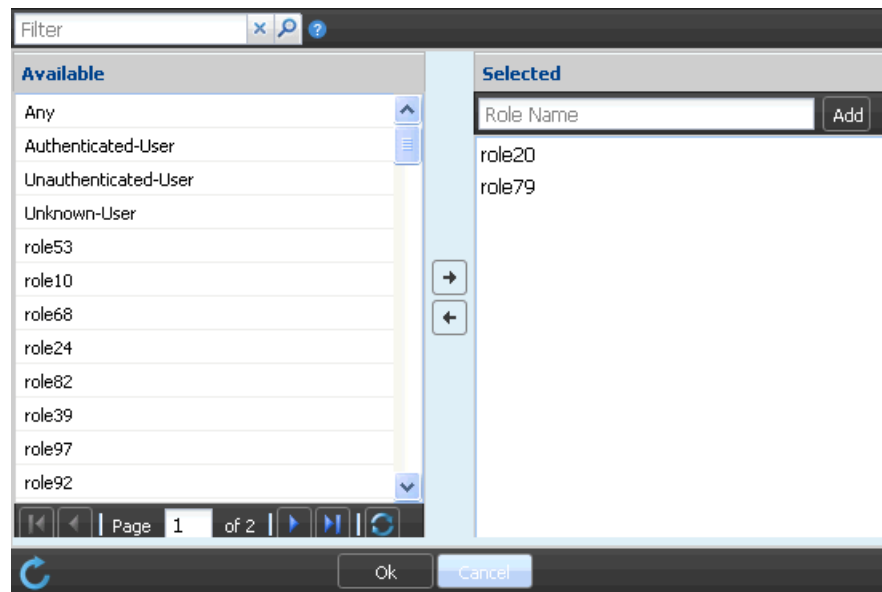
The Infranet Controller (IC) maps users to roles based on the information provided by an authentication server. For example, a user could be mapped to a role based on membership in Active Directory groups.

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 65 on page 126](#).

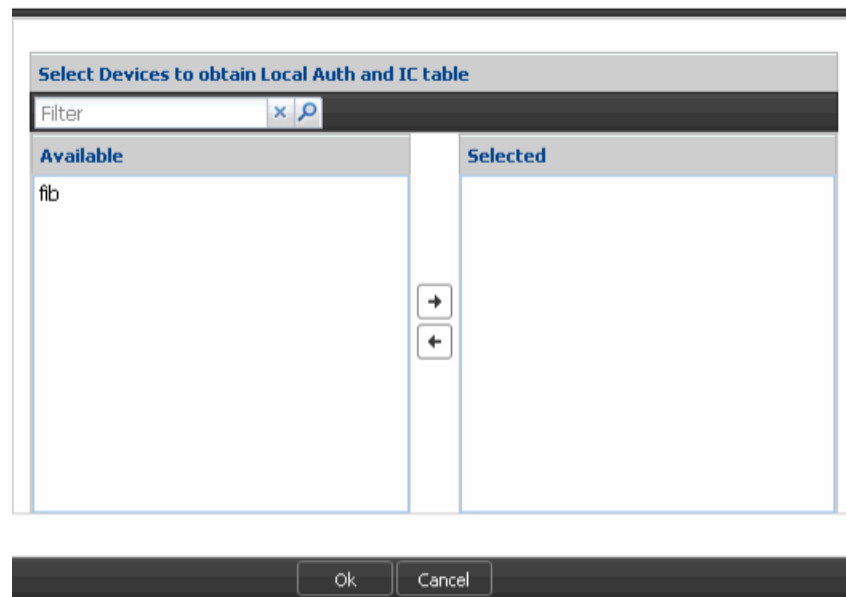
Figure 65: Source Identity Page



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 66 on page 127](#).

Figure 66: Select Devices Page



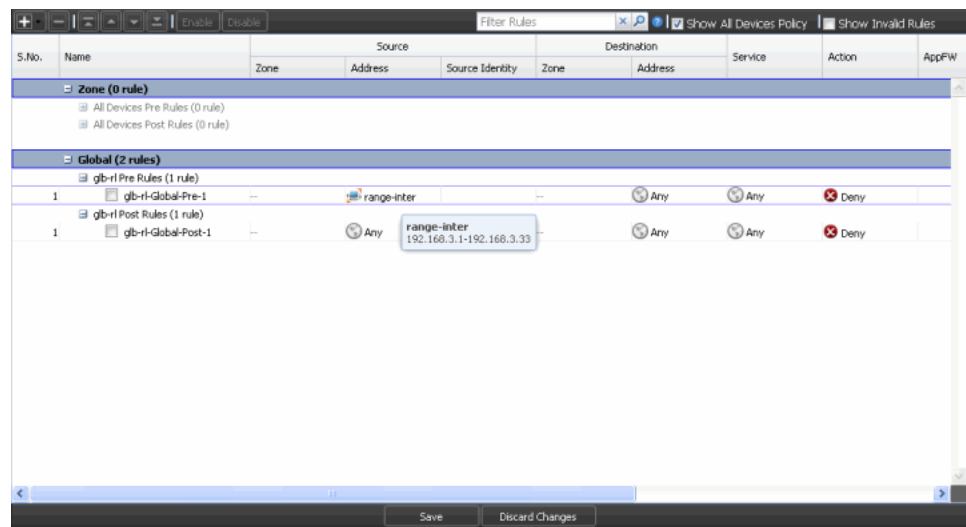
Security Director maintains a list of roles available for a group or for individual devices. You can manually retrieve the available roles from a single SRX Series device or from multiple SRX Series devices.



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 67 on page 128](#). For address group, the tooltip shows details regarding its members.

Figure 67: 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 6 on page 128](#)

Table 6: 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 6: 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 68 on page 129](#).

Figure 68: Advanced Search Dialog for Firewall Policies

Advanced Search

Rule Name:

Source

Zone:

Address:

Destination

Zone:

Address:

Service:

Action:

IPS:

Description:

Custom Columns

c1:

Filter Reset Cancel

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 7 on page 131 explains certain specific Security Director search behavior.

Table 7: 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 8 on page 131 shows example search results for different parameters.

Table 8: 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 8: 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 107](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Managing Firewall Policies on page 155](#)
- [Publishing Firewall Policies on page 149](#)
- [Unlocking Locked Policies on page 132](#)

Unlocking Locked Policies

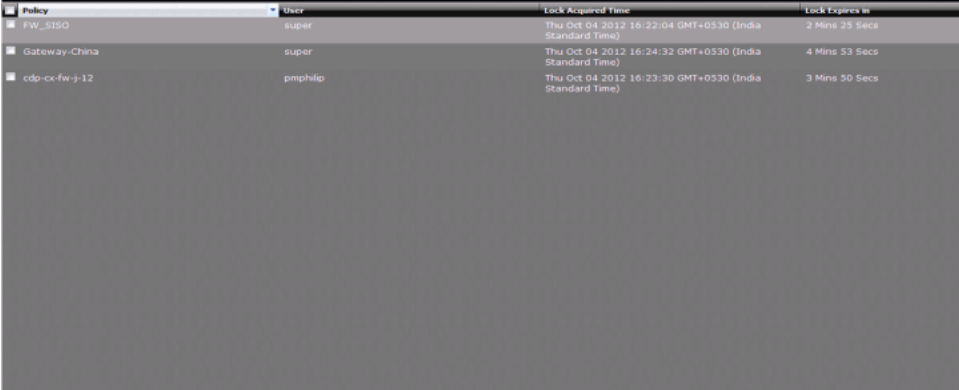
All the locked policies can be viewed in a single page. This page is available for a user having Manage Policy Locks tasks assigned. This page shows all the locks only if the user has Unlock task assigned, other wise user will see only his locks. To view the locked policies:

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 69: Firewall Policy: Manage Policy Locks



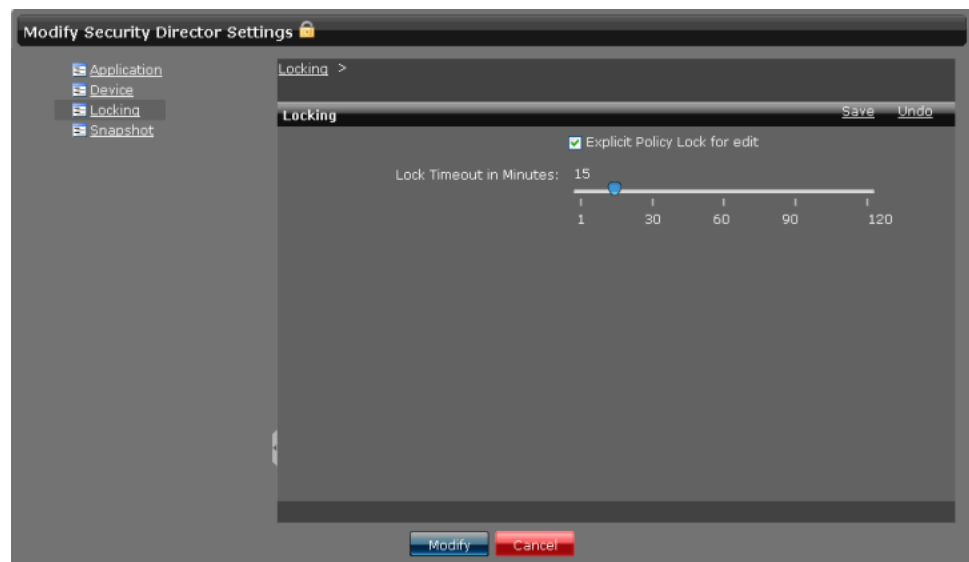
Policy	User	Lock Acquired Time	Lock Expires in
FW_S150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 25 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilo	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	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 70 on page 133](#).

Figure 70: 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 117](#)
- [Managing Firewall Policies on page 155](#)

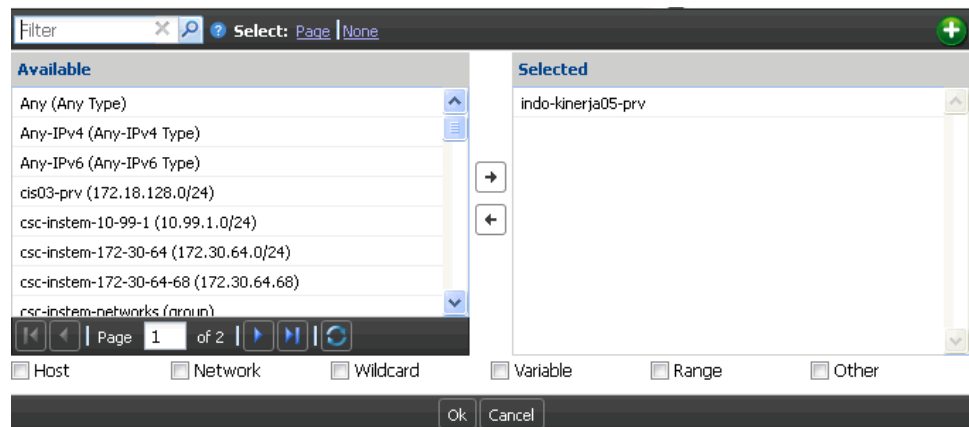
Inline Creation of Objects in Policy

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 71 on page 134](#) 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 71: Inline Address Object Creation in the Source Address Window



- Click the plus sign (+) to create the new address object or address group. By default, the Address radio button is selected

Figure 72 on page 135 shows the page that appears.

Figure 72: Inline Address Object Create Page

Create Address Object

Object Type: ☒ Address ☐ Address Group

Name:

Description:

Type:

IP Get IP Get Hostname

The Type can be Host, Range, or Network.

- 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 73: Address Selector Page Showing the New Inline Object

Filter Select: Page | None

Available

- 10.0.254.96 (10.0.254.96)
- 10.0.254.96/27 (10.0.254.96/27)
- 10.10.0.0/16 (10.10.0.0/16)
- 10.10.1.2 (10.10.1.2) **Selected**
- 10.10.11.10 (10.10.11.10)
- 10.10.11.11 (10.10.11.11)
- 10.10.11.12 (10.10.11.12)
- 10.10.11.9 (10.10.11.9)

Selected

- 10.10.1.2

Page 1 of 107

☐ Host ☐ Network ☐ Wildcard ☐ Variable ☐ Range ☐ Other

To create address group:

1. Select the Address Group radio button to create the new address group. [Figure 74 on page 136](#) shows the page that appears.

Figure 74: Inline Address Group Creation

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 address selector.

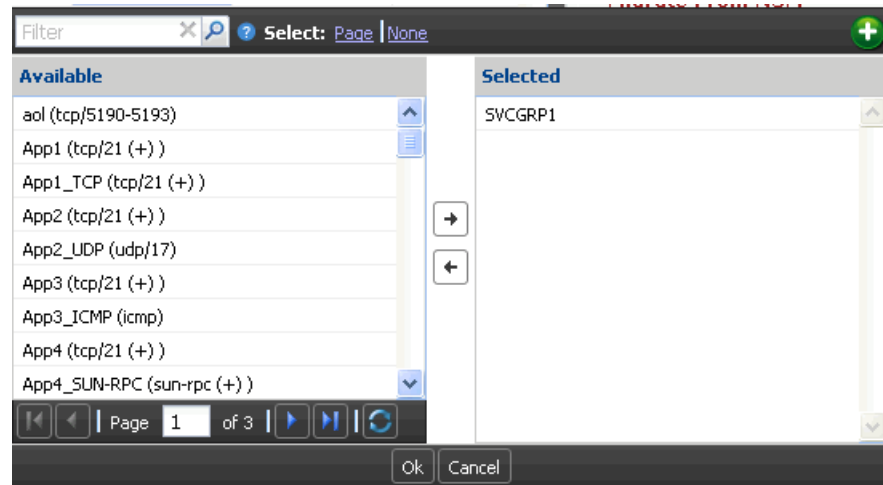


NOTE: Follow the same steps to create objects for the destination address.

To create objects for a service:

1. Click the Service column. Figure 75 on page 137 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 75: Inline Service Object Creation in the Service List



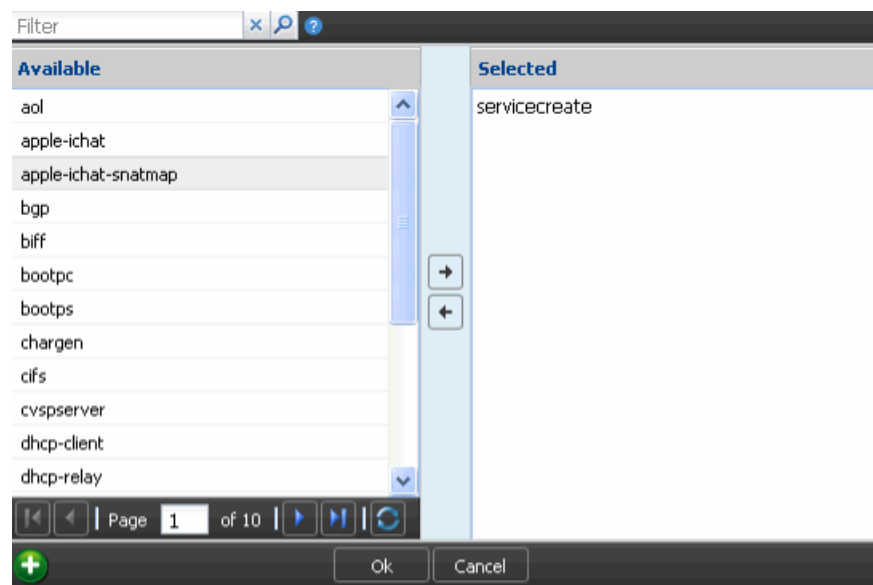
2. Click the plus sign (+) to create objects for the service.

Figure 76: Inline Service Object Creation Page

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 77: Service Selector Page Showing the New Object



4. Click **Cancel** to discard your changes and return to the service selector.

**Related
Documentation**

- [Firewall Policies Overview on page 107](#)
- [Managing Firewall Policies on page 155](#)

Policy Priority Precedence Setting

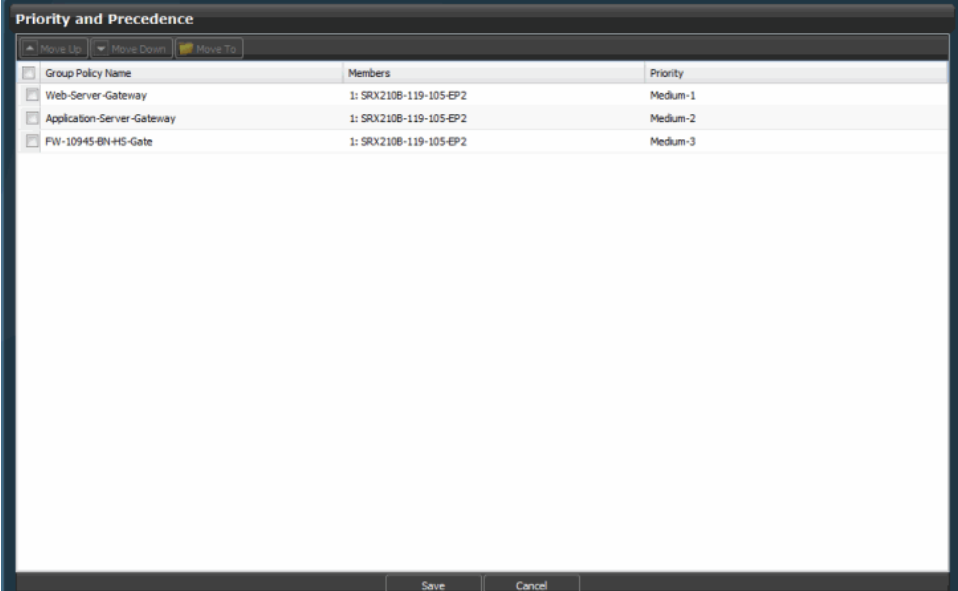
To change the priorities and precedences of different policies simultaneously:

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

The Priority and Precedence page appears with all the group policy names. The page contains the following fields:

- Group Policy Name—Name of the group policies.
- Members—Devices attached to the individual group policies. For example: 1:10.205.119.8 indicates that there is only one device attached to the group policy, and the device name or IP address is 10.205.119.8.
- Priority—Priority of the group policy (Low, Medium, or High).

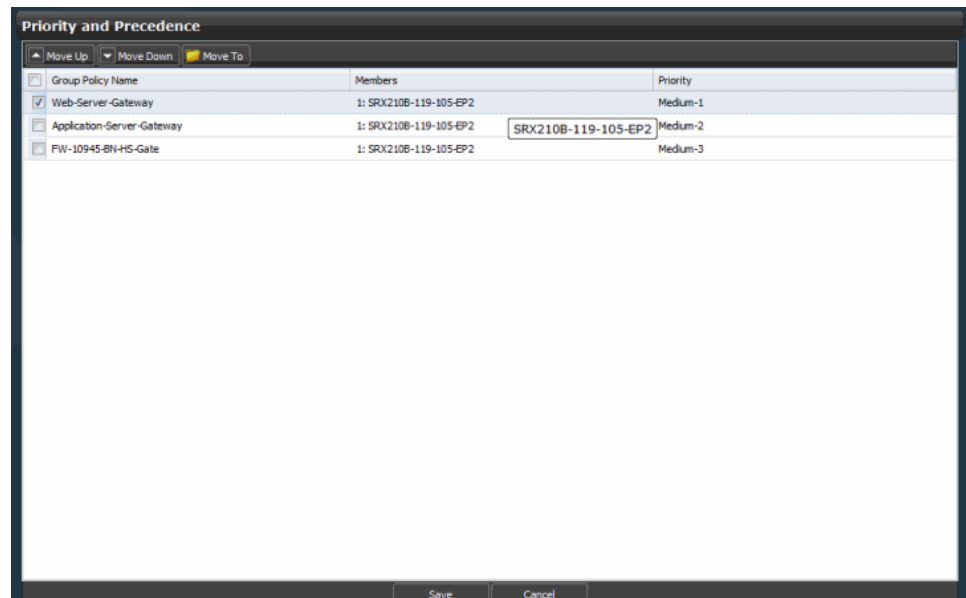
Figure 78: Policy: Priority And Precedence Page



Group Policy Name	Members	Priority
Web-Server-Gateway	1: SRX210B-119-105-EP2	Medium-1
Application-Server-Gateway	1: SRX210B-119-105-EP2	Medium-2
PW-10945-6N+HS-Gate	1: SRX210B-119-105-EP2	Medium-3

The tool tip is provided to list the number of devices attached to any group policy. Move the mouse over the Members column to get the tool tip, as shown in [Figure 79 on page 140](#).

Figure 79: Priority Precedence Tool Tip



2. Select any group policy and right-click the selected policy. The following options shown in [Table 9 on page 141](#) are provided to move the priority up or down or to change the precedence and priority simultaneously.

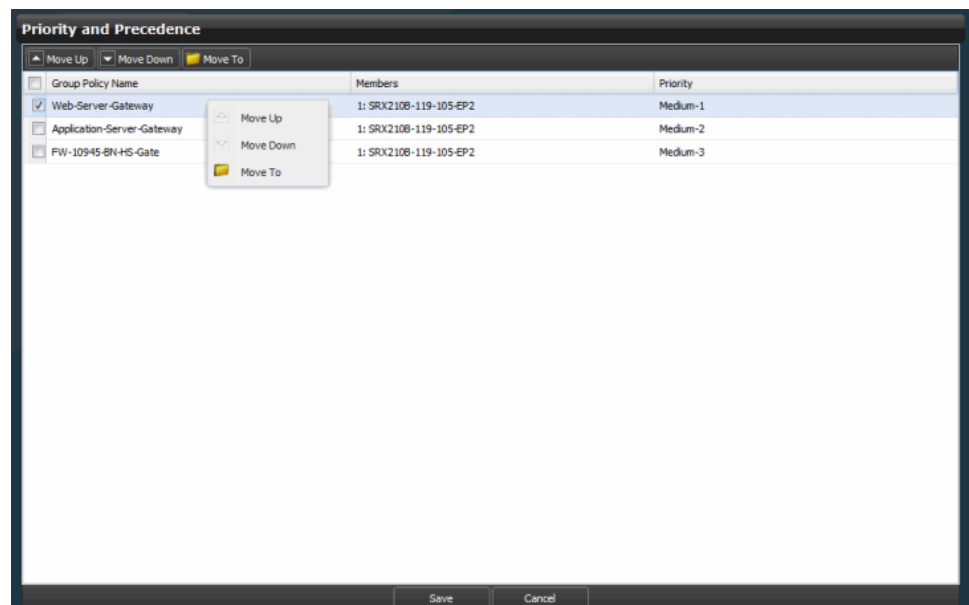
Table 9: Priority and Precedence for Firewall Policies

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"> • 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. • 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. • 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. <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"> • 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.

Table 9: Priority and Precedence for Firewall Policies (*continued*)

Options	Description
Move To	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.

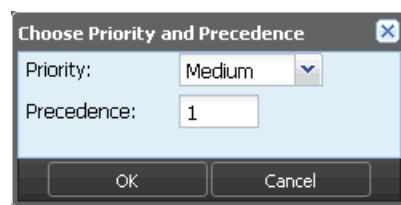
Figure 80: Priority And Precedence Right-Click Page



NOTE: If multiple policies are selected, all the policies are moved one-by-one to the given priority and precedence slot sequentially.

- Click **Move To** to provide precedence value.

Figure 81: Setting Priority And Precedence Value Page



- 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 110](#)
 - [Managing Firewall Policies on page 155](#)

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:

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

The Policy Tabular view appears.

2. Click the security policy you want to add rules to from the left pane.

The existing rules of the security policy are displayed in the right pane.

3. 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 **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.

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.

6. Click the **Source Address** field in the rule.

The address selector appears.

7. Select the addresses you want to associate the rule to, from the Available column.
8. Click the right arrow in the address selector.

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.

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.

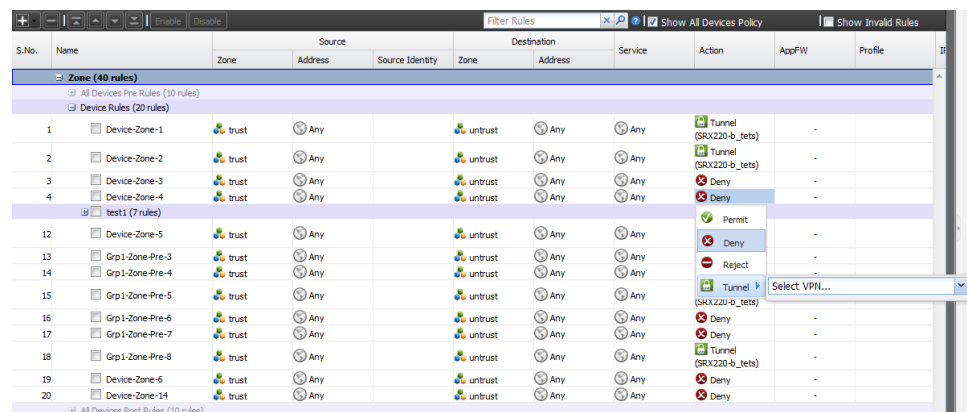
18. Click **OK**.

19. Click the **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 82 on page 144](#).

Figure 82: 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.

20. 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.

21. 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. 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 83 on page 145](#).

Figure 83: TCP-Session Options

The screenshot shows a 'Custom Settings' dialog box. At the top, 'Profile Type' has four radio button options: 'None', 'Inherit Profile From Policy', 'Select Another Profile', and 'Custom' (which is selected). Below this is a 'Template' dropdown menu. There are three tabs: 'Logging', 'Authentication', and 'Advanced Settings' (which is active). Under 'Advanced Settings', there are three settings: 'Datacenter SRX Acceleration' with a checkbox for 'Services Offload' (unchecked), 'Destination Address Translation' with a dropdown set to 'None', and 'Redirect' with a dropdown set to 'None'. Below these is a section titled 'TCP-Session Options' containing two checkboxes: 'TCP-SYN Check' and 'TCP Sequence Check', both of which are unchecked. At the bottom are 'Ok' and 'Cancel' buttons.

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.
-

22. Click **Rule Options** to assign a scheduler for a rule. Select the required scheduler from the Scheduler field, and click **OK**.

For the rules with an expired scheduler, a warning message appears during the Publish workflow.

23. 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.

24. Click the **Description** field and enter a description for the security policy.

25. Click **Save**.

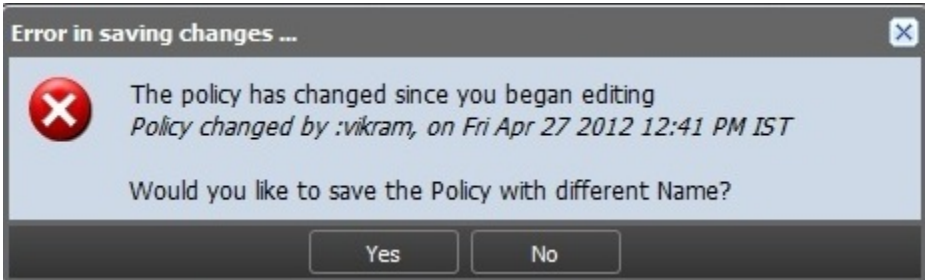


NOTE: You should click **Save** to save any changes you have made to the firewall policy. While in the process of making changes to the firewall policy, If you click any of the tasks in the task ribbon before saving the firewall policy changes, all changes you have made will be lost. If you click anywhere 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 84 on page 147](#) appears.

Figure 84: 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 107](#)
- [Creating Firewall Policies on page 117](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Managing Firewall Policies on page 155](#)
- [Publishing Firewall Policies on page 149](#)

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.

Icon Name	Description
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.

Related Documentation

- [Firewall Policies Overview on page 107](#)
- [Creating Firewall Policies on page 117](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Managing Firewall Policies on page 155](#)
- [Publishing Firewall Policies on page 149](#)

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 **Security Director > Firewall Policy > 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.

- Click the **Schedule at a later time** check box if you want to schedule and publish the configuration later, as shown in [Figure 85 on page 150](#).

Figure 85: Policy Publish Page

Name	Publish State	Description	Priority	Precedence
All Devices Policy	Not Published	Predefined Policy for all devices	-	-
gls-ft	Not Published		Medium	1
gls-ft-zn	Not Published		Medium	2

☒ Include IPS Policy
☒ Schedule at a later time
 Date and Time: 04/16/12 1:29 PM IST

Back Next Publish Publish and Update Cancel

- Click **Next**.

The Affected Devices page displays the devices on which the policies will be published as shown in [Figure 86 on page 150](#).

Figure 86: Devices on Which the Policies Will Be Published

Name	Managed Status	Connection Status	Services	Configuration
longzhou	In Sync	Up	Global Policy	View

☒ Include IPS Policy
☒ Schedule at a later time
 Date and Time: 03/20/12 12:35 PM IST

Back Next Publish Publish and Update Cancel

- 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 87 on page 151](#).

Figure 87: Policy Publish: CLI Configuration

```

Generated Configuration for device srx100-3
CLI Configuration | IPS Configuration

##Security Policy Settings##
set security policies policy-match
##Security Firewall Policy - trust - untrust##
set security policies from-zone trust-to-zone untrust
set security policies from-zone trust-to-zone untrust policy group-1-Pre-2 match application any
set security policies from-zone trust-to-zone untrust policy group-1-Pre-2 match destination-address any
set security policies from-zone trust-to-zone untrust policy group-1-Pre-2 match source-address any
set security policies from-zone trust-to-zone untrust policy group-1-Pre-2 then deny
insert security policies from-zone trust-to-zone untrust policy group-1-Pre-2 before policy Device-1
##Security Firewall Policy - global ##
set security policies global
set security policies global policy group-1-Pre-Global-2 match application any
set security policies global policy group-1-Pre-Global-2 match destination-address any
set security policies global policy group-1-Pre-Global-2 match source-address any
set security policies global policy group-1-Pre-Global-2 then deny
set security policies global policy global-device-1 match application any
set security policies global policy global-device-1 match destination-address any
set security policies global policy global-device-1 match source-address any
set security policies global policy global-device-1 then deny
insert security policies global policy group-1-Pre-Global-2 before policy global-device-0
insert security policies global policy global-device-1 before policy global-device-0

```

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 88 on page 151](#).

Figure 88: Device Validation Warning Message

```

Preview Policy Configuration for Device - 10.205.119.109
CLI Configuration | IPS Configuration

[Warning]: Number of services in rule: Global-Zone-Pre-1 is 255. This exceeds the maximum number of recommended services in a rule for this device which is 128.
[Warning]: Number of addresses in rule: Global-Zone-Pre-1 is 1,105. This exceeds the maximum number of recommended addresses in a rule for this device which is 512.

```

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 89](#) on page 152.

Figure 89: Policy Publish: LSYS Device CLI Configuration

```

Firewall Policy Configuration For Device - scale-lsys1
CLI Configuration  IP Configuration
##Entering User LSYS context##
edit logical-systems scale-lsys1
##Entering User LSYS context##
exit
##Captive Portal Settings##
set services unified-access-control captive-portal captiveportal_32797 redirect-traffic all
##Entering User LSYS context##
edit logical-systems scale-lsys1
##Security Firewall Policy : trust - untrust##
set security policies from-zone trust to-zone untrust policy ge-Zone-Pre-1
delete security policies from-zone trust to-zone untrust policy ge-Zone-Pre-1
set security policies from-zone trust to-zone untrust policy Device-Zone-1 match application any
set security policies from-zone trust to-zone untrust policy Device-Zone-1 match destination-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-1 match source-address any
set security policies from-zone trust to-zone untrust policy Device-Zone-1 then permit application-services uac-policy captive-portal captiveportal_32797
##Entering User LSYS context##
exit
  
```



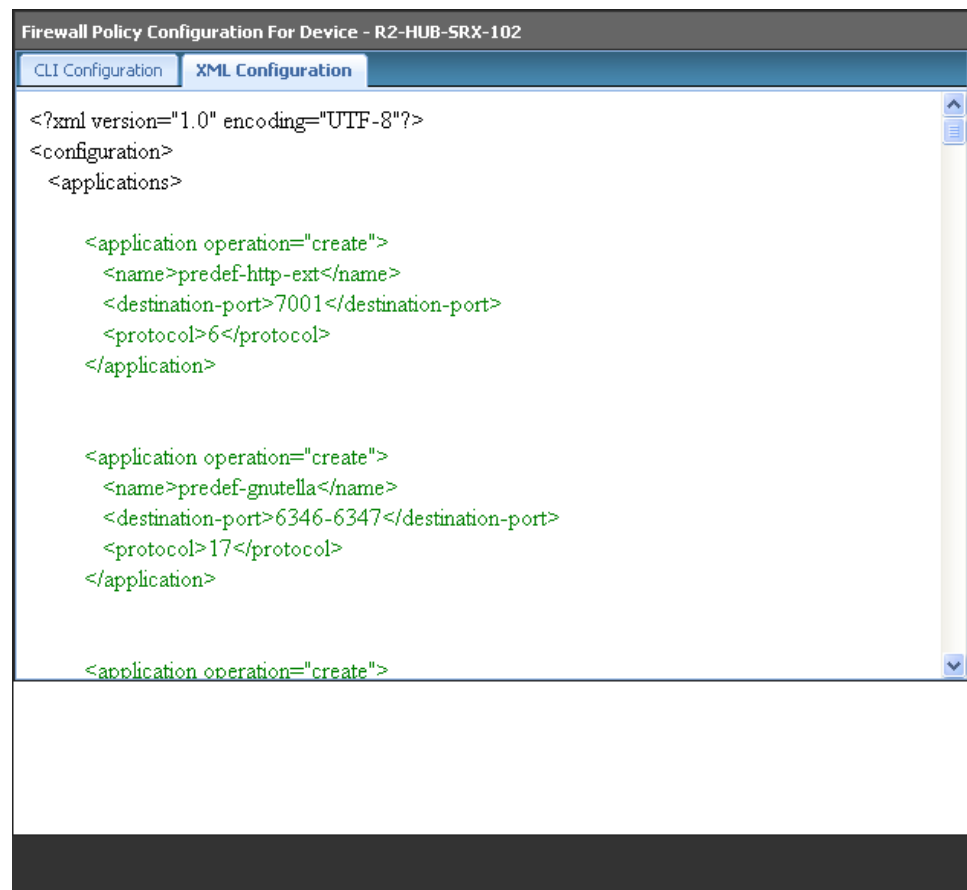
NOTE: Captive portal setting can be configured only at the root logical system and referenced only in the user logical system.



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 90](#) on page 153.

Figure 90: 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.

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.

Related Documentation

- [Firewall Policies Overview on page 107](#)
- [Creating Firewall Policies on page 117](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Managing Firewall Policies on page 155](#)

Managing Firewall Policies

You can modify, delete, clone, or export security policies listed in 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 156](#)
2. [Comparing Firewall Policies on page 158](#)
3. [Deleting Firewall Policies on page 159](#)
4. [Adding Rules to a Firewall Policy on page 160](#)
5. [Cloning Firewall Policies on page 160](#)
6. [Promoting a Firewall Policy on page 161](#)
7. [Exporting a Firewall Policy on page 161](#)
8. [Policy Versioning on page 162](#)
9. [Managing Policy Versioning on page 164](#)
10. [Deleting Rules in a Firewall Policy on page 169](#)
11. [Cloning a Rule in a Firewall Policy on page 169](#)
12. [Grouping Rules in a Firewall Policy on page 170](#)
13. [Enabling/Disabling Rules in a Firewall Policy on page 170](#)
14. [Expanding/Collapsing All Rules in a Firewall Policy on page 171](#)
15. [Cutting/Copying and Pasting Rules or Rule Groups in a Firewall Policy on page 171](#)
16. [Assigning Devices to a Firewall Policy on page 172](#)
17. [Deleting Devices from a Firewall Policy on page 173](#)
18. [Rule Operations on the Filtered Rules on page 173](#)
19. [Managing Custom Column Data on page 175](#)
20. [Modifying Custom Columns Definitions on page 175](#)
21. [Deleting a Custom Columns Definition on page 176](#)
22. [Exporting a Custom Columns Definition on page 176](#)

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 91: Modify Policy Page

Edit Policy

Name: Gateway-BNG

Description: Created by Import

☒ Manage Zone Policy

☐ Manage Global Policy

Policy Priority: Low

Precedence: 4 Of 15

Profile: Select profile...

IPS Configuration Mode: ☒ None ☐ Basic ☐ Advanced

Modify

Cancel

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 10 on page 157](#) shows the precedence value that can be set for different priorities.

Table 10: 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
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:

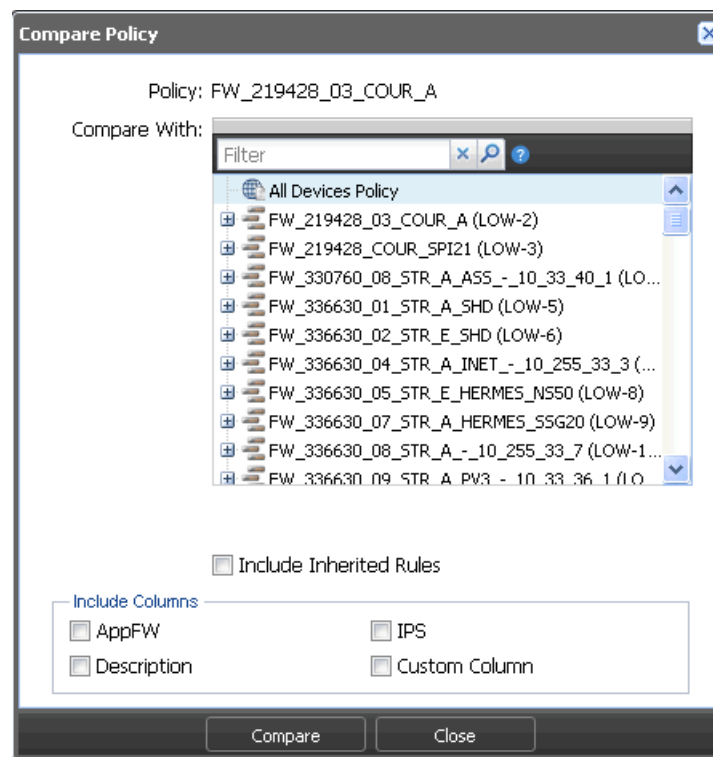
1. Select **Security Director > Firewall Policy**.

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 92 on page 158](#).

Figure 92: 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 93 on page 159](#).

Figure 93: 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:

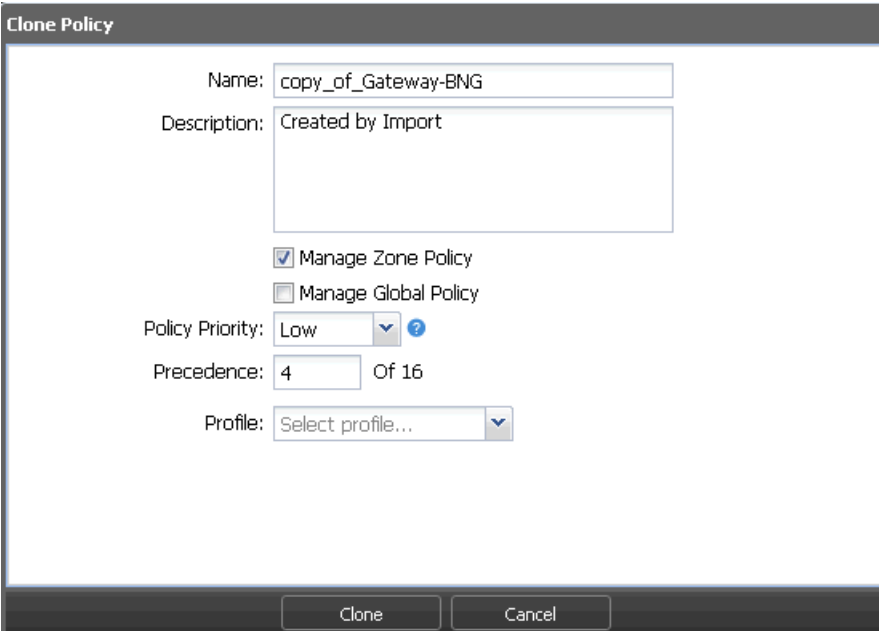
1. Select **Security Director > Firewall Policy**.

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 94: Clone Policy Page



The image shows a 'Clone Policy' dialog box with the following fields and controls:

- Name:** A text input field containing 'copy_of_Gateway-BNG'.
- Description:** A text input field 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 blue information icon to its right.
- Precedence:** A text input field 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 95 on page 161](#).

Figure 95: 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 97 on page 164](#). 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:

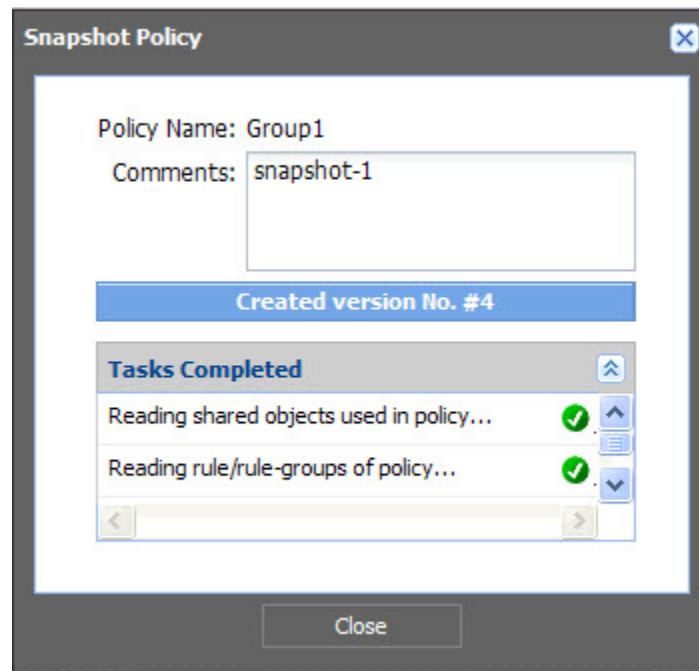
1. Select **Security Director > Firewall Policy**.

The Policy Tabular view appears.

2. Right-click the firewall policy you want to take a snapshot of, and select **Snapshot Policy**.

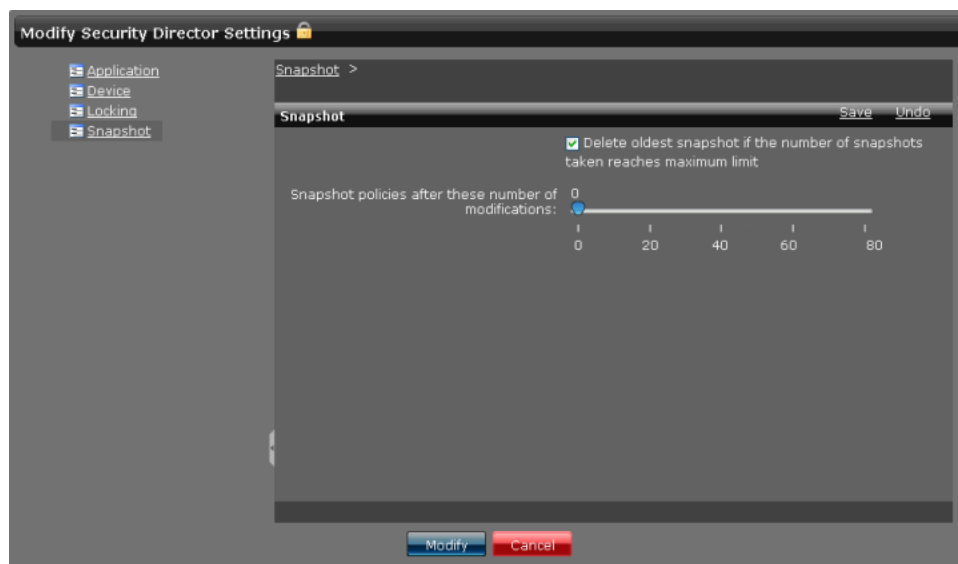
The Policy Name field shows the name of the firewall policy for which the snapshot is taken. Enter your comments in the Comments field, and press **Create to take the snapshot**. The Snapshot Policy Window appears, showing the status of the version as it is created, [Figure 96 on page 163](#).

Figure 96: Snapshot Policy Window



**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 97 on page 164](#). When the snapshot is taken automatically, Security Director does not make any log entry because it is an internal operation.

Figure 97: 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.

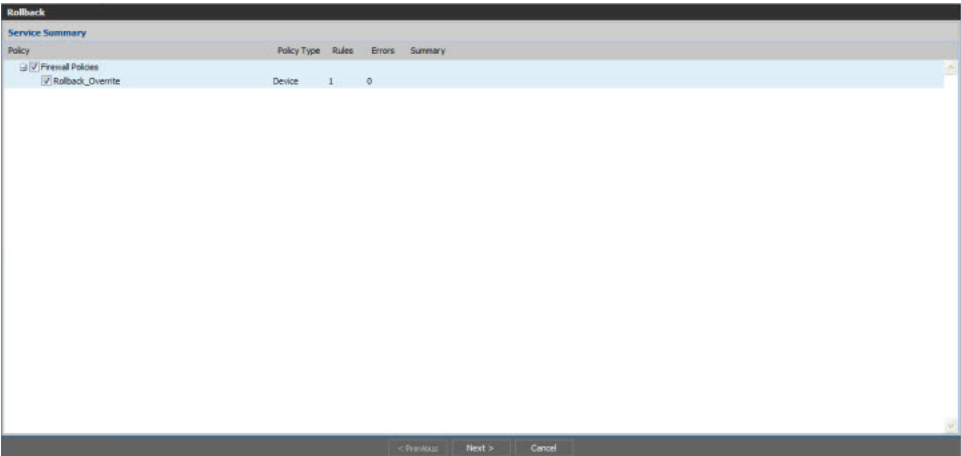
2. Right-click the firewall policy and select **Manage Snapshots**.

A window appears showing all the versions of the policy.

3. Select the version that you want to make as current and click **Rollback**.

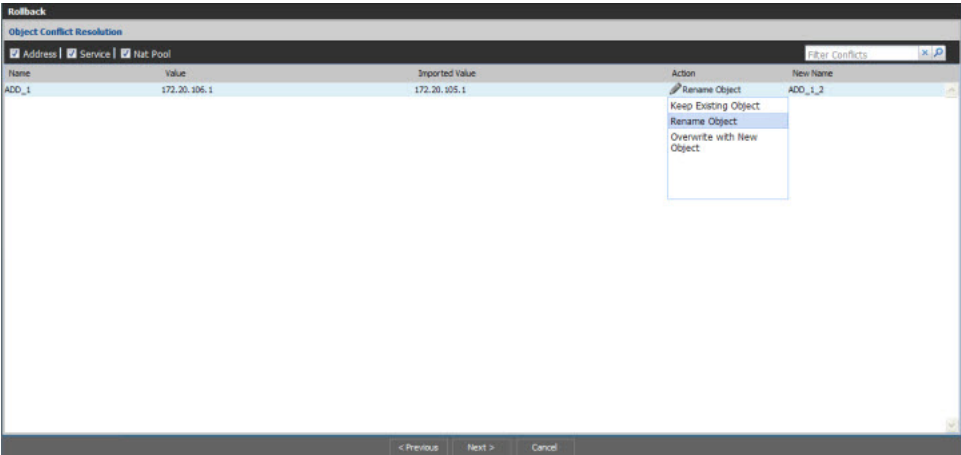
A service summary window appears, as shown in [Figure 98 on page 165](#).

Figure 98: 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 99 on page 165](#).

Figure 99: 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 100 on page 166](#).

Figure 100: Rollback OCR Summary Report



Rollback

Print Report

Selected Services

Type	Name	Policy Type	Total Lines	Errors	Warning	Summary
Firewall	Rollback_Overrite	Device	1	0	0	

Object Error Summary

Type	Object	Affected Objects	Errors
No Errors			

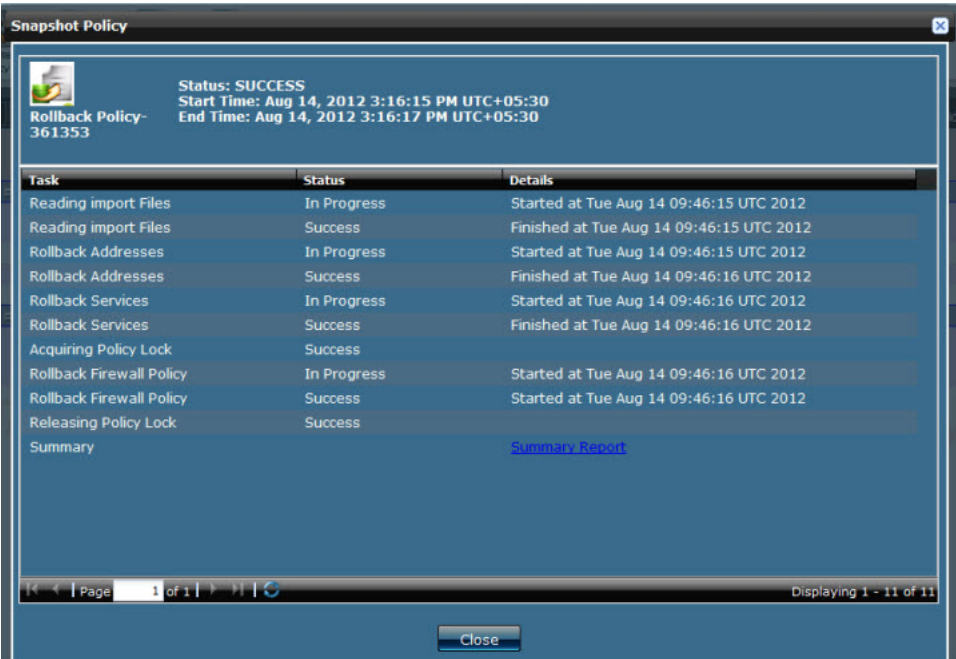
Object Conflict Resolution

Object Type	Original Name	Resolution	Resolved Name	Old Value	New Value
Address	ADD_1	Create with New Name	ADD_1_2	172.20.106.1	172.20.105.1

< Previous Finish Cancel

- Click **Finish** to replace the current policy with the versioned data. Summary of the snapshot policy is provided, as shown in Figure 101 on page 166.

Figure 101: Rollback Snapshot Policy Report



Snapshot Policy

Status: SUCCESS
Start Time: Aug 14, 2012 3:16:15 PM UTC+05:30
End Time: Aug 14, 2012 3:16:17 PM UTC+05:30

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		Summary Report

Page 1 of 1 | Displaying 1 - 11 of 11

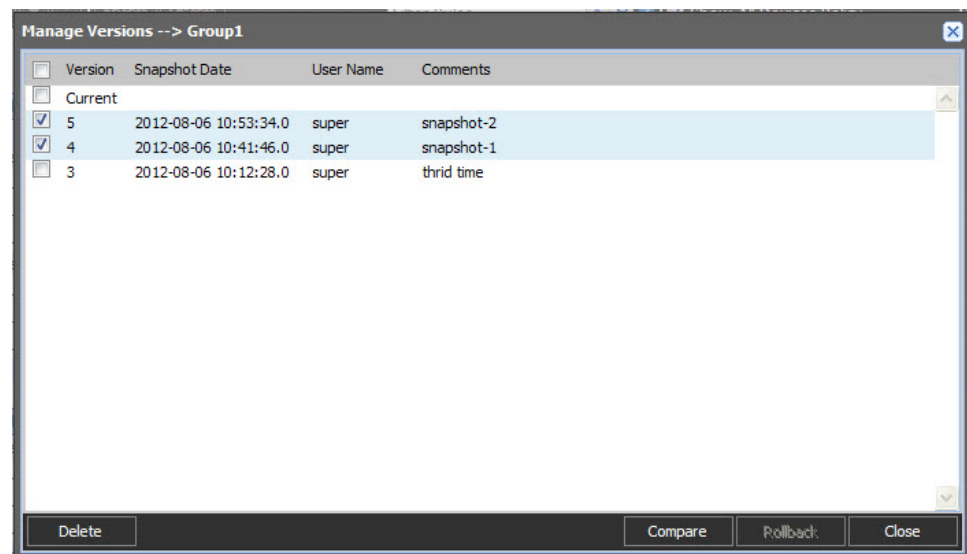
Close

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 Snapshots**.

The Manage Versions window appears, showing all policy versions, as shown in Figure 102 on page 167.

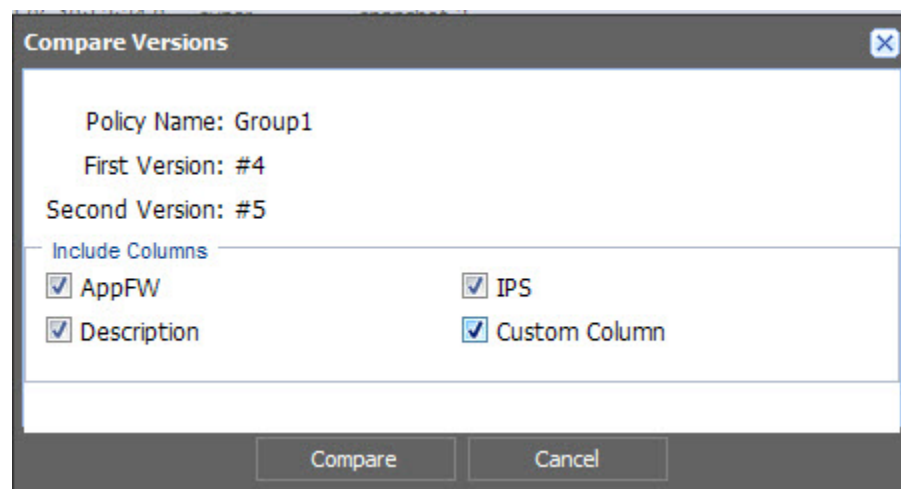
Figure 102: Manage Versions Window



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 103 on page 167](#).

Figure 103: 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 104 on page 168](#).

Figure 104: 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

PERMIT

Custom

None

IPS ON

Device-Global-2

Any

Any

Any

Deny

None

Device-Global-3

Any

Any

Any

Deny

None

Device-Global-4

Any

Any

Any

Deny

None

Device-Global-6

Any

Any

Any

Deny

None

Device-Global-7

Any

Any

Any

Deny

None

Device-Global-8

Any

Any

Any

Deny

None

Device-Global-9

Any

Any

Any

Deny

None

Device-Global-11

Any

Any

Any

Deny

None

Device-Global-111

Any

Any

Any

Deny

None

Device-Global-1

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

Refresh

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.

To delete versions:

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

The Policy Tabular view appears.

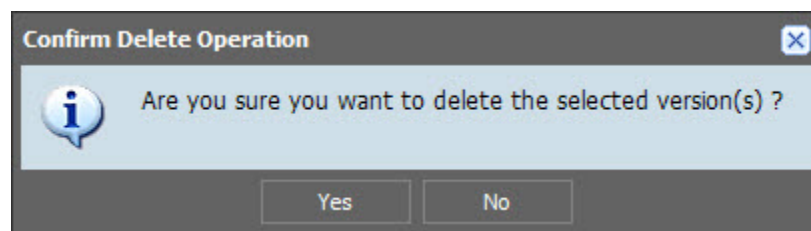
2. Right-click the firewall policy, and select **Manage Snapshots**.

A window appears, showing all policy versions.

3. You can delete multiple versions at a time. In case of roll back operation, you will get 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 105 on page 168](#).

Figure 105: 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.

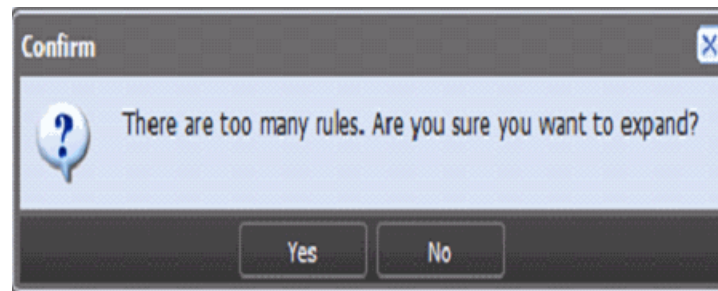
2. Select the firewall policy whose rules you want to expand.

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 106 on page 171](#).

Figure 106: ExpandAll Warning Message for More Than Thousand 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.

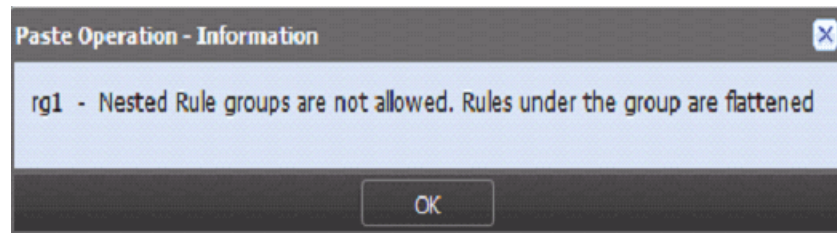
You can copy the rules without locking a policy. However, you must lock the policy for the cut operation. You can select the combination of rules or rule groups for cutting or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

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.

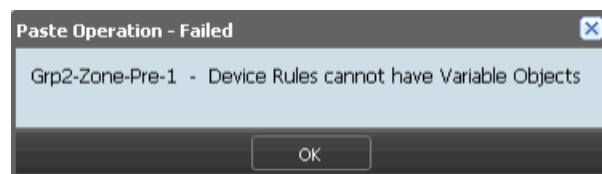
Security Director does not support nested rule grouping. If you paste a rule group in another custom rule group, an error message is displayed, giving you the option to proceed by flattening the copied rule group, as shown in [Figure 107 on page 172](#).

Figure 107: 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 108: 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.
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.

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 11 on page 173](#) explains the various rule operations on the filtered rules.

Table 11: 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>

Table 11: Various Rule Operation on the Filtered Rules (*continued*)

Rule Operation	Action
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>
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.



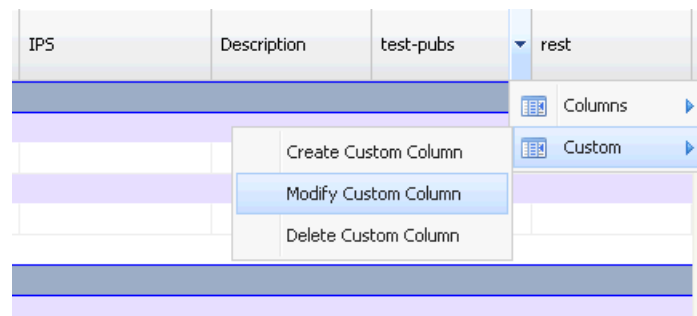
NOTE: The Save and Discard buttons, which are used to save or discard all the edits—including inline edits of custom column fields—are not used for registering custom columns. These actions are committed as soon as they are completed in their respective UI and are independent of the Save or Discard button.

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 109: Modifying a Custom Column



2. Once the edit is complete, the column header is refreshed to reflect the changes.



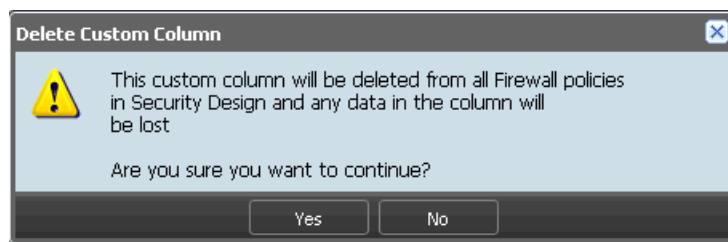
NOTE: You must have edit permissions to modify the custom column registration settings.

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 110 on page 176](#). After you confirm the deletion and the delete process finishes, Security Director updates the header and removes the column.

Figure 110: Deleting a Custom Column



Exporting a Custom Columns Definition

Custom column definition is exported when a firewall rule is exported.

Related Documentation

- [Firewall Policies Overview on page 107](#)
- [Creating Firewall Policies on page 117](#)
- [Adding Rules to a Firewall Policy on page 143](#)
- [Ordering the Rules in a Firewall Policy on page 147](#)
- [Publishing Firewall Policies on page 149](#)

PART 5

VPN

- [VPN on page 179](#)

CHAPTER 17

VPN

- [IPsec VPN Overview on page 179](#)
- [Creating IPsec VPNs on page 181](#)
- [Publishing IPsec VPNs on page 192](#)
- [Managing IPsec VPNs on page 194](#)

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:

- IKE and IPsec security associations (SAs) must be configured at the root level for each VPN tunnel.
 - Only route-based VPNs are supported for the logical systems. Policy-based VPNs are not supported.
 - The assigned interface, *st0.x*, in one logical system must not overlap with other logical systems. However, multiple logical systems can be assigned with their own *st0* interfaces.
 - The *st0.0* interface must not be assigned to any logical system, because you cannot set up SA to this interface.
-

Proxy ID is supported for both route-based and policy-based VPNs. Security Director supports only a single proxy ID.

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 181](#)
 - [Managing IPsec VPNs on page 194](#)
 - [Publishing IPsec VPNs on page 192](#)
 - [VPN Profiles Overview on page 83](#)
 - [Creating VPN Profiles on page 84](#)
 - [Managing VPN Profiles on page 87](#)

Creating IPsec VPNs

1. [Creating IPsec VPNs on page 181](#)

Creating IPsec VPNs

1. In the left pane, under Security Director application, select **VPN**.

The VPN Tabular view appears, as shown in [Figure 111 on page 181](#).

Figure 111: VPN Landing Page

Device	External Interface	Tunnel Zone	Initiator/Recipient	Protected Zone/Networks	Routing Instance	Proxy ID
SRX240B-10B	fe-0/0/6.0 (172.16.4.2)	VPN	Initiator	Addresses AG	vr3	2.2.2.0/24
SRX650-119-2	ge-0/0/1.0 (172.16.3.2)	VPN	Recipient	Addresses AG2	R11	4.4.4.0/24

2. Expand VPN by clicking on plus sign (+), and select **Create VPN**.

The Create VPN page appears.

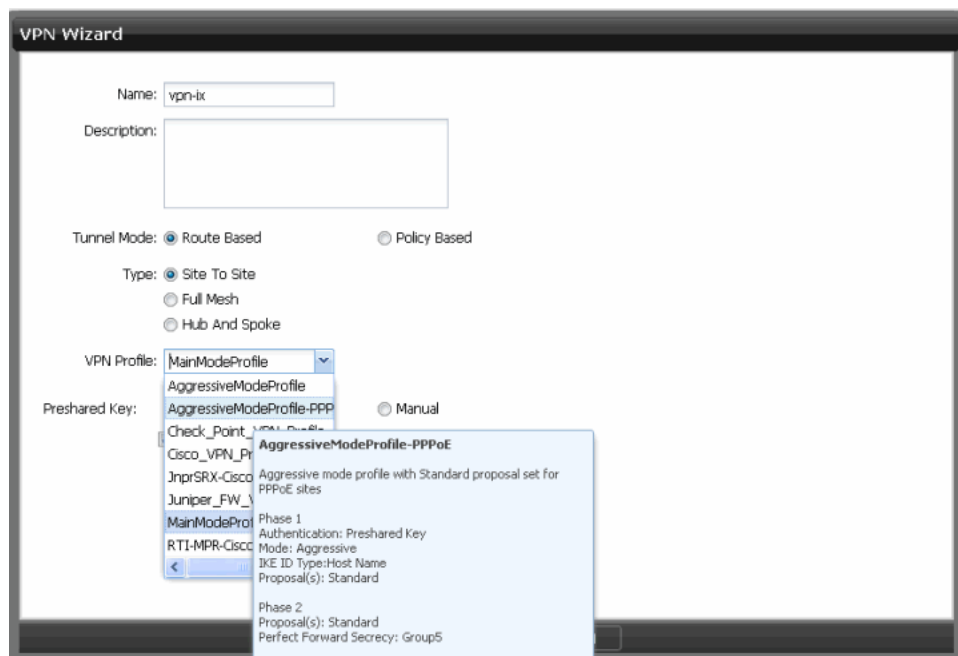
3. In the Name field, enter a name for the new VPN.
4. In the Description field, enter a description for the new VPN.
5. Select the Tunnel Mode as either Route Based or Policy Based.
6. If you have selected Route Based:
 - a. Select the option button next to the type of VPN you want to create.
 - b. 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 299](#).

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 112 on page 182](#).

- Phase 1
 - Authentication
 - Mode
 - Proposal(s)
- Phase 2
 - Proposal(s)
 - Perfect Forward Secrecy

Figure 112: VPN Profile Tooltip



NOTE: If you choose to create a full-mesh VPN, you can choose only the MainModeProfile 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 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 113 on page 183](#).

Figure 113: Create VPN Page—Route-Based VPN

Create VPN

Name:

Description:

Tunnel Mode: ☒ Route Based ☐ Policy Based

Type: ☒ Site To Site ☐ Full Mesh ☐ Hub And Spoke

VPN Profile:

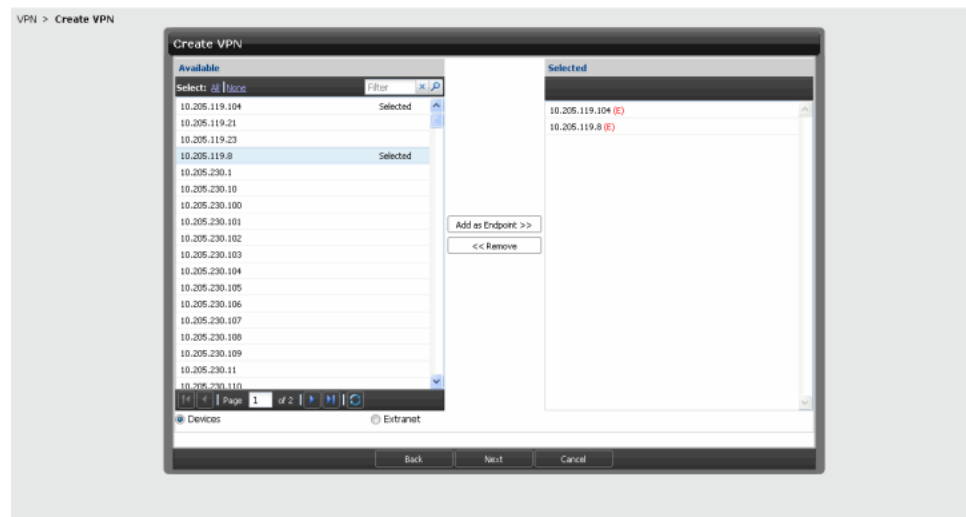
Preshared Key: ☒ Auto-generate ☐ Manual

☒ Generate Unique key per tunnel

Back Next Cancel

2. If you select Manual as the option for the preshared key, enter the manual key in the Manual Key field.
- d. Click **Next**.
- This page displays the Available and Selected panes.
- e. Select the device from the Available column, and click **Add as Endpoint**, as shown in [Figure 114 on page 184](#).

Figure 114: Create VPN: Add as Endpoint Page



- f. Click **Next**.
- g. 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, as shown in [Figure 115 on page 184](#).

Figure 115: Create VPN—Tunnel, Route, and Global Setting Pane

- h. 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.
- In the Global Settings pane, under Endpoint Configurations, enter the external interface in the External Interface field.
 - In the Global Settings pane, under Endpoint Configurations, enter the tunnel zone in the Tunnel Zone field.
 - 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.

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 116: Create VPN: Hub and Spoke Configuration

The screenshot shows the 'Create VPN' configuration window with three main sections: Tunnel Settings, Route Settings, and Global Settings.

Tunnel Settings

- Interface Type: ☐ Unnumbered, ☒ Numbered
- IP Subnet:
- Number of spoke devices per tunnel interface: ☒ All, ☐ Specify Values

Route Settings

- Routing Options: ☒ Static Routing, ☐ No Routing, ☐ OSPF, ☐ RIP

Global Settings

Please select default values to be used for all devices in VPN. Per-device settings can be modified in the next step.

Type	External Interface	Tunnel Zone	Protected Network Zone
Hub			
Spoke			

At the bottom of the window are buttons for Back, 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.

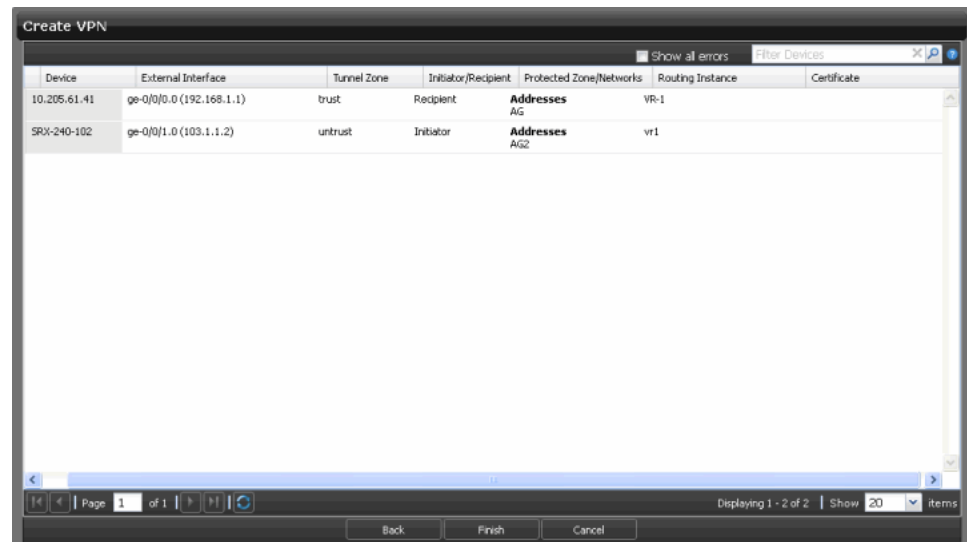
-
- l. For the certificate-based VPNs, another Certificate column appears, displaying the certificate information. Under the Certificate column, you can choose one of the certificate names available from the device. The same certificate is used for all devices. If the certificate specified does not exist in some of the devices, you can choose a device-specific certificate in the next step, as shown in [Figure 117 on page 187](#). If a certificate is not configured, an error message appears.
 - m. If you have selected **Static Routing**, enter the values in the External Interface, Tunnel Zone, and Protected Network Zone fields for the type Endpoint.
 - n. 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.
 - o. You can configure the custom routing instance for every device level, as shown in [Figure 117 on page 187](#). 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.

- p. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in [Figure 117 on page 187](#). 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 117: Create VPN Page Showing Custom Routing Instance Option



q. Click **Finish**.

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.

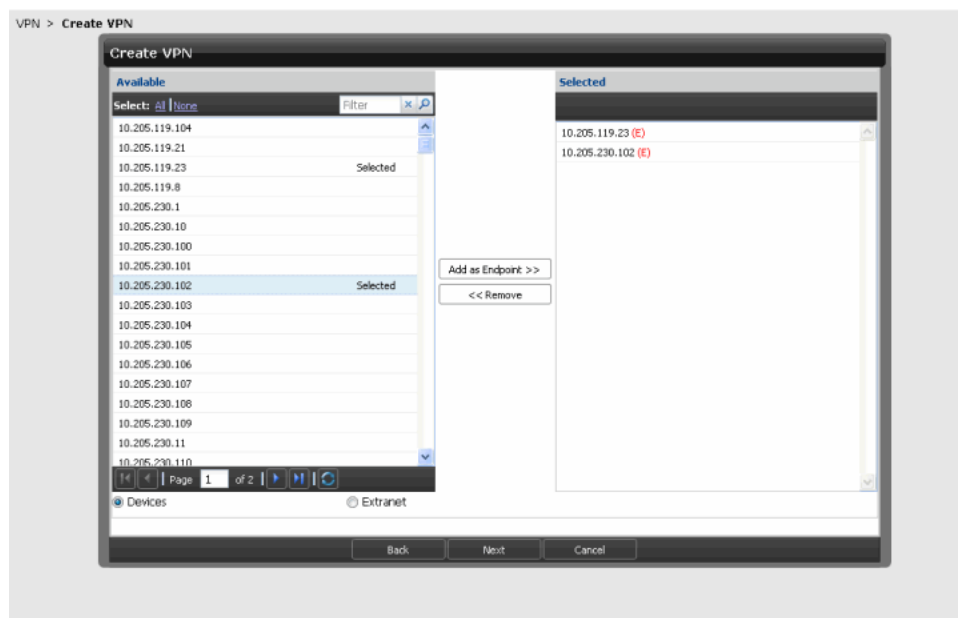
1. If you select **Autogenerate**, select the **Generate Unique key per tunnel** check box to generate a unique key per tunnel.
2. If you select **Manual**, enter the manual key in the **Manual Key** field.

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 118 on page 188](#).

Figure 118: Create VPN Policy-Based—Add as Endpoint Page

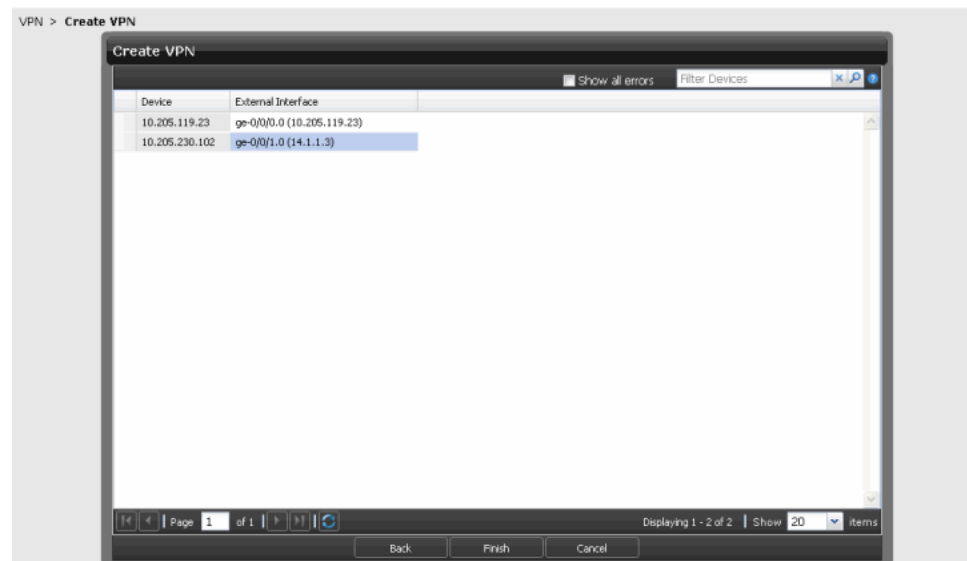


f. Click **Next**.

The page that appears gives you a preview of the values you entered for the VPN, as shown in [Figure 119 on page 189](#). 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 119: Create VPN Page—External Interface Selection



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.

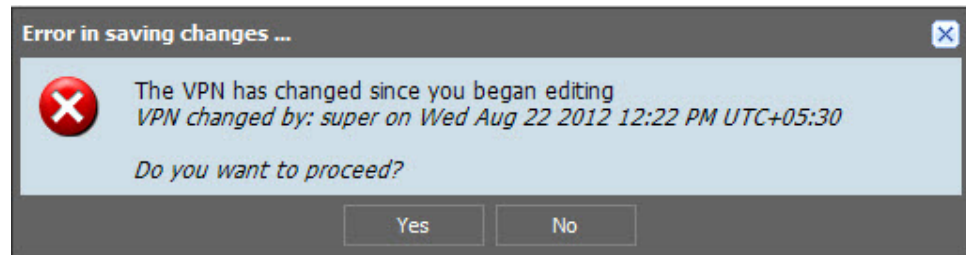


NOTE: Policy-based VPN is not supported on SRX Series devices with logical systems. Security Director does not show logical systems when you select the policy-based VPN.



NOTE: 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 120 on page 190](#).

Figure 120: VPN: Concurrent Save Error Message



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 111 on page 181](#). 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.

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 121 on page 191](#). 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 121: Inline Address Object Creation Page

2. Click the first plus sign (+) to create the new address object.
3. Click **Create** to create the object, or click **Cancel** to discard the changes.

To create address group:

1. Click the second plus sign (+) to create the new address group. [Figure 122 on page 192](#) shows the page that appears.

Figure 122: Inline Address Group Creation for VPN Object

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 or **Cancel** to discard the changes.

Related Documentation

- [IPsec VPN Overview on page 179](#)
- [Publishing IPsec VPNs on page 192](#)
- [Managing IPsec VPNs on page 194](#)
- [VPN Profiles Overview on page 83](#)
- [Creating VPN Profiles on page 84](#)
- [Managing VPN Profiles on page 87](#)

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 179](#)
- [Creating IPsec VPNs on page 181](#)
- [Managing IPsec VPNs on page 194](#)
- [VPN Profiles Overview on page 83](#)
- [Creating VPN Profiles on page 84](#)
- [Managing VPN Profiles on page 87](#)

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 194](#)
2. [Modifying Endpoint Settings in a VPN on page 195](#)
3. [Deleting IPsec VPNs on page 196](#)

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.

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.

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.

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.
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 179](#)
- [Creating IPsec VPNs on page 181](#)
- [Publishing IPsec VPNs on page 192](#)
- [VPN Profiles Overview on page 83](#)
- [Creating VPN Profiles on page 84](#)

- [Managing VPN Profiles on page 87](#)

PART 6

NAT Policies

- [NAT Policy on page 201](#)

CHAPTER 18

NAT Policy

- [NAT Overview on page 201](#)
- [Creating NAT Policies on page 205](#)
- [Unlocking Locked Policies on page 218](#)
- [Global Address Book Overview on page 219](#)
- [Adding Rules to a NAT Policy on page 221](#)
- [Ordering the Rules in a NAT Policy on page 227](#)
- [Publishing NAT Policies on page 227](#)
- [Managing NAT Policies on page 230](#)

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 12 on page 202 shows the persistent NAT support for different source NAT and destination NAT addresses.

Table 12: Persistent NAT Support

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT
IPv4	IPv6	IPv4	No
IPv4	IPv6	IPv6	No

Table 12: Persistent NAT Support (*continued*)

Source NAT Address	Translated Address	Destination NAT Address	Persistent NAT
IPv6	IPv4	IPv4	Yes
IPv6	IPv6	IPv6	No

Table 13 on page 203, and Table 14 on page 203 show the translated address pool selection for source NAT, destination NAT, and static NAT addresses.

Table 13: 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 14: 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 205](#)
- [Publishing NAT Policies on page 227](#)
- [Managing NAT Policies on page 230](#)
- [Managing NAT Pools on page 69](#)
- [Global Address Book Overview on page 219](#)

Creating NAT Policies

To create a NAT policy:

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

The NAT Policy Tabular view appears, as shown in [Figure 123 on page 205](#). 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 123: NAT Tabular View

NAT Policy

NAT

Filter

Location

+

-

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

↕

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 124 on page 206](#).

Figure 124: Create NAT Policy Page

Create NAT Policy

Type: ☒ Group ☐ Device

Name:

Description:

☐ Show Assigned Devices

Select Devices

Filter

Available		Selected
10.205.230.10		10.205.230.1
10.205.230.2		10.205.230.3
10.205.230.4		
10.205.230.5		
10.205.230.6		
10.205.230.7		

e. Click **Create**.



NOTE: One device can hold configuration data related to one NAT policy only. Therefore you cannot share devices for multiple NAT policies.

4. To create a device policy:
 - a. Enter the name of the device policy in the Name field.
 - b. Enter a description for the device policy in the Description field.
 - c. Select the device on which the device policy will be published from the Device menu.
 - d. Click **Create**.

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.

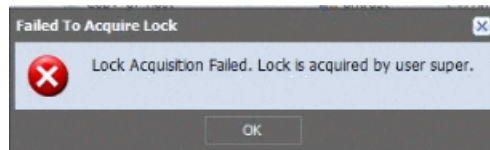
Security Directors permits you to save policies that contain errors. Warnings messages are displayed for policies that contain errors, but you can proceed to save such policies as drafts. You cannot publish policies that are in the draft state. The tooltip for the policy shows the state as draft; because 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.

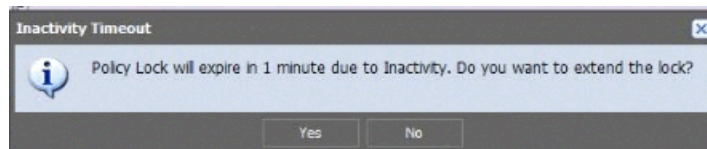
Before you can edit the policy, you must lock it by clicking the lock icon, which is available in the policy tabular view, as shown in [Figure 123 on page 205](#). You can hold more than one policy lock at a given time. You can unlock the policy by clicking the unlock icon next to the lock icon in the 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 125 on page 207](#). The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

Figure 125: Lock Failure Error Message for the Second User



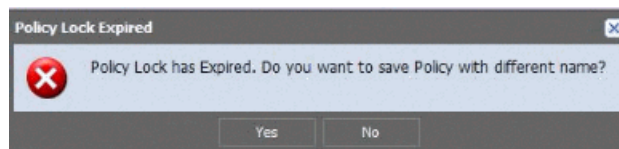
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 126 on page 207](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see “[Unlocking Locked Policies](#)” on page 218

Figure 126: Inactivity Timeout Error



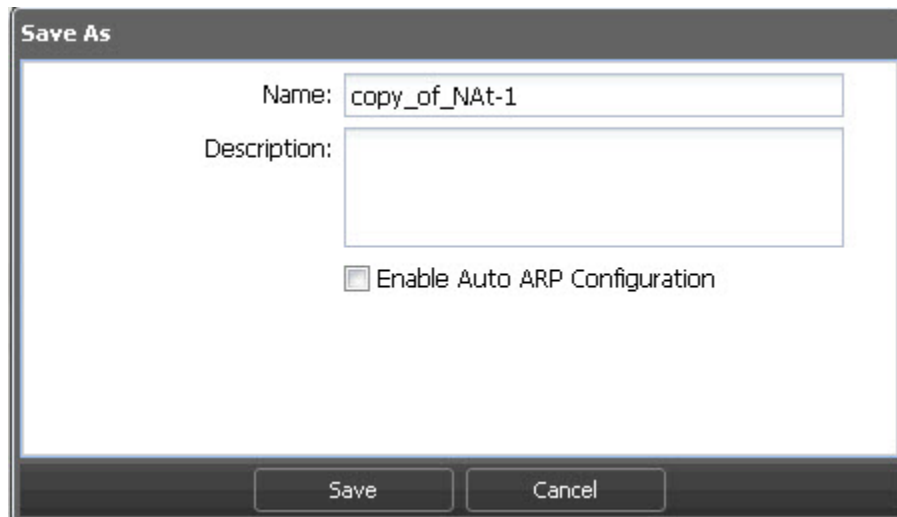
Click **Yes** to extend the locking period. If you click **No**, and if there is activity on the policy within the last minute of the lock's life, the timer will be reset and the lock will not be released. If you ignore the message, when the policy lock timeout interval expires 1 minute later, you are prompted to either save the edited policy with a different name or lose the changes, as shown in [Figure 127 on page 207](#)

Figure 127: 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 128 on page 208](#). 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 128: NAT Locked Policy: Save As Window

A "Save As" dialog box with a dark gray title bar. It contains two text input fields: "Name:" with the text "copy_of_NAt-1" and "Description:" which is empty. Below these fields is a checkbox labeled "Enable Auto ARP Configuration" which is unchecked. At the bottom are "Save" and "Cancel" buttons.

Save As

Name: copy_of_NAt-1

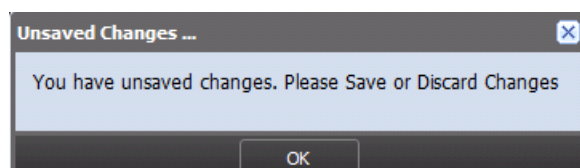
Description:

☐ Enable Auto ARP Configuration

Save Cancel

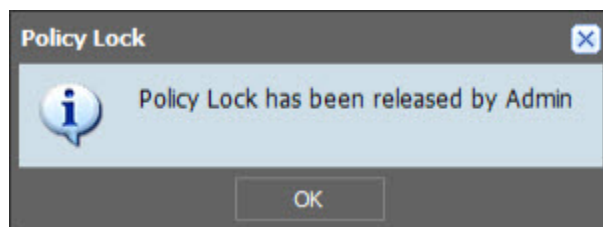
After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 129 on page 208](#).

Figure 129: NAT Policy: Unsaved Changes Message



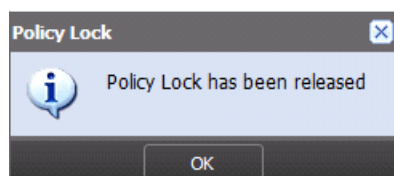
If the Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 130 on page 208](#).

Figure 130: 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 131 on page 208](#).

Figure 131: 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 132: Setting Source NAT Pool Page

Translation Type: Pool

Source Pool: Select Pool ... +

Pool Address:

Advanced

☐ Configure Proxy ARP for Pool Addresses

☐ Persistent

Ok Cancel

2. Click the plus sign to create the source NAT pool.

Figure 133: Create Source NAT Pool Page

Create Source NAT Pool

Name:

Description:

Pool Address: Select Address ... +

Advanced

Translation: Port/Range

Port: Range

Start:

End:

Create Cancel

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 134: Setting the Destination Pool Page

2. Click the plus sign (+) to create the destination NAT pool.

Figure 135: Create Destination NAT Pool Page

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 136: Create Inline NAT Address Object

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 137 on page 212](#). By default, the Address radio button is selected.

Figure 137: 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 138 on page 212](#) shows the page that appears.

Figure 138: Inline Address Group Creation for NAT Policy

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 15 on page 213](#) shows the protocols that have unique names. The other protocols, which do not have names, are identified with numbers.

Table 15: 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, as shown in figure. 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 139 on page 214](#).

Figure 139: Advanced Search Box for NAT Policies

The screenshot shows a web-based search interface titled "Advance Search". It includes the following fields and controls:

- Rule Name:** A text input field.
- Type:** A dropdown menu with a downward arrow.
- Original Packet Source:** A section containing "Ingress:" and "Address:" text input fields.
- Original Packet Destination:** A section containing "Egress:", "Address:", and "Port:" text input fields.
- Translated Packet Address:** A text input field.
- Buttons:** "Filter", "Reset", and "Cancel" buttons at the bottom.

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 16 on page 215](#) explains certain specific Security Director search behavior.

Table 16: 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 17 on page 215](#) shows example search results for different parameters.

Table 17: 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 17: 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 140 on page 217](#).

Figure 140: 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 140 on page 217](#).
3. Policies without any assigned devices are hidden in the left pane.

Related Documentation

- [Adding Rules to a NAT Policy on page 221](#)
- [Ordering the Rules in a NAT Policy on page 227](#)
- [Publishing NAT Policies on page 227](#)
- [Managing NAT Policies on page 230](#)

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 141: NAT Policy: Manage Policy Locks

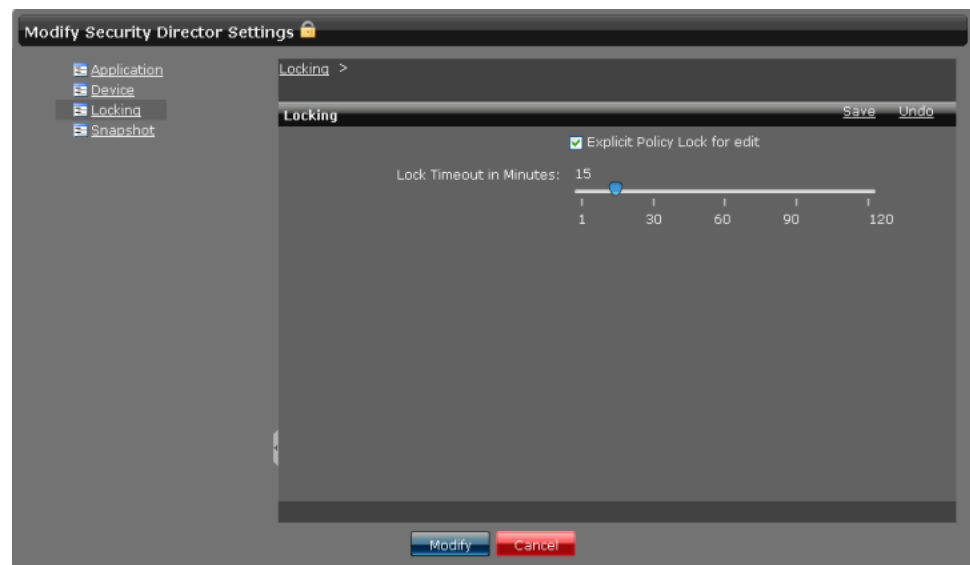
Policy	User	Lock Acquired Time	Lock Expires In
FW_3150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 25 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilo	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	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 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 142 on page 219](#).

Figure 142: 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 205](#)
- [Managing NAT Policies on page 230](#)

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 201](#)
- [Creating NAT Policies on page 205](#)
- [Managing NAT Policies on page 230](#)

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.

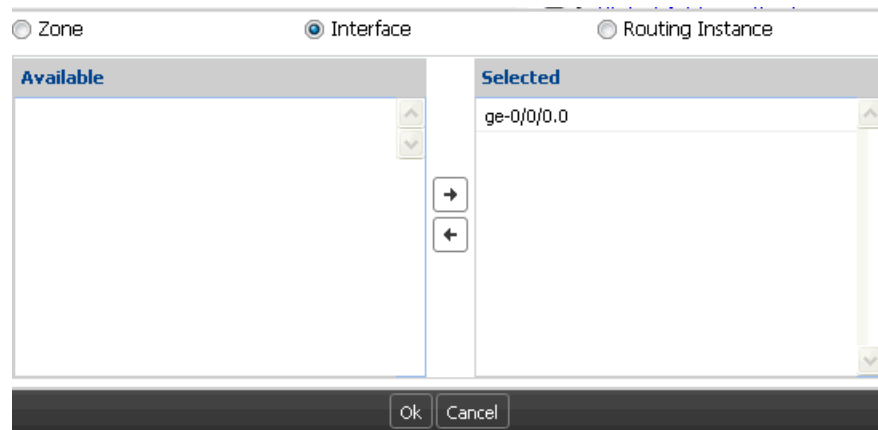
11. In the address selector, select the addresses you want to associate the rule to, from the Available section. You can select all addresses by clicking **Page** and unselect them all by clicking **None**.
12. Click the right arrow in the selector.

The selected addresses are now moved to the Selected section.

13. Click **OK**.
14. Click the **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 143: Destination Traffic Match Type Selector Page



15. Select the appropriate option from the Destination Traffic Matching Type list.

16. 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.

17. Click the right arrow in the selector.

The selected zones or interfaces or routing instance are now moved to the Selected column.

18. Click **OK**.

19. Click the **Address** field in the Original Packet Destination column and select the appropriate addresses.

The Address selector appears.

20. 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**.

21. Click the right arrow in the selector.

The selected addresses are now moved to the Selected column.

22. Click **OK**.

23. Click the **Port** field in the Original Packet Source column.

The Port selector appears.

24. Select the appropriate port type from the Port Type drop-down menu.

25. Click **OK**.

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 12.1R13.5, 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 144: Port Configuration for Static NAT

No.	Name	NAT Type	Original Packet Source	Ingress	Address	Egress	Address	Port	Translated Packet Source	Translated Packet Destination	Description
1	Device-2	STATIC	Zones: junos-host trust untrust-root	Not Applicable	Not Applicable	10.241.11.27/32	12345	Not Applicable	Not Applicable	10.241.11.18/32	Mapped Port: 4563-4566
2	Device-1	STATIC	Zones: junos-host trust untrust-root	Not Applicable	Not Applicable	64.62.209.60	Any	Not Applicable	Not Applicable	10.241.11.18/32	Mapped Port: 4563-4566

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 18 on page 225 shows the rule set names for different ingress and egress values.

Table 18: 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 19 on page 225 shows the rule set names for different ingress values.

Table 19: 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

Table 19: Example: Rule Set Names for Destination NAT and Static NAT (*continued*)

Ingress Value	Rule Set Name
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.

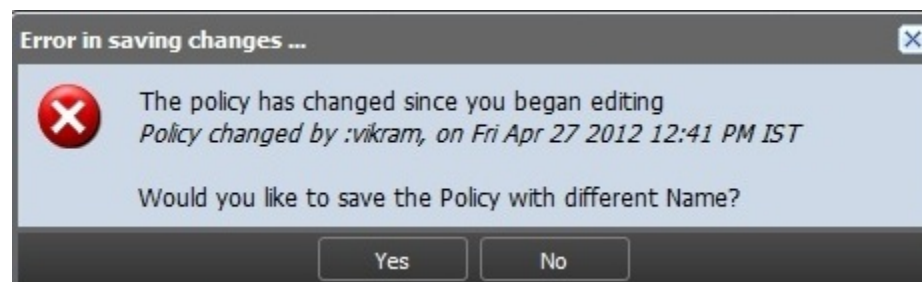


NOTE: You should click **Save** to save any changes you have made to the NAT policy. While in the process of making changes to the NAT policy, If you click on any of the tasks in the task ribbon before saving the NAT policy changes, all changes you have made will be lost. If you click anywhere inside 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 145 on page 226](#).

Figure 145: 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 227](#)
- [Publishing NAT Policies on page 227](#)
- [Managing NAT Policies on page 230](#)

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.

Related Documentation

- [Creating NAT Policies on page 205](#)
- [Adding Rules to a NAT Policy on page 221](#)
- [Publishing NAT Policies on page 227](#)
- [Managing NAT Policies on page 230](#)

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.



NOTE: 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.

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 14-6: NAT Policy CLI Configuration

```

Configuration for device
CLI Configuration XML 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 10.33.77.5/32 10.33.77.5/32
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_Fsp00-IF_Fsp00 from interface Fsp0.0
set security nat source rule-set IF_Fsp00-IF_Fsp00 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.

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.
-

**Related
Documentation**

- [Creating NAT Policies on page 205](#)
- [Adding Rules to a NAT Policy on page 221](#)
- [Ordering the Rules in a NAT Policy on page 227](#)
- [Managing NAT Policies on page 230](#)

Managing NAT Policies

- [Modifying NAT Policies on page 231](#)
- [Deleting NAT Policies on page 231](#)
- [Cloning NAT Policies on page 231](#)
- [Exporting a NAT Policy on page 232](#)
- [Configuring NAT Rule Sets on page 232](#)
- [NAT Policy Versioning on page 232](#)
- [Managing NAT Policy Versioning on page 234](#)
- [Deleting Rules in a NAT Policy on page 238](#)
- [Grouping Rules in a NAT Policy on page 239](#)
- [Enabling/Disabling Rules in a NAT Policy on page 239](#)
- [Expanding/Collapsing All Rules in a NAT Policy on page 240](#)
- [Cutting/Copying and Pasting Rules or Rule Groups in a NAT Policy on page 240](#)
- [Assigning Devices to a NAT Policy on page 242](#)
- [Deleting Devices from a NAT Policy on page 242](#)
- [Rule Operations on the Filtered Rules on page 243](#)

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 148 on page 234](#). 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:

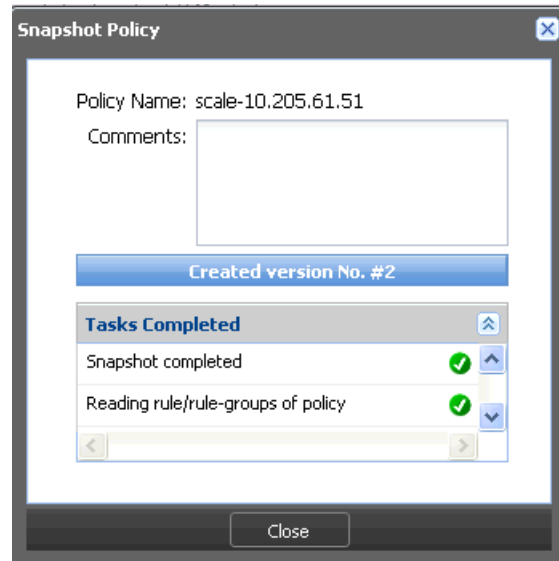
1. Select **Security Director > NAT Policy**.

The Policy Tabular view appears.

2. Right-click the NAT policy you want to take a snapshot of, and select **Snapshot Policy**.

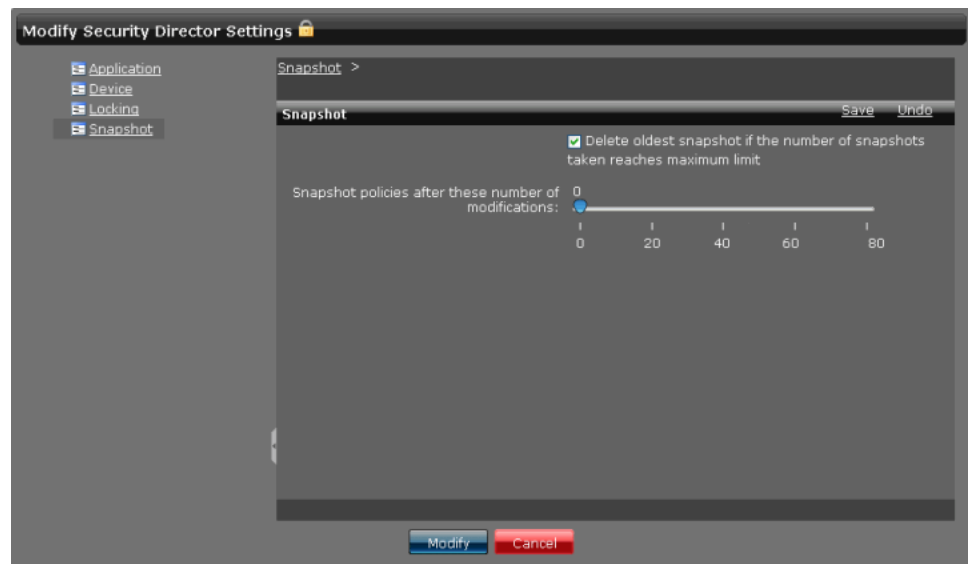
The Policy Name field shows the name of the NAT policy for which the snapshot is taken. Enter your comments in the Comments field, and press **Create to take the snapshot**. The Snapshot Policy Window appears, showing the status of the version as it is created, as shown in [Figure 147 on page 233](#).

Figure 147: 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 148 on page 234](#). When the snapshot is taken automatically, Security Director does not make any log entry because it is an internal operation.

Figure 148: Modify Security Director Settings**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.

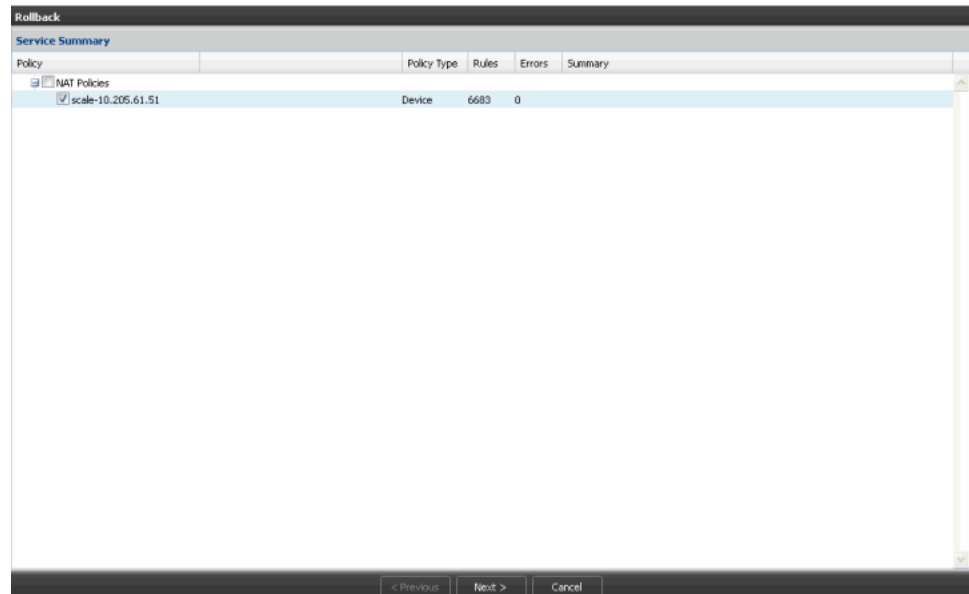
2. Right-click the natl policy, and select **Manage Snapshots**.

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 149 on page 235](#).

Figure 149: 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 150 on page 235](#).

Figure 150: 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 151 on page 236](#).

Figure 151: 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 152 on page 236.

Figure 152: 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		Summary Report

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.

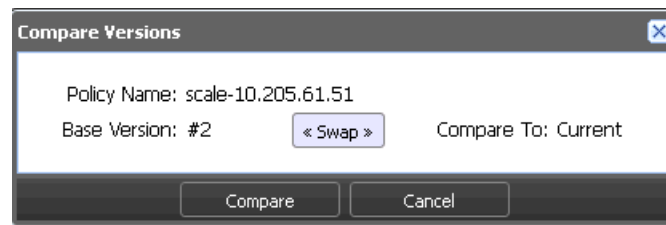
2. Right-click the NAT policy, and select **Manage Snapshots**.

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 153 on page 237](#).

Figure 153: 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 154 on page 237](#).

Figure 154: 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.

To delete versions:

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

The Policy Tabular view appears.

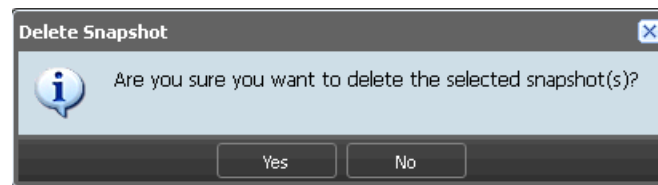
2. Right-click the NAT policy, and select **Manage Snapshots**.

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 155 on page 238](#).

Figure 155: 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.

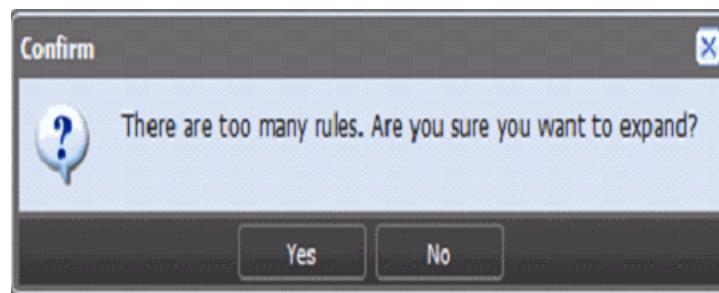
2. Select the NAT policy whose rules you want to expand.

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 156 on page 240](#).

Figure 156: ExpandAll Warning Message for More Than Thousand 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.

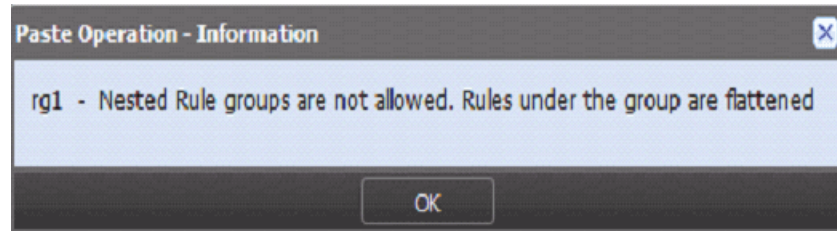
You can copy the rules without locking a policy. However, you must lock the policy for the cut operation. You can select the combination of rules or rule groups for cutting or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

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 157 on page 241](#).

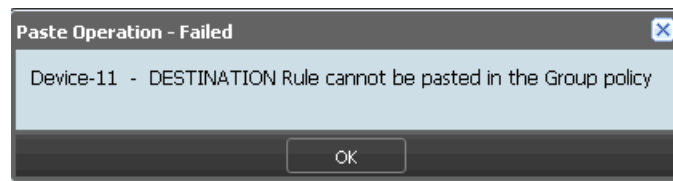
Figure 157: Nested Rule Group Operation Warning Message



Rule paste fails under the following conditions:

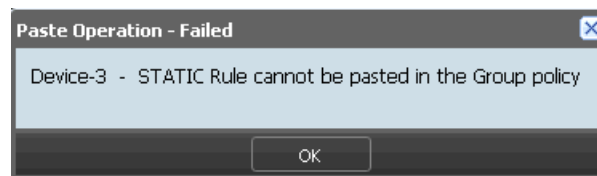
- If you copy the destination NAT rule and paste the rule in the group policy, the error shown in [Figure 158 on page 241](#) appears.

Figure 158: Destination NAT Rule Paste Error



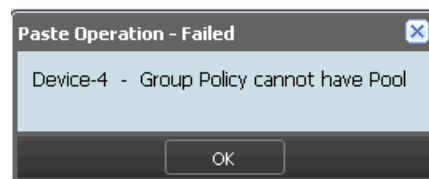
- If you copy the static NAT rule and paste the rule in the group policy, the error shown in [Figure 159 on page 241](#) appears.

Figure 159: Static NAT Rule Paste Error



- If you copy a source rule of translation type Pool to the group rule, the error shown in [Figure 160 on page 241](#) appears.

Figure 160: 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.
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 > Firewall Policy**.

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 20 on page 243](#) explains the various rule operations on the filtered rules.

Table 20: 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>

Table 20: Various Rule Operation on the Filtered Rules (*continued*)

Rule Operation	Description
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>

- Related Documentation**
- [Creating NAT Policies on page 205](#)
 - [Adding Rules to a NAT Policy on page 221](#)
 - [Ordering the Rules in a NAT Policy on page 227](#)
 - [Publishing NAT Policies on page 227](#)

PART 7

Global Search

- [Global Search on page 247](#)

CHAPTER 19

Global Search

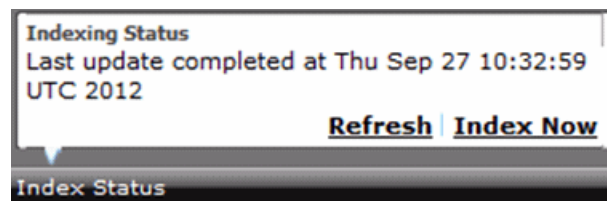
- [Indexing Overview on page 247](#)
- [Global Search on page 247](#)

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 161 on page 247](#) shows the indexing status for Security Director.

Figure 161: Indexing Status Message



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 247](#)

Global Search

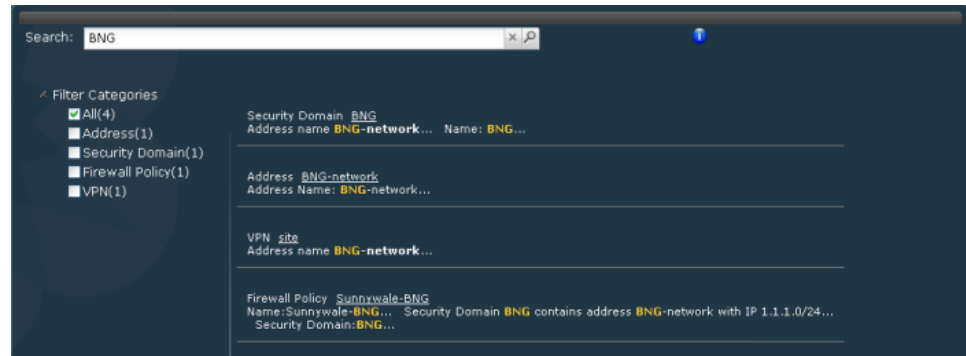
The Security Director home page provides a global search option to find objects and security configurations. You can also click a search result and navigate to its page.

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 162 on page 248](#).

Figure 162: 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 21 on page 248](#) specifies the objects and configurations that you can search using Global search.

Table 21: 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.
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”. Youd can search on “enet” “dest” or 112 or type “ene*” “des*” and so on.

Related Documentation

- [Indexing Overview on page 247](#)

PART 8

Downloads

- [Downloads on page 253](#)

CHAPTER 20

Downloads

- Downloading the Signature Database on page 253
- Installing the Signature Database on page 255

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 163 on page 253](#).

Figure 163: Signature Download Logs



User Name	User IP	Task	Timestamp	Result	Description
super	172.24.78.111	Download IPS signatures	Nov 15, 2011 8:59:38 PM IST	Success	Signature download successfully
super	10.208.3.164	Probe IPS Devices	Nov 11, 2011 4:19:23 AM IST	Success	Number of devices: 1 Successful: 1 Failed: 0
super	10.208.3.164	Probe IPS Devices	Nov 11, 2011 4:01:38 AM IST	Success	Number of devices: 1

Page 1 of 1 | Displaying 1 - 20 of 20

2. Select **Signature Database** from the Downloads workspace.

The Signature Database page appears, as shown in [Figure 164 on page 254](#). You can see the active databases that were downloaded earlier. At any time, Security Director will have only one active signature database.

Figure 164: Signature Database Page

Signature Database					
Active Database on Space					
Database Version	Publish date	Update Job	Installed Device Count	Detectors	Action
2030	2011-11-15 12:16:19	327686	0	5.1.110110809...	Install
Latest list for IPS signatures					
Database Version	Publish date	Update Summary	Detectors	Search Version: <input type="text"/>	
Database Version	Publish date	Update Summary	Detectors	Action	
2035 (latest)	2011-11-23 12:16:06	1 new signatures 2 updated signatures	11.6.140110920...	Download	
2034	2011-11-22 12:02:12	6 new signatures 6 updated applications	11.6.140110920...	Download	
2033	2011-11-21 12:04:41	19 new signatures 4 updated signatures	11.6.140110920...	Download	
2032	2011-11-17 13:00:49	1 new signatures 2 updated signatures 22 updated applications	11.6.140110920...	Download	
2031	2011-11-16 14:02:29	10 new signatures 2 updated signatures 2 renamed signatures	11.6.140110920...	Download	
2029	2011-11-14 11:59:16	7 new signatures 4 new applications 5 updated signatures 1 renamed signatures	11.6.140110920...	Download	

3. Select **Download Configuration**.

The Download Configuration page appears, as shown in Figure 165 on page 254.

Figure 165: Download Configuration Page

Download Configuration	
Download URL: <input type="text" value="https://services.netscreen.com"/>	
<div> <div>Use Proxy Server</div> <div> <input type="checkbox"/> Enable Proxy: <div> <input type="text" value="Host Name"/> <input type="text" value="Host Port"/> <input type="text" value="User Name"/> <input type="password" value="User Password"/> </div> </div> </div>	
<input checked="" type="checkbox"/> Schedule at a later time <div> Date and time: <input type="text" value="11/24/11"/> <input type="text" value="7:52 AM"/> <input type="text" value="IST"/> </div>	
<input checked="" type="checkbox"/> Repeat <div> <input type="text" value="1"/> <input type="text" value="Hours"/> </div>	
<input type="checkbox"/> End Time <div> <input type="text"/> </div>	
<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**.

Related Documentation • [Installing the Signature Database on page 255](#)

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 166 on page 256](#).

Figure 166: Install Configuration Page



4. Click the down arrow next to Signature Summary to view the version of the database and platforms that support this database.
5. 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**.

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.

**Related
Documentation**

- [Downloading the Signature Database on page 253](#)

PART 9

IPS Management

- [IPS Management Overview on page 261](#)
- [IPS Management on page 263](#)

CHAPTER 21

IPS Management Overview

- [IPS Management Overview on page 261](#)

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.

Related Documentation

- [Downloading the Signature Database on page 253](#)
- [Installing the Signature Database on page 255](#)

CHAPTER 22

IPS Management

- [Creating IPS Signatures on page 263](#)
- [Managing IPS Signatures on page 265](#)
- [Creating IPS Signature Sets on page 268](#)
- [Adding Rules to an IPS Signature Set on page 269](#)
- [Managing IPS Signature Sets on page 270](#)
- [Creating IPS Policies on page 274](#)
- [Managing Policy Locks on page 283](#)
- [Ordering the Rules in a IPS Policy on page 284](#)
- [Adding Rules to an IPS Policy on page 285](#)
- [Publishing IPS Policies on page 287](#)
- [Managing IPS Policies on page 291](#)

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 167 on page 264](#). 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 167: 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 168 on page 264](#).

Figure 168: Create IPS Signature Page

IPS Policy > IPS Signature > Create IPS Signature

Create IPS Signature

Name: Category: Action:

Keywords: Severity:

Description:

Signature Details | Supported Detectors

Binding: Time Scope: Match Assurance:

Protocol: Time Count: Performance Impact:

Add Signature

m01

Context: Direction:

Pattern: Regexp: Negated: ☐

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 265](#)

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 266](#)
- [Modifying IPS Signatures on page 266](#)
- [Deleting IPS Signatures on page 266](#)
- [Cloning IPS Signatures on page 267](#)
- [Creating Static Signature Groups on page 267](#)

- [Creating Dynamic Signature Groups on page 267](#)
- [Creating IPS Signature Sets on page 268](#)

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 **Create Static Group** from the Actions drawer.

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 **Create Dynamic Group** from the Actions drawer.

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 263](#)

Creating IPS Signature Sets

To create an IPS signature-set:

1. Select **Security Director > IPS Management**.
You see the IPS Policies Tabular view.
2. Click **IPS Signature-Set**.

You see the IPS Signature Set Tabular view with two panes and the first signature set is selected by default. The left pane displays all the IPS signature sets in the system. The right pane displays all the rules in a specific IPS signature set as shown in [Figure 169 on page 269](#).

Figure 169: IPS Signature Set Tabular View

S.No.	Name	Rule Type	IPS Signature	Action	Notification	IPS Options
Web_Server (Predefined) Rules (6 rules)						
1	Web_Server-1	IPS	IP - Critical IP - Major TCP - Critical TCP - Major	Drop packet		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More
2	Web_Server-2	IPS	DNS - Critical DNS - Major	Drop packet		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More
3	Web_Server-3	IPS	FINR - Critical FINR - Major FTP - Critical FTP - Major	Drop packet		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More
4	Web_Server-4	IPS	DNS - Minor FINR - Minor FTP - Minor Gopher - Minor	No action		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More
5	Web_Server-5	IPS	Anomaly - Warning Signature - Warning	No action		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More
6	Web_Server-6	IPS	Anomaly - Info	No action		IP Action: None IP Target: None Timeout: 0 Log IP Action: Disable More

All the IPS signature sets under the Predefined node are predefined signature sets.
All the IPS signature sets under the Custom node are user-defined signature sets.

3. Click **Create IPS Signature-Set**.

The Create IPS Signature-Set page appears.

4. Enter the name of the IPS signature set in the Name field.

5. Enter the description for the IPS signature set in the Description field.

6. Click **Create**.

Validate IPS signature sets 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 signature sets.

Related Documentation

- [Adding Rules to an IPS Signature Set on page 269](#)
- [Managing IPS Signature Sets on page 270](#)

Adding Rules to an IPS Signature Set

To add rules to an IPS signature-set:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS signature set Tabular view appears.

2. Click the IPS signature set you want to add rules to from the left pane.

The existing rules of the IPS signature-set 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 IPS Signature Sets on page 268](#)
- [Managing IPS Signature Sets on page 270](#)

Managing IPS Signature Sets

- [Deleting IPS Signature Sets on page 271](#)
- [Cloning IPS Signature Sets on page 271](#)
- [Enable or Disable Rules in an IPS Signature-set on page 271](#)
- [Grouping Rules in an IPS Signature Set on page 272](#)
- [Expanding/Collapsing All Rules in an IPS Signature Set on page 272](#)

- [Cutting/Copying And Pasting Rules or Rule Groups in an IPS Signature Set on page 273](#)
- [Adding Rules to an IPS Signature Set on page 273](#)

Deleting IPS Signature Sets

To delete IPS signature sets:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefined and custom signature sets. The right pane displays the signatures in the respective signature-set.

2. Right-click the signature set you want to delete and select **Delete IPS Signature Set**.

A confirmation window appears.



NOTE: You cannot delete a predefined signature set. You can only delete a custom signature set.

3. Click **Yes**.

Cloning IPS Signature Sets

To clone IPS signature sets:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefined and custom signature sets. The right pane displays the signatures in the respective signature-set.

2. Right-click the signature set you want to clone and select **Clone IPS Signature Set**.

You are redirected to the Clone IPS Signature Set page. You can modify the name and description on this page.

3. Click **Clone**.

Enable or Disable Rules in an IPS Signature-set

To enable or disable rules in an IPS signature-set:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefined and custom signature sets.

2. Select the signature set for which you want to enable or disable the rule in the left pane.

All rules of the this signature set 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 an IPS Signature Set

To group rules in an IPS policy:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefines and custom signature sets.

2. Select the signature set for which you want to group all rules, in the left pane.

All rules of the this signature set 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 an IPS Signature Set

To expand or collapse all rules in an IPS policy:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefines and custom signature sets.

2. Select the signature set 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 signature set are expanded.
4. Click the **Collapse All RuleGroups** icon to collapse all rules.

Cutting/Copying And Pasting Rules or Rule Groups in an IPS Signature Set

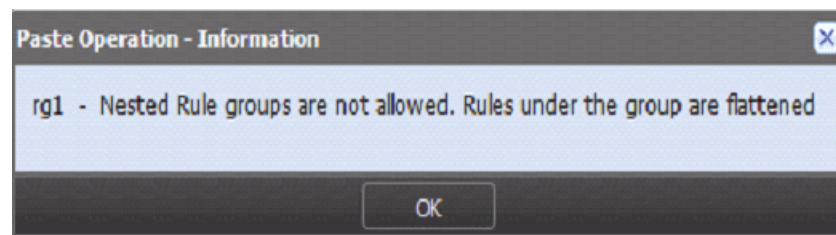
To copy and paste rules in an IPS signature set:

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 IPS signature set 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 IPS signature sets, you must first save the cut operation in the current signature set before moving to another IPS signature set 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 170 on page 273](#).

Figure 170: Nested Rule Group Paste Warning Message



Adding Rules to an IPS Signature Set

You can add the rules before or after the IPS rule or exempt rule. To add rules:

1. Select **Security Director > IPS Management > IPS Signature-Set**.

The IPS Signature Set page displays all signature sets. The left pane displays the predefines and custom signature sets.

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 IPS Signature Sets on page 268](#)
- [Adding Rules to an IPS Signature Set on page 269](#)

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 22 on page 274](#) shows different IPS configuration modes and their purposes:

Table 22: 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.

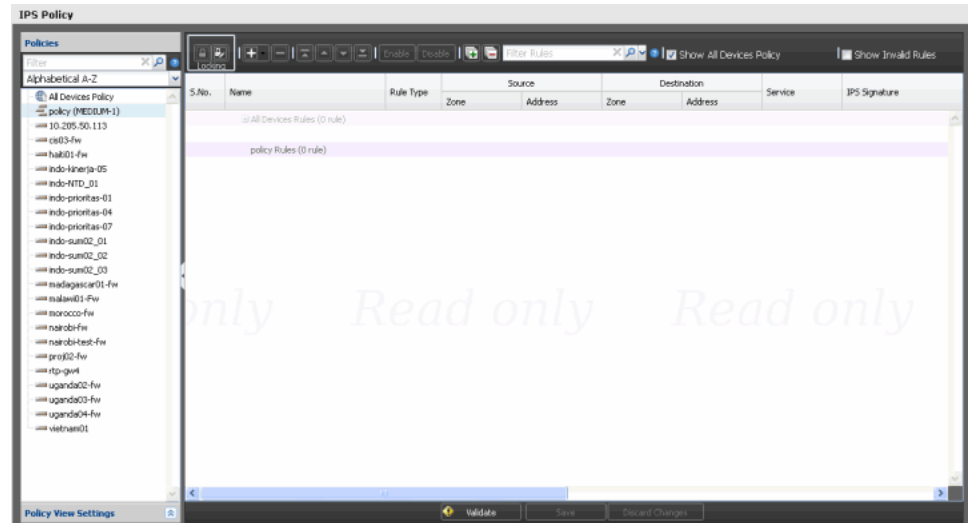
- Set the Action field for the device rule for which you want to enable the firewall policy to Permit.
- Select IPS field to IPS ON or IPS OFF when the firewall policy is configured with IPS mode basic or advanced, and the firewall rule action is set to either permit or tunnel.

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 171 on page 275](#).

Figure 171: 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.

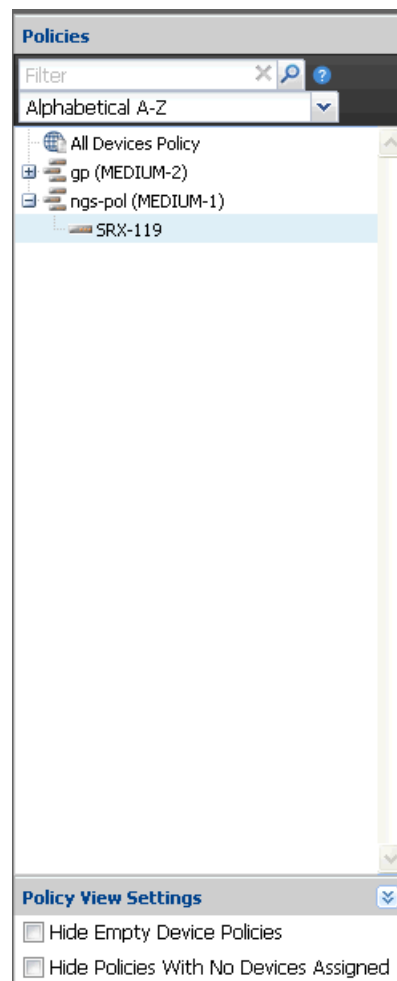
**NOTE:**

- 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 172 on page 277](#).

Figure 172: 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 172 on page 277](#).
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 173 on page 278](#).

Figure 173: IPS Advance Search Window

The screenshot shows the 'Advanced Search' window for IPS. It features a search form with the following fields:

- Rule Name:
- Rule Type:
- Source:
 - Zone:
 - Address:
- Destination:
 - Zone:
 - Address:
- Service:
- IPS Signature Name:
- Action:
- Description:

At the bottom of the window are three buttons: **Filter**, **Reset**, and **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 23 on page 279 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 279 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.

Table 24: Examples of Different Advanced Search Parameters (*continued*)

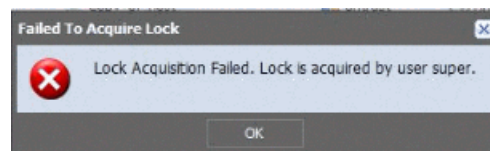
Source zone and source address to destination zone and destination address	SrcZone:(<i>polyzone</i>) AND SrcAddress:(<i>any</i>) AND DstZone:(<i>untrust</i>) AND DstAddress:(<i>polyaddr</i>)	Rules with source zone <i>polyzone</i> , source address <i>any</i> , destination zone <i>untrust</i> , and destination 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.

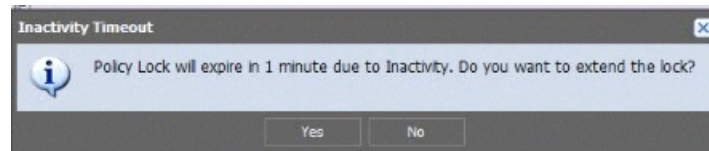
Before you can edit the policy, you must lock it by clicking the lock icon, which is available in the policy view toolbar. You can hold more than one policy lock at a given time. You can unlock the policy by clicking the unlock icon next to the lock icon in the policy tabular view. If you attempt to lock a policy that is already locked by another user, the following message appears, as shown [Figure 174 on page 280](#). The tooltip shows the policy locked user information. Mouse over the policy that you want to lock to view the tooltip.

Figure 174: Lock Failure Error Message for the Second User



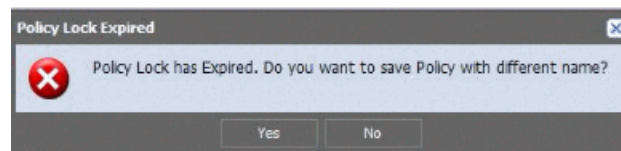
If the locked policy is inactive for the set timeout value (default 5 minutes), just 1 minute before the timeout interval expires, the following message appears, as shown in [Figure 175 on page 281](#). If the policy lock timeout interval expires for multiple locked policies, the same warning message appears for each locked policy. To understand the configuration of timeout value and session timeout value, see [“Managing Policy Locks” on page 283](#).

Figure 175: 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 176 on page 281](#).

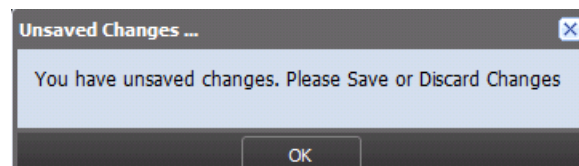
Figure 176: Policy Lock Expired Message



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.

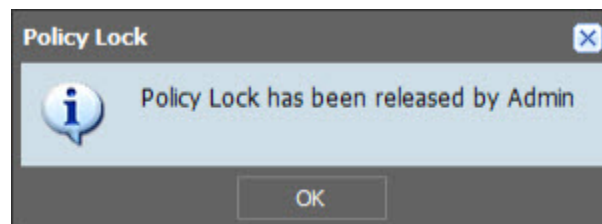
After editing a locked policy, if you move to another policy without saving your edited policy, or if you unlock the policy without saving, the following warning message appears, as shown in [Figure 177 on page 281](#).

Figure 177: Unsaved Changes Warning Message

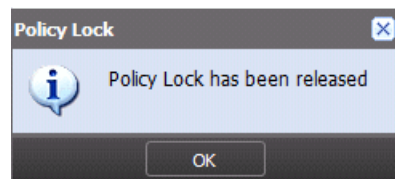


If Security Director administrator releases the lock, you will receive the following warning message, as shown in [Figure 178 on page 281](#).

Figure 178: 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 179 on page 282](#).

Figure 179: 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 287](#)
- [Managing IPS Policies on page 291](#)

Managing Policy Locks

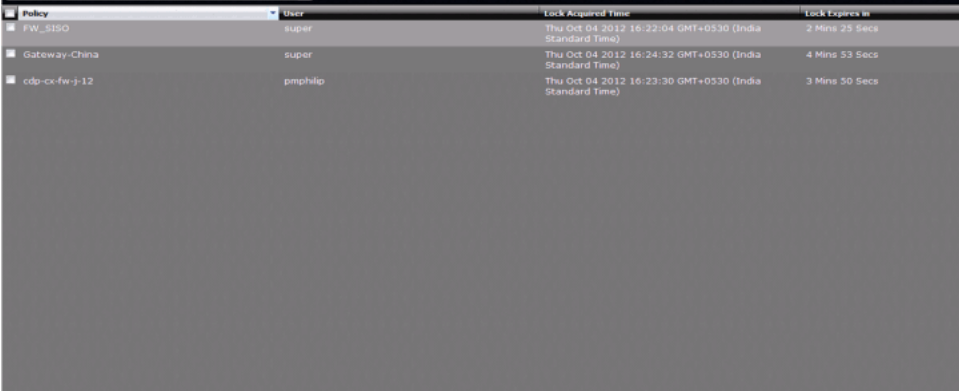
All the locked policies can be viewed in a single page. This page is available for a user having Manage Policy Locks tasks assigned. This page shows all the locks only if the user has Unlock task assigned, other wise user will see only his locks. To view the locked policies:

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 180: IPS Policy: Manage Policy Locks



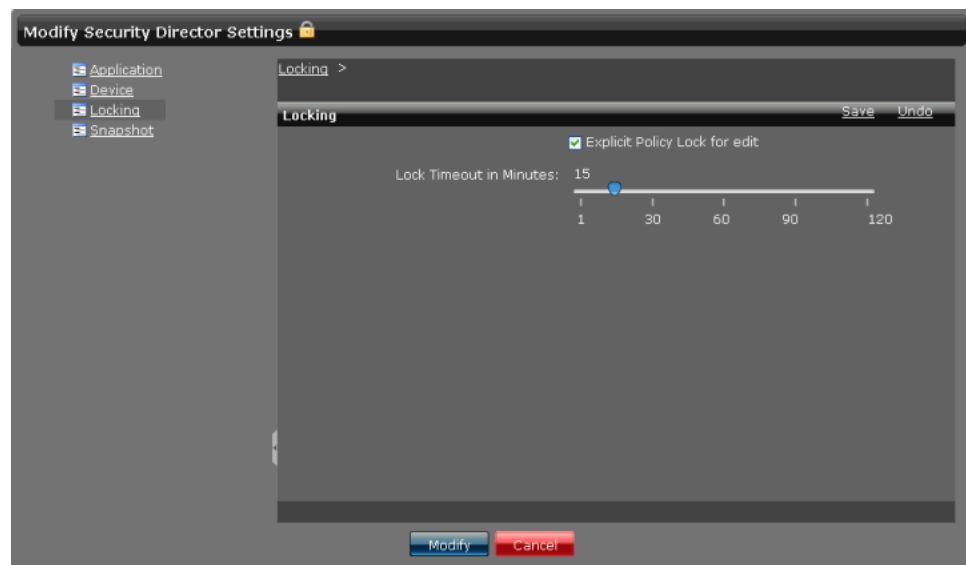
Policy	User	Lock Acquired Time	Lock Expires In
FW_3150	super	Thu Oct 04 2012 16:22:04 GMT+0530 (India Standard Time)	2 Mins 25 Secs
Gateway-China	super	Thu Oct 04 2012 16:24:32 GMT+0530 (India Standard Time)	4 Mins 53 Secs
cdp-cx-fw-j-12	pmphilo	Thu Oct 04 2012 16:23:30 GMT+0530 (India Standard Time)	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 181 on page 284](#).

Figure 181: 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 274](#)
- [Publishing IPS Policies on page 287](#)
- [Managing IPS Policies on page 291](#)

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.

Related Documentation

- [Creating IPS Policies on page 274](#)
- [Adding Rules to an IPS Policy on page 285](#)
- [Publishing IPS Policies on page 287](#)
- [Managing IPS Policies on page 291](#)

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 274](#)
- [Ordering the Rules in a IPS Policy on page 284](#)
- [Publishing IPS Policies on page 287](#)
- [Managing IPS Policies on page 291](#)

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 182 on page 288](#).

Figure 182: 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

- Click **Next**.

The Affected Devices page displays the devices on which this IPS policy will be published, as shown in [Figure 183 on page 288](#).

Figure 183: Policy Publish: Affected Devices Page

Affected Devices

Type to Search Devices

Name	Managed Status	Connection Status	Services	Configuration
tongzhou	In Sync	Up	x1	View

Page 1 of 1

Displaying 1 - 1 of 1 Devices | Show 20

☒ Schedule at a later time

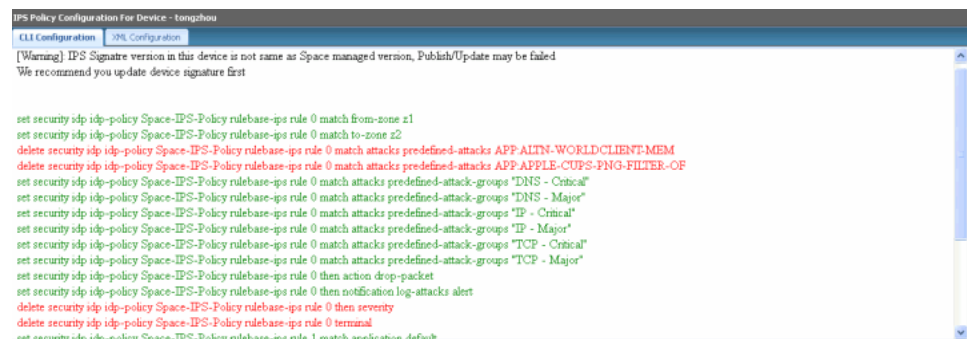
Date and Time: 03/13/12 2:40 PM IST

Back Publish Publish and Update Cancel

- 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.

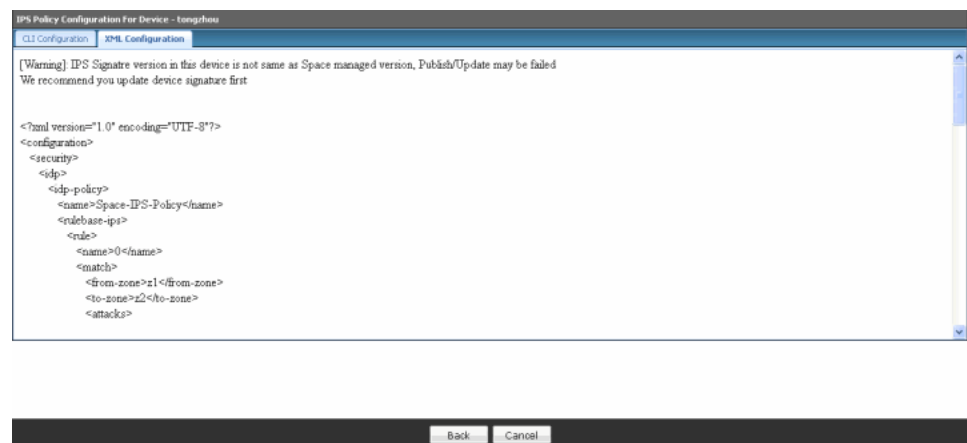
The CLI Configuration tab appears by default. You can view the configuration details in CLI format, as shown in [Figure 184 on page 289](#).

Figure 184: Policy Publish: CLI Configuration



6. View the XML format of the configuration by clicking the **XML Configuration** tab, as shown in Figure 185 on page 289.

Figure 185: 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.
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.

Related Documentation

- [Creating IPS Policies on page 274](#)
- [Managing IPS Policies on page 291](#)

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 292](#)
2. [Enabling or Disabling Rules in an IPS Policy on page 292](#)
3. [Cloning a Rule in an IPS Policy on page 292](#)
4. [Grouping Rules in an IPS Policy on page 293](#)
5. [Expanding/Collapsing All Rules in an IPS Policy on page 293](#)
6. [Cutting/Copying And Pasting Rules or Rule Groups in an IPS Policy on page 293](#)
7. [Adding Rules to an IPS Policy on page 294](#)
8. [Rule Operations on the Filtered Rules on page 294](#)

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

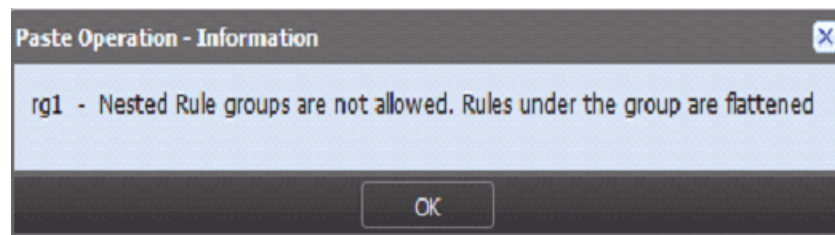
or copying operation. However, a rule group and one or more rules inside the same rule group cannot be copied or cut simultaneously.

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 186 on page 294](#).

Figure 186: 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 25 on page 295](#) explains the various rule operations on the filtered rules.

Table 25: 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 25: 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 274](#)
 - [Ordering the Rules in a IPS Policy on page 284](#)
 - [Adding Rules to an IPS Policy on page 285](#)
 - [Publishing IPS Policies on page 287](#)

PART 10

Security Director Devices

- [Security Director Devices on page 299](#)

CHAPTER 23

Security Director Devices

- Updating Devices with Pending Services on page 299
- Importing Firewall, NAT, and IPS Policies from a Device to Security Director on page 303
- NSM Migration on page 309
- Managing Consolidated Configurations on page 315

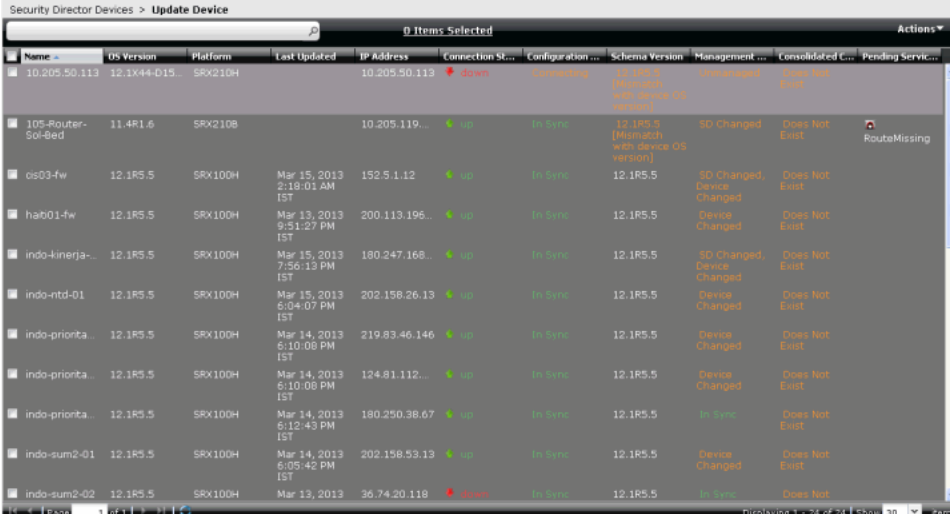
Updating Devices with Pending Services

To update a device with pending services:

1. Select **Security Director > Security Director Devices**.

The Security Director Devices page appears, as shown in [Figure 187 on page 299](#).

Figure 187: Security Director Devices Page

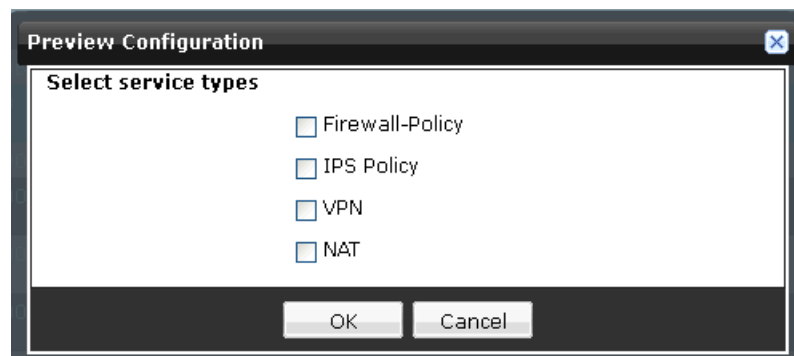


Name	OS Version	Platform	Last Updated	IP Address	Connection St...	Configuration	Schema Version	Management	Consolidated	Pending Services
10.205.50.113	12.1X44-D15...	SRX210H		10.205.50.113	Down	Out of Sync	12.1R5.5 (Mismatch with device OS version)	SD Changed	Does Not Exist	RouteMissing
105-Router-Sol-Bed	11.4R1.6	SRX210B		10.205.119...	Up	In Sync	12.1R5.5 (Mismatch with device OS version)	SD Changed, Device Changed	Does Not Exist	
os03-fw	12.1R5.5	SRX100H	Mar 15, 2013 2:18:01 AM IST	152.5.1.12	Up	In Sync	12.1R5.5	SD Changed, Device Changed	Does Not Exist	
ha01-fw	12.1R5.5	SRX100H	Mar 13, 2013 9:51:27 PM IST	200.113.196...	Up	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-kinerja...	12.1R5.5	SRX100H	Mar 15, 2013 7:56:13 PM IST	180.247.168...	Up	In Sync	12.1R5.5	SD Changed, Device Changed	Does Not Exist	
indo-ntd-01	12.1R5.5	SRX100H	Mar 15, 2013 6:04:07 PM IST	202.158.26.13	Up	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita...	12.1R5.5	SRX100H	Mar 14, 2013 6:10:08 PM IST	219.83.46.146	Up	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita...	12.1R5.5	SRX100H	Mar 14, 2013 6:10:08 PM IST	124.81.112...	Up	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita...	12.1R5.5	SRX100H	Mar 14, 2013 6:12:43 PM IST	180.250.38.67	Up	In Sync	12.1R5.5	In Sync	Does Not Exist	
indo-sum2-01	12.1R5.5	SRX100H	Mar 14, 2013 6:05:42 PM IST	202.158.53.13	Up	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-sum2-02	12.1R5.5	SRX100H	Mar 13, 2013	36.74.20.118	Down	In Sync	12.1R5.5	In Sync	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 188 on page 300](#).

Figure 188: Update Window



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**.

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. 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.



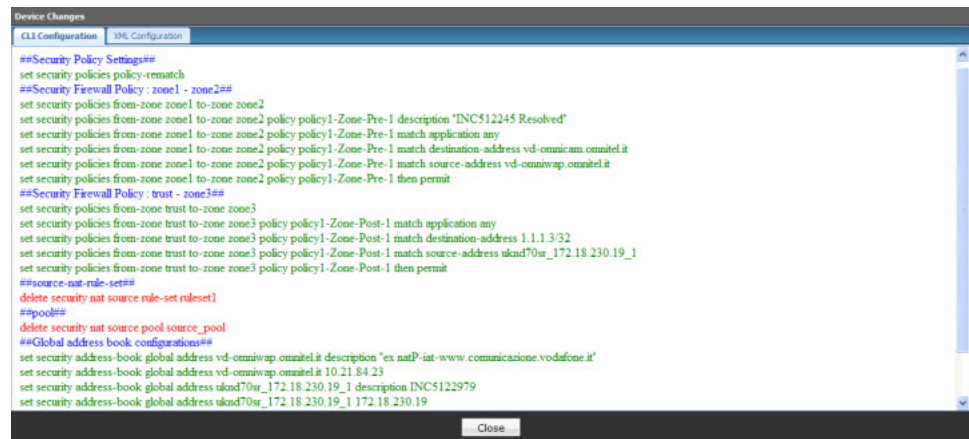
NOTE: If you make changes with NAT and firewall policies through the device CLI, and while updating the device you must select both firewall policy and NAT policy in the Select service types window. If you select either firewall policy or NAT policy alone for update, the device status remains Device 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 189 on page 301](#).

Figure 189: 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.



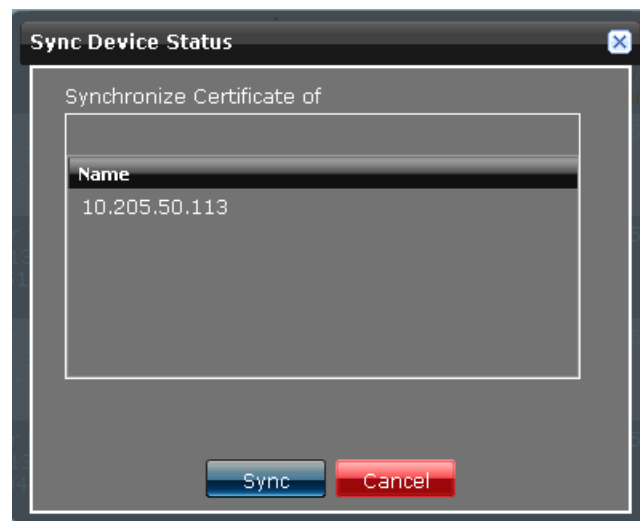
NOTE: A warning message appears when the management status for any device is changed to Device Changed.

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 190 on page 302](#).

Figure 190: 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*.

Related Documentation

- [Importing Firewall, NAT, and IPS Policies from a Device to Security Director on page 303](#)

- [NSM Migration on page 309](#)
- [Managing Consolidated Configurations on page 315](#)

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 191 on page 304](#).

Figure 191: Manage Security Devices Page

Name	OS Version	Platform	Last Updated	IP Address	Connection St...	Configuration ...	Schema Version	Management ...	Consolidated C...	Pending Servic...
10.205.50.113	12.1X44-D15...	SRX210H		10.205.50.113	Down	Configuring	12.1R5.5 (Mismatch with device OS version)	SD Changed	Does Not Exist	
105-Router-Sol-6ed	11.4R1.6	SRX210B		10.205.119...	In Sync	In Sync	12.1R5.5 (Mismatch with device OS version)	SD Changed	Does Not Exist	RouteMissing
cis03-fw	12.1R5.5	SRX100H	Mar 15, 2013 2:19:01 AM IST	152.5.1.12	In Sync	In Sync	12.1R5.5	SD Changed, Device Changed	Does Not Exist	
hab01-fw	12.1R5.5	SRX100H	Mar 13, 2013 9:51:27 PM IST	200.113.196...	In Sync	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-kinerja...	12.1R5.5	SRX100H	Mar 15, 2013 7:56:13 PM IST	180.247.168...	In Sync	In Sync	12.1R5.5	SD Changed, Device Changed	Does Not Exist	
indo-ntd-01	12.1R5.5	SRX100H	Mar 15, 2013 6:04:07 PM IST	202.158.26.13	In Sync	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita	12.1R5.5	SRX100H	Mar 14, 2013 6:10:08 PM IST	219.83.46.146	In Sync	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita...	12.1R5.5	SRX100H	Mar 14, 2013 6:10:08 PM IST	124.81.112...	In Sync	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-priorita...	12.1R5.5	SRX100H	Mar 14, 2013 6:12:43 PM IST	180.250.38.67	In Sync	In Sync	12.1R5.5	In Sync	Does Not Exist	
indo-sum2-01	12.1R5.5	SRX100H	Mar 14, 2013 6:05:42 PM IST	202.158.53.13	In Sync	In Sync	12.1R5.5	Device Changed	Does Not Exist	
indo-sum2-02	12.1R5.5	SRX100H	Mar 13, 2013	36.74.20.118	Down	In Sync	12.1R5.5	In Sync	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 192 on page 304](#).

Figure 192: Service Import Summary Page

Policy	Policy Type	Rules	Errors	Summary
NAT Policies				
<input checked="" type="checkbox"/> ind-h26-41	Device	9	0	
Firewall 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 193 on page 305](#).

Figure 193: 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:2E00::0000:0022:F376:#f376ab3f	2001:db8:85a3:b4d3:1319:8a2e:370:7348	Rename Object	HOST_v6_1
ADDR-GROUP-v4	[HOST_v4, HOST_v6]	[HOST_v4_1, 10.159.2.0/25, DNS]	Rename Object	ADDR-GRO_1
IPS-Host	4.3.3.1	1.1.1.1	Rename Object	IPS-Host_1
IPS-Address-Group	[IPS-Host, HOST_v4]	[IPS-Host_1, IPS-Host_2, IPS-Network, IPS-Range]	Rename Object	IPS-Address_1
TCP-2967	1. one_Rp, 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. 10, ICMP Code: 1, ICMP Type: 23 2. 11, ICMP Code: 0, ICMP Type: 29	1. icmp0, ICMP Code: 0, ICMP Type: 11 2. icmp1, ICMP Code: 0, ICMP Type: 4, 1...	Rename Object	ICMP_App_1
CUSTOM-APP-GROUP-1	icmp_App TCP-2967	icmp_Net_Unreachable TCP-2967 TCP-440 UDP-1404	Rename Object	CUSTOM-AP_1
IPS-Service-4	1. one_Rp, Acl: Rp, Protocol: TCP, Source Port: 32, Destination Port: 21, Inactiv...	1. IPS-Service-4, ICMP Code: 124, ICMP Type: 123	Rename Object	IPS-Service_1
IPS-Service-Group	IPS-Service-4	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-cust-req	Name: static-cust-req, Type: static, Members: HTTP:MSDC:KOPFS-WEBROOT	Name: static-cust-req_1, Type: static, Members: Severity-Info	Rename Object	static-cust_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-fa_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.

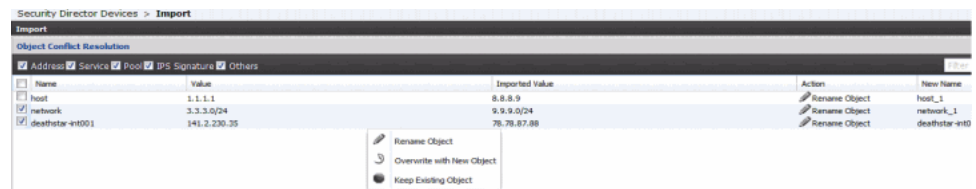
Conflicting objects can be address, service, NAT pool objects, IPS Signature, static group, or dynamic group. The inactive rules on the device are disabled in the imported policy and the unused objects, such as unused IPS signatures are removed during the IPS import. Security Director imports attacks 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 194 on page 306](#).

Figure 194: 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 195 on page 306](#).

Figure 195: Policy Import Status Page



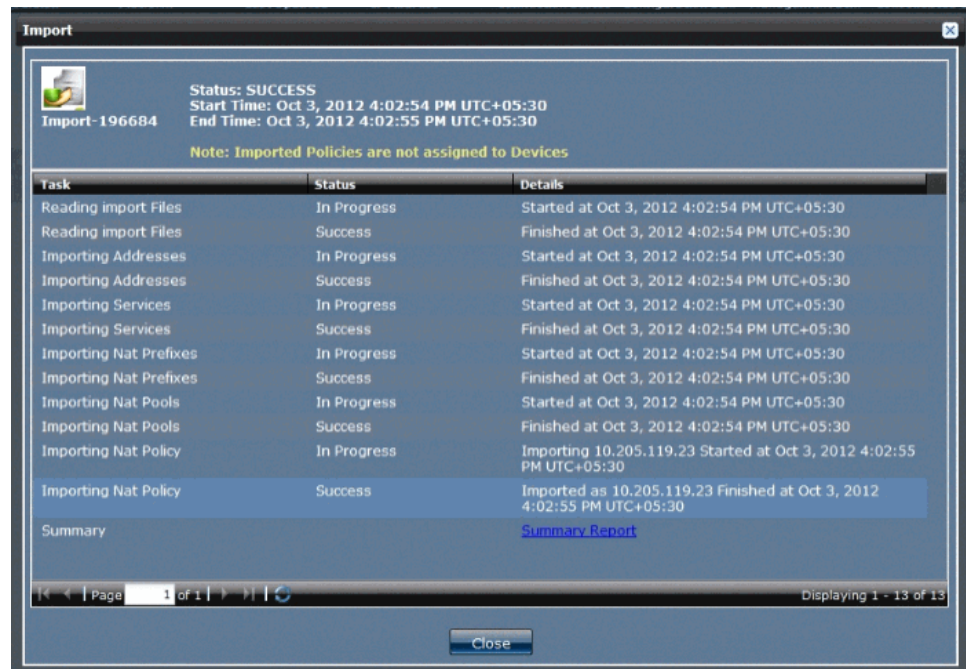
To print the summary report, click **Print Report** at the beginning of the page.



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 196 on page 307](#).

Figure 196: Firewall Policy Final Import Status Page



- Click **Summary Report** to view the import summary as shown in Figure 195 on page 306.
- 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.

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.

**Related
Documentation**

- [NSM Migration on page 309](#)

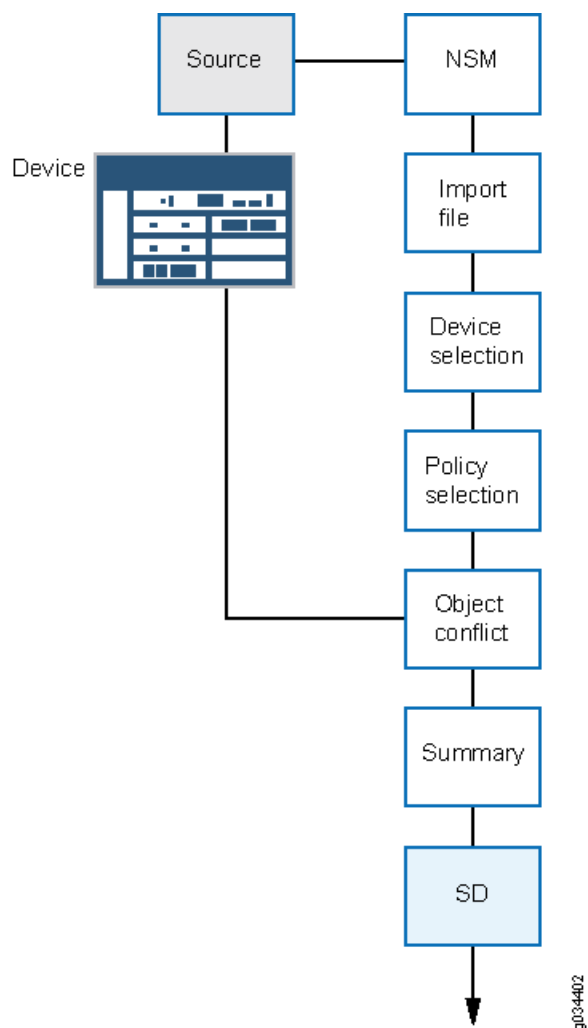
NSM Migration

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 migrate 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 197 on page 310 shows the workflow of device import.

Figure 197: High-level Device Import Workflow



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 198 on page 311](#).

Figure 198: NSM Xdiff File Upload Page



NOTE: The supported NSM versions for the database import are 2010.3 through 2011.4.

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 199: 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	srx220n	global



NOTE: In Security Director Release 12.2 and later releases, ScreenOS based policies (SRX Series specific fields) are migrated from NSM to Security Director and ScreenOS devices are listed in the devices page in the NSM migration workflow.

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 200 on page 312](#).

Figure 200: Service Import Summary Page

Policy	Rules	Errors	Summary
nm-srx220-2	6	0	
SRX-119.8	15	0	

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 (UTM, Scheduler)

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 201 on page 312](#).

Figure 201: NSM—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:2E00:0000:0022:F376:#32ab3F	2001:db8:85a3:b4d3:1319:8a2e: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-Host-2, IPS-Host-3, IPS-Host-4, IPS-Host-5, IPS-Host-6, IPS-Host-7, IPS-Host-8, IPS-Host-9, IPS-Host-10, IPS-Host-11, IPS-Host-12, IPS-Host-13, IPS-Host-14, IPS-Host-15, IPS-Host-16, IPS-Host-17, IPS-Host-18, IPS-Host-19, IPS-Host-20, IPS-Host-21, IPS-Host-22, IPS-Host-23, IPS-Host-24, IPS-Host-25, IPS-Host-26, IPS-Host-27, IPS-Host-28, IPS-Host-29, IPS-Host-30, IPS-Host-31, IPS-Host-32, IPS-Host-33, IPS-Host-34, IPS-Host-35, IPS-Host-36, IPS-Host-37, IPS-Host-38, IPS-Host-39, IPS-Host-40, IPS-Host-41, IPS-Host-42, IPS-Host-43, IPS-Host-44, IPS-Host-45, IPS-Host-46, IPS-Host-47, IPS-Host-48, IPS-Host-49, IPS-Host-50, IPS-Host-51, IPS-Host-52, IPS-Host-53, IPS-Host-54, IPS-Host-55, IPS-Host-56, IPS-Host-57, IPS-Host-58, IPS-Host-59, IPS-Host-60, IPS-Host-61, IPS-Host-62, IPS-Host-63, IPS-Host-64, IPS-Host-65, IPS-Host-66, IPS-Host-67, IPS-Host-68, IPS-Host-69, IPS-Host-70, IPS-Host-71, IPS-Host-72, IPS-Host-73, IPS-Host-74, IPS-Host-75, IPS-Host-76, IPS-Host-77, IPS-Host-78, IPS-Host-79, IPS-Host-80, IPS-Host-81, IPS-Host-82, IPS-Host-83, IPS-Host-84, IPS-Host-85, IPS-Host-86, IPS-Host-87, IPS-Host-88, IPS-Host-89, IPS-Host-90, IPS-Host-91, IPS-Host-92, IPS-Host-93, IPS-Host-94, IPS-Host-95, IPS-Host-96, IPS-Host-97, IPS-Host-98, IPS-Host-99, IPS-Host-100]	Rename Object	IPS-Address-Group_1
TCP-2967	1. one_fdp, 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. ID, 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	1. one_fdp, Protocol: TCP, Source Port: 32, Destination Port: 21, Inactiv...	1. Icmp_Unreachable TCP-2967 TCP-445 UDP-1434	Rename Object	CUSTOM_APP_GROUP-1_1
IPS-Service-6	1. one_fdp, Alg: Rfp, Protocol: TCP, Source Port: 32, Destination Port: 21, Inactiv...	1. IPS-Service-6, ICMP Code: 124, ICMP Type: 123	Rename Object	IPS-Service-6_1
IPS-Service-Group	IPS-Service-6	IPS-Service-1 IPS-Service-2 IPS-Service-3 IPS-Service-4 IPS-Service-5 IPS-Service-6 IPS-Service-7 IPS-Service-8 IPS-Service-9 IPS-Service-10 IPS-Service-11 IPS-Service-12 IPS-Service-13 IPS-Service-14 IPS-Service-15 IPS-Service-16 IPS-Service-17 IPS-Service-18 IPS-Service-19 IPS-Service-20 IPS-Service-21 IPS-Service-22 IPS-Service-23 IPS-Service-24 IPS-Service-25 IPS-Service-26 IPS-Service-27 IPS-Service-28 IPS-Service-29 IPS-Service-30 IPS-Service-31 IPS-Service-32 IPS-Service-33 IPS-Service-34 IPS-Service-35 IPS-Service-36 IPS-Service-37 IPS-Service-38 IPS-Service-39 IPS-Service-40 IPS-Service-41 IPS-Service-42 IPS-Service-43 IPS-Service-44 IPS-Service-45 IPS-Service-46 IPS-Service-47 IPS-Service-48 IPS-Service-49 IPS-Service-50 IPS-Service-51 IPS-Service-52 IPS-Service-53 IPS-Service-54 IPS-Service-55 IPS-Service-56 IPS-Service-57 IPS-Service-58 IPS-Service-59 IPS-Service-60 IPS-Service-61 IPS-Service-62 IPS-Service-63 IPS-Service-64 IPS-Service-65 IPS-Service-66 IPS-Service-67 IPS-Service-68 IPS-Service-69 IPS-Service-70 IPS-Service-71 IPS-Service-72 IPS-Service-73 IPS-Service-74 IPS-Service-75 IPS-Service-76 IPS-Service-77 IPS-Service-78 IPS-Service-79 IPS-Service-80 IPS-Service-81 IPS-Service-82 IPS-Service-83 IPS-Service-84 IPS-Service-85 IPS-Service-86 IPS-Service-87 IPS-Service-88 IPS-Service-89 IPS-Service-90 IPS-Service-91 IPS-Service-92 IPS-Service-93 IPS-Service-94 IPS-Service-95 IPS-Service-96 IPS-Service-97 IPS-Service-98 IPS-Service-99 IPS-Service-100	Rename Object	IPS-Service-Group_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, Ra...	Rename Object	Severity-Info_1
static-cust-sig	Name: static-cust-sig, Type: static, Members: HTTP:MISC:XOOPS:WEBROOT	Name: static-cust-sig_1, Type: static, Members: Severity-Info	Rename Object	static-cust-sig_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-false-positives_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.

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 202 on page 313](#).

Figure 202: NSM Migration Status Page

Print Report

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

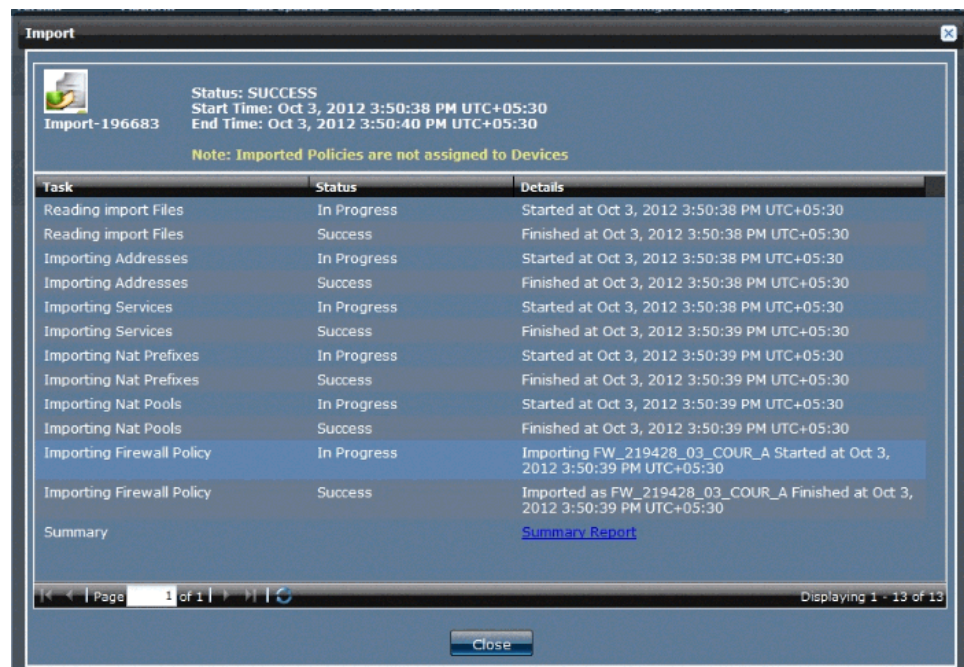
To print the summary report, click **Print Report** at the beginning of the page.



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 203 on page 314](#).

Figure 203: NSM Migration Final Status Report Page



7. Click on **Summary Report** to view the import summary as shown in [Figure 202](#) on [page 313](#)
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.

In Security Director, firewall rules are not disabled if IPS policy is configured during the device import. Security Director imports IPS policies along with the IPS on or off state in firewall rule. By default, after the import, firewall policy mode for IPS will be in *not configured* state.



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 303](#)

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 315](#)

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 204 on page 316](#).

Figure 204: Consolidated Config Status from Security Director

Name (Cluster)	OS Version	Platform	Last Updated	IP Address	Connection S...	Configuration...	Management...	Consolidated...	Pending Servi...
10.205.119...	11.2R7.4	SRX100B		10.205.119...	up	In Sync	Unmanaged	Does Not Exist	
10.205.50.2...	12.1R2.9	SRX1400		10.205.50.2...	up	In Sync	Unmanaged	Draft	
10.205.50.2...	12.1R2.9	SRX1400	Sep 11, 2012 3:27:03 PM UTC+05:30	10.205.50.2...	up	In Sync	Device Changed	Does Not Exist	
IsysDevice1 (10.205.50...	12.1R2.9	SRX1400	Sep 11, 2012 3:21:21 PM UTC+05:30	10.205.50.2...	up	In Sync	SD Changed, Device Changed	Does Not Exist	IsysDevice1
IsysDevice2 (10.205.50...	12.1R2.9	SRX1400	Sep 11, 2012 2:40:17 PM UTC+05:30	10.205.50.2...	up	In Sync	SD Changed, Device Changed	Does Not Exist	IsysDevice2
IsysDevice2 (Node-178) (Cluster)	11.4R5.5	SRX3400		10.205.50.1...	up	Out Of Sync	Unmanaged	Does Not Exist	
NewLSYS (10.205.50...	12.1R2.9	SRX1400		10.205.50.2...	up	In Sync	Unmanaged	Does Not Exist	
Node-178 (Cluster)	11.4R5.5	SRX3400		10.205.50.1...	up	In Sync	Unmanaged	Does Not Exist	
sd-srx240-1	12.1R2.9	SRX240B		10.205.119.5	up	In Sync	Unmanaged	Does Not Exist	
sd-srx240-6	12.1R2.9	SRX240B	Sep 12, 2012 3:07:28 PM UTC+05:30	10.205.119...	up	Out Of Sync	In Sync	Draft	
sd-srx650-4	12.1R2.9	SRX650	Sep 11, 2012 2:40:17 PM UTC+05:30	10.205.119.4	up	In Sync	SD Changed, Device Changed	Approved	All Devices Policy

Table 26 on page 316 shows different consolidated configuration status at different configuration levels.

Table 26: Different Status of Consolidated Configuration

CC Status	Description
Prepare	Subtask consists of publishing the consolidated configuration so that it can be reviewed, that is, validated on the device, approved or rejected, and deployed. NOTE: If you want to exclude or include configurations from a specific server-type (Firewall policy, NAT, and so on), the consolidated configuration must be regenerated with the changed parameters.
Validate	Validating a configuration on a device is a recommended prerequisite to deploying the configuration. Only a consolidated configuration that has already been generated can be validated.
Approve	Approving a consolidated configuration enables it to be deployed. Unapproved consolidated configurations cannot be deployed.
Reject	Rejecting a consolidated configuration prevents it from being deployed. Both approved and unapproved consolidated configurations can be rejected.
Deploy	Only approved consolidated configurations can be deployed.



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 299](#)

PART 11

Index

- [Index on page 321](#)

Index

Symbols

#, comments in configuration statements.....	xx
(), in syntax descriptions.....	xx
< >, in syntax descriptions.....	xx
[], in configuration statements.....	xx
{ }, in configuration statements.....	xx
(pipe), in syntax descriptions.....	xx

A

address and address groups overview.....	35
address groups	
creating.....	45
deleting.....	46, 47
managing.....	46
modifying.....	46
addresses	
cloning.....	38
creating.....	35
delete unused.....	44
deleting.....	38
duplicate objects.....	39
exporting.....	39
find usage.....	42
importing.....	39
managing.....	37
modifying.....	38
replace.....	42
unused.....	44
application groups	
deleting.....	32, 33
modifying.....	32
application signatures	
creating.....	53
managing.....	55
applications	
delete unused.....	30
deleting.....	25, 26
duplicate objects.....	26
find usage.....	27
modifying.....	25

replace.....	28
unused.....	30

B

braces, in configuration statements.....	xx
brackets	
angle, in syntax descriptions.....	xx
square, in configuration statements.....	xx

C

comments, in configuration statements.....	xx
configurations	
consolidated.....	315
consolidated configurations	
generating.....	315
managing.....	315
conventions	
text and syntax.....	xix
curly braces, in configuration statements.....	xx
customer support.....	xxi
contacting JTAC.....	xxi

D

dashboard	
overview.....	7
documentation	
comments on.....	xxi
Dynamic signature group	
creating.....	267

E

extranet device	
cloning.....	51
managing.....	50
modifying.....	50
Extranet Device	
deleting.....	50

F

Firewall policy	
adding rules.....	143
Adding rules before or after.....	160
address book.....	114
assigning devices.....	172
cloning.....	160
cloning rules.....	169
copying or pasting rules.....	171
creating.....	117

custom column.....	175, 176	IPS signature	
See also deleting		cloning.....	267
See also exporting		creating.....	263
See also managing		deleting.....	266
See also modifying		filtering.....	266
deleting.....	159	modifying.....	266
deleting devices.....	173	IPS signature set	
deleting rules.....	169	copying and pasting rules.....	273
enabling or disabling rules.....	170	expanding or collapsing rules.....	272
expanding or collapsing rules.....	171	grouping rules.....	272
exporting.....	161	IPS signature-set	
grouping rules.....	170	adding rules.....	269
inline object.....	134	creating.....	268
See also creating		managng.....	271
manage lock.....	132	IPsec VPN	
manage versioning.....	164	deleting.....	196
modifying.....	156	modifying.....	194
multiple group policy.....	110	modifying endpoint settings.....	195
ordering rules.....	147	overview.....	179
overview.....	107	publishing.....	192
priority and precedence.....	139	IPsec VPNs	
promoting.....	161	creating.....	181
publishing.....	149		
versioning.....	162		
Firewall Policy		M	
comparing.....	158	manuals	
font conventions.....	xix	comments on.....	xxi
G		N	
Global search.....	248	NAT	
		NAT policy	
I		publishing.....	227
Indexing overview.....	247	NAT pool	
IPS policy		managing.....	69
Adding rule before or after.....	294	NAT policy	
adding rules.....	285	assigning devices.....	242
cloning rules.....	292	cloning.....	231
copying and pasting rules.....	293	creating.....	205
creating.....	274	cutting/copying and pasting rules.....	240
deleting rules.....	292	deleting.....	231
enabling or disabling rules.....	292	deleting devices.....	242
expanding or collapsing rules.....	293	deleting rules.....	238
grouping rules.....	293	enabling or disabling rules.....	239
manage lock.....	283	expanding or collapsing rules.....	240
ordering rules.....	284	exporting.....	232
IPS Policy		global address book.....	219
publishing.....	287	grouping rules.....	239
		manage lock.....	218
		manage versioning.....	234
		modifying.....	231

overview.....	201	T	
publishing.....	227	technical support	
versioning.....	232	contacting JTAC.....	xxi
NAT pool		V	
duplicate objects.....	70	VPN profiles	
find usage.....	72	creating.....	84
replace.....	73	overview.....	83
unused.....	74		
NAT pools			
delete unused.....	75		
O			
Object Builder overview.....	19		
P			
parentheses, in syntax descriptions.....	xx		
S			
scheduler			
creating.....	60		
overview.....	59		
Scheduler			
deleting.....	62		
find usage.....	63		
managing.....	62		
modifying.....	62		
show unused.....	63		
Security Director devices			
importing policies.....	304		
updating.....	299		
Security Director Overview.....	3		
security policy profiles			
creating.....	78		
managing.....	81		
overview.....	77		
service and service groups overview.....	21		
service groups			
creating.....	31		
managing.....	32		
services			
creating.....	22		
managing.....	25		
Signature database			
downloading.....	253		
installing.....	255		
Static signature group			
creating.....	267		
support, technical See technical support			
syntax conventions.....	xix		

